GOETHE UNIVERSITÄT FRANKFURT

DOCTORAL THESIS

Sparse Random Models in Combinatorics

Author:
Joon LEE

Supervisor:
Prof. Dr. Amin COJA-OGHLAN

A thesis submitted in fulfillment of the requirements
for the degree of Doctor of Philosophy

in the

Discrete Mathematics
Institute of Mathematics

May 25, 2022

Declaration of Authorship

I, Joon LEE, declare that this thesis titled, “Sparse Random Models in Combinatorics” and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed:

_____

Date:

_____

GOETHE UNIVERSITÄT FRANKFURT

Abstract

Institute of Mathematics

Doctor of Philosophy

Sparse Random Models in Combinatorics

by Joon LEE

In this thesis, we cover two intimately related objects in combinatorics, namely random constraint satisfaction problems and random matrices. First we solve a classic constraint satisfaction problem, 2-SAT using the graph structure and a message passing algorithm called Belief Propagation. We also explore another message passing algorithm called Warning Propagation and prove a useful result that can be employed to analyze various type of random graphs. In particular, we use this Warning Propagation to study a Bernoulli sparse parity matrix and reveal a unique phase transition regarding replica symmetry. Lastly, we use variational methods and a version of local limit theorem to prove a sufficient condition for a general random matrix to be of full rank.

Acknowledgements

I have been given an incredible opportunity to research in mathematics for which I am indebted to so many people.

First I would like to thank my advisor, Professor Coja-Oghlan. He has been patient with me to stretch my mind and raise me up to think like a mathematician. I appreciate his generous giving of time, funding and brilliant discussions.

I also would like to sincerely thank Professor Gao for kindly agreeing to be an examiner and reading my thesis.

Additionally, I am thankful to Professors Gerstner, Neininger, Weth for their generosity with their time as reviewers.

I also appreciate my coauthors for their contribution and for their insight. Among those, I especially thank Professor Kang, Dr. Cooley, Professor Gao, Noela, Jean, Maurice and Max.

My colleagues in our group have become good friends over the past three years. I appreciate their sense of humor, candor and humanity. They are Max, Oli, Jean and Maurice. Special thanks go to Maurice who accommodated my extended stays in Dortmund.

Lastly, I thank my family. My parents have given their all for me. Their sacrifice afforded me to achieve this degree. I also thank my in-laws for their love and support.

My deepest appreciation goes to my wife, Tina. I thank her for her trust in me, for her love for me and our kids and all her hard work behind the scene. Because of her, I was able to finish it.

Contents

1 Preliminary

The so-called Big Data Analytics is pushing the boundary of human knowledge. It makes new discoveries that seemed unreachable just a few years ago while revealing its limitation still. Nevertheless, it will continue to impact many aspects of humanity as it already has [52]. Thus understanding the implication of given information and knowing how to use it would be crucial. How does one process such complex networks of data and find something useful? This quest has been a driving force of the modern world [17].

It seems daunting to analyze such networks where the data points are astronomical and demonstrate varying characteristics. The theory of random graphs offers accessible models that emulate the real world networks. The term *random graphs* came to the scene when Erdös and Rényi produced seminal papers on evolution of random graphs [40, 42]. In the Erdös - Rényi (ER) graph, V denotes the set of vertices or nodes and E denotes the set of edges between two nodes. The edges are randomly present according to a certain probability distribution. Their works are significant in many ways but especially so in promoting probabilistic methods and signifying the idea of phase transitions [9]. Alon and Spencer describe probabilistic methods in general as follows. In order to prove the existence of a structure with certain desired properties, one can define a probability space of structures and then show that such properties show up in this structure with positive probability. Furthermore, ER found phase transitions of such properties in terms of related parameters such that as the parameter passes through a critical value, the existence of the property shifts from surety to naught or vice versa [40, 41, 42]. Since they broke the ground of random graphs, countless others followed from many disciplines such as computer science, statistical physics, and biology, just to name a few.

Random graphical models are the favored representations of well-known models in statistical physics such as Ising model and spin glass model. Furthermore, various random constraint satisfaction models in computer science can easily be represented as random factor graphs to be discussed in Section 1.1.2. A popular way to analyze such models is by way of approximate message passing algorithms to be introduced in Section 2.1. Random graphs also have relevance in inference problems where one attempts to recover the underlying truth from noisy observations [90].

Another way to study random graphs is by their matrix representations. There are a number of helpful representations. The most natural representation is the adjacency matrix, a symmetric matrix whose ij-th entry is 1 if there exists an edge between the nodes i and j and 0 otherwise. Another related and more useful model for this work is the biadjacency matrix where the nodes are divided in two categories, one representing the rows and the other the columns. Edges are present only between two nodes from different categories. The benefit of using the biadjacency matrix to represent a bipartite

graph will be further explored in 1.1.2 when we define the factor graph. We also consider an even more general version in Section 3.2.

Random matrix in its own right is also a rich field to study (See [57]). Among many paths one can take in the random matrix theory, a combinatorial slice of it would be most closely related to the heart of this thesis. By that, we mean that the entries of the matrix are drawn from a discrete probability distribution. Among many interesting questions that can be raised about them, we consider the nullity and rank, especially the condition of being full rank (See [83, 84] for recent development).

The thesis is organized as follows. The papers in this thesis can largely be divided in two topics, namely random constraint satisfiability problems (rCSP) and combinatorial random matrices (CRM). In some aspects, they are the same objects represented distinctly. Before we introduce them, first we discuss some relevant ideas from statistical physics in Section 1.1. In Section 1.2, we introduce the particular rCSP problems we probed in this thesis . In Section 1.3, we discuss the particular models of CRM explored in this thesis. In Chapter 2, we present the methods used in the papers. In particular, a statistical physics inspired idea called message passing algorithm is presented and two specific models are highlighted in Section 2.1. We further explore ideas from statistical physics in Section 2.2 and detail variational methods such as Aizenman-Sims-Starr, cavity ansatz, and replica symmetry. In Chapter 3, we present the results of the four papers and succinctly lay out the proof strategies. In Chapter 4, the author's contribution for each paper is summarized. In Chapter 5, the summary is given in German. The papers are attached in the Appendix.

1.1 Angle from Statistical Physics

1.1.1 Mathematical Models for Disordered System

This section follows the exposition in [60] closely. Let Ω be a finite set of *spins* and let n denote the number of particles in a physical system. We call Ω^n the configuration space. For a configuration $\sigma \in \Omega^n$, let $\sigma_i \in \Omega$ denote the state of the i-th particle. In addition, let Λ denote a d dimensional lattice and let Λ_{adj} be the set of pairs of adjacent particles on Λ. The number of particles on the lattice Λ is n. When the system is made up of interactions among k particles, we define the *Hamiltonian* of the system as

$$H(\sigma) = -\sum_{i_1,\dots,i_k} J_{i_1,\dots,i_k}(\sigma_{i_1},\dots,\sigma_{i_k}) - \sum_{i=1}^{n} J_i(\sigma_i), \tag{1.1.1}$$

where $J_{i_1,\dots,i_k}(\sigma_{i_1},\dots,\sigma_{i_k})$ means the interaction energy among k particles and $J_i(\sigma_i)$ comes from the external energy which affects each particle and is usually expressed as $h\sigma_i$. We can think of $H(\sigma)$ as the *discomfort* function that measures the level of frustration when the configuration $\sigma \in \Omega^V$ assigns values to the variables.

In case $k = 2$ if the choice of pairs are restricted to Λ_{adj} and $\Omega = \{\pm 1\}$, the system is called the *Edwards-Anderson* model [39]. If the interaction energy term $J_{i_1,i_2} > 0$ for all adjacent pairs i_1, i_2, the system would prefer equal spins among the interacting particles and if $J_{i_1,i_2} < 0$, the system would prefer opposing spins since the lower the energy is, the more stable the system would be. In the first

case we call the system the *ferromagnetic Ising* model and for the latter, the *antiferromagnetic Ising*. If J_{i_1,i_2} is a mixed bag, then the system is called the *spin glass* model (See [69] for a brief introduction). The probability that the system is at the configuration σ then is expressed in terms of the *Boltzmann distribution*,

$$\mu_\beta(\sigma) = \frac{1}{Z(\beta)} \exp\left[-\beta H(\sigma)\right], \qquad Z(\beta) = \sum_{\tau \in \Omega^v} \exp\left[-\beta H(\tau)\right], \tag{1.1.2}$$

where $\beta = 1/T$ denotes the inverse temperature. $Z(\beta)$ is called the partition function which contains crucial information about the system (See [14] for an exposition of partition function). The minus sign here makes sense because the system prefers lower energy. It gives more weight to the lower energy. It resembles the earlier notion of searching for a configuration to get the lowest discomfort. We will denote the expectation of a random variable x drawn from a probability distribution ν as $\mathbb{E}_\nu[x]$. When the distribution is clear from context, then we write $\mathbb{E}[x]$.

It is possible to use the Boltzmann distribution in any system with n particles but it can be cumbersome to compute the partition function (1.1.2) by summing over Ω^n terms. One way to approximate the quantity is to use *mean-field approximation* where we consider all particles to interact with one another (see [39, 69, 79] for an exposition for mean-field models). A mean-field version of the Ising model is called the *Curie-Weiss* model where $\Omega = \{\pm 1\}$ as in the Ising model but any pair $i, j, 1 \le i < j \le n$ of particles interact with each other. One step further in generalization, the spin glass model of the Curie-Weiss model is called the *Sherrington-Kirkpatrick* (SK) model where we consider J_{i_1,i_2} to be drawn from the standard Gaussian distribution. Both models will be discussed further in Section 1.1.2.

1.1.2 Factor Graphs

Mean-field approximation provides a good initial step in studying disordered system because it ignores the geometrical structure of the lattice. However since these models came about to reflect physical systems where such geometrical restrictions must be accounted for, a mean-field model is not so realistic in a way. A remedy for such conundrum is the diluted mean field approach [82]. In SK model, all pairs are connected as in a complete graph but the interaction is of order $n^{-1/2}$. In a dilute SK model, the interaction is strong, of order $O(1)$ but only p/n fraction of nodes are connected. As $p \to \infty$, this dilute model behaves like SK. Thus, the dilute model offers a model that reflects the finite connection of the physical systems and yet is solvable as in SK. One convenient way to express the diluted interactions is to use a *factor graph*, expressing the interactions (mutual dependencies) of particles in a configuration by *factors* of adjacent particles [54]. The following portion defines and describes few more terms related to factor graphs, mirroring the exposition in [60].

Let Ω be a finite set as before. Enter the bipartite graph $G = (V, F)$ where V represents the set of n variables (particles) of the system and F denotes the set of factors. Edges are present with a random chance between a variable and a factor. If there exists an edge between $v \in V$ and $a \in F$, we call them neighbors. For $x \in V \cup F$, let ∂x denote the vertices in the neighborhood of x. The factor graph G has one more component, a weight function $\psi_a : \Omega^{\partial a} \to (0, \infty)$. Given a configuration $\sigma \in \Omega^n$, let $\sigma_{\partial a}$ denote the spins of the variables in ∂a. Then G has a Boltzmann probability distribution on the

configuration space Ω^n similarly as in (1.1.2),

$$\begin{aligned} \mu_G(\sigma) &= \frac{\psi_G(\sigma)}{Z_G}, \qquad & \sigma \in \Omega^n, \\ \psi_G(\sigma) &= \prod_{a \in F} \psi_a(\sigma_{\partial a}), \qquad & Z_G = \sum_{\sigma \in \Omega^n} \psi_G(\sigma), \end{aligned} \tag{1.1.3}$$

where Z_G is the partition function as before. In physics problems, $\psi_a(\sigma_{\partial a})$ takes the form of $\exp\left[-\beta E_a(\sigma_{\partial a})\right]$ so we can see this form is analogous to the interacting energy term in (1.1.1) and Boltzmann distribution (1.1.2). We defined the sum of interacting energy in (1.1.1) as the total energy which in turn can be expressed with factor graph terms, namely $E_G = -\log \psi_G(\sigma)$. Furthermore, the *internal energy* of G is defined as the expectation of the total energy,

$$U_G = -\mathbb{E}_{\mu_G}\left[\log \psi_G(\sigma)\right] = -\sum_{\sigma \in \Omega^n} \mu_G(\sigma) \sum_{a \in F} \psi_a(\sigma_{\partial a}). \tag{1.1.4}$$

The entropy according to a probability distribution ν on Ω^n takes the usual form

$$H(\nu) = -\sum_{\sigma \in \Omega^n} \nu_G(\sigma) \log \nu_G(\sigma) \tag{1.1.5}$$

which gauges the level of uncertainty of the random variable σ such that the lower the entropy is, the more information is known. We also define the *free energy* of G as

$$\Phi_G = \log Z_G. \tag{1.1.6}$$

We have defined the terms so far to make a point about the Boltzmann distribution. It turns out that the Boltzmann distribution μ_G can be viewed as the maximizer of a certain functional called the *Gibbs free energy* of a probability distribution ν on Ω^n [60],

$$\mathscr{G}[\nu] = H(\nu) - \mathbb{E}_\nu\left[E_G\right]. \tag{1.1.7}$$

A few lines of calculation shows that (1.1.7) can be expressed in terms of the free energy, $\mathscr{G}[\nu] = \Phi_G - D_{\mathrm{KL}}\left(\nu \| \mu_G\right)$ where $D_{\mathrm{KL}}\left(\nu \| \mu_G\right)$ stands for Kullback-Leibler divergence of the two probability distributions ν, μ_G. Because $D_{\mathrm{KL}}\left(a \| b\right) \geq 0$ for any distributions a, b, $\mathscr{G}[\nu]$ yields a lower bound on Φ_G for any ν. Moreover, because $D_{\mathrm{KL}}\left(a \| b\right) = 0$ iff $a \equiv b$, the Boltzmann distribution μ_G is the unique maximizer of $\mathscr{G}[\nu]$ which equals the free energy, Φ_G.

We are mostly concerned with the state of matter in the limit of n. Thus the *free energy density* is defined as

$$\phi(\beta) = \lim_{n \to \infty} \frac{1}{n} \Phi_{G_n}. \tag{1.1.8}$$

As we will see in Section 2.1, under certain conditions on the system, the free energy density can be calculated by a message passing algorithm called the *Belief Propagation*. That is, the free energy density is effectively given by a functional called the *Bethe free energy*, $\mathscr{B}$, to be shown in (2.1.5) in Section 2.1.1. That is one side of the equation. The other side of the equation is to express the free energy density by perturbing the system. This perturbation is done by what physicists call the *cavity*

method [61]. It involves removing either a variable or a constraint node from the system thereby creating a *cavity*. We will come to the details of this idea in Sections 2.3.2.

1.2 Random Constraint Satisfiability Problems

A constraint satisfiability problem (CSP) consists of n variables, $x_1, x_2, \ldots, x_n$ and m constraints $a_1, a_2, \ldots a_m$. The aim is to see if there is a configuration that satisfies all the constraints, and if so, to come up with such a configuration and to see collectively what the solution set looks like. The idea of a random CSP was introduced in 1980s in order to come up with an efficient algorithm to solve CSPs [43]. Based on the cavity method, first the survey propagation [62] was invented, followed by the belief propagation's success in solving CSPs [15, 12, 68]. We will now use the factor graph model to define the k-SAT, in particular 2-SAT and the k-XORSAT. We will also discuss the solution space of k-SAT to illustrate the idea of phase transition.

1.2.1 k-SAT

Let $k \geq 2$ be an integer and here $\Omega = \{0,1\}$. For $n, m > 0$, we define an instance $\Phi_k(n,m) = a_1 \wedge \cdots \wedge a_m$ a k-SAT formula when each of m clauses chooses k Boolean variables among $\{x_1, \neg x_1, \ldots, x_n, \neg x_n\}$ uniformly at random out of all $(2n)^{km}$ possible such formulas. The solution space then is a subset of the lattice Ω^n, i.e. the set of configurations that satisfy all m constraints. Given a value for the inverse temperature $\beta > 0$, we define the weight function for the factor graph model as

$$\psi_{\beta,i}(\sigma) = \exp\left[-\beta \mathbb{1}[a_i \text{ is violated under } \sigma]\right]. \tag{1.2.1}$$

The Boltzmann distribution and the partition function are similarly defined as in (1.1.3). Then it is easy to see that

$$\mu_{\Phi,\beta}(\sigma) = \frac{\exp\left[-\beta \cdot |\{a_i, \text{ such that } a_i = \text{false}\}|\right]}{Z_{\Phi,\beta}}.$$

Therefore, if we consider $\beta \to 0$ thus $T \to \infty$, then $\mu_{\Phi,\beta}$ becomes the uniform distribution among Ω^n. On the other hand, when $\beta \to \infty$, therefore $T \to 0$, μ puts more weight on satisfying assignments thereby facing hard constraints. We call $\alpha = m/n$ the *constraint density*. Experimental work had already confirmed the conjecture that there exists a sharp satisfiability threshold for $k \geq 3$ [23, 63]. In other words, there exists $\alpha_{sat} > 0$ (sat for satisfiability) such that as α passes over α_{sat}, the probability of that the random formula Φ has a solution goes from 1 w.h.p.to 0 w.h.p. Much work has been done in the last few decades to identify α_{sat} in various settings (See [29, 30, 37, 68]).

Statistical physicists used a non-rigorous yet effective scheme called the cavity method to study the random k-SAT [30]. In particular, they made a conjecture [58, 62] that the satisfiability threshold is

$$\alpha_s = 2^k \ln 2 - \frac{1+\ln 2}{2} + o_k(1). \tag{1.2.2}$$

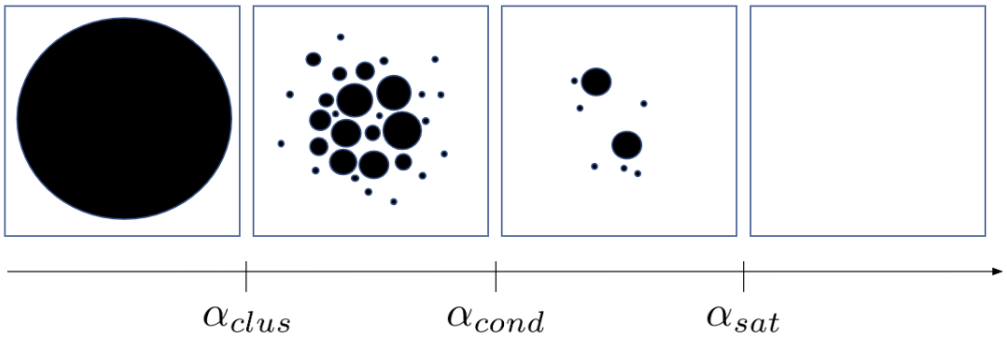

FIGURE 1.1: *Figure adapted and modified from* [53]. *Leftmost:* $\mathscr{S}$ is one cluster w.h.p.; *Second:* As α passes through α_{clus}, $\mathscr{S}$ the solutions are split among a large of number of disconnected clusters until α_{cond}; *Third:* a few clusters dominate $\mathscr{S}$; *Rightmost:* beyond α_{sat} $\mathscr{S}$ is empty. w.h.p..

Coja-Oghlan and Panagiotou proved this result [30]. The gap between the upper bound and the lower bound was closed by Ding, Sun, and Sly [37] for large $k \geq k_0$, where k_0 is some unspecified constant,

$$\alpha_s = 2^k \ln 2 - \frac{1+\ln 2}{2} + O(2^{-k}). \tag{1.2.3}$$

For small k, the threshold is still an open question.

1.2.2 Phase Transition and Replica Symmetry

Let $\mathscr{S}$ denote the solution space of a random constraint satisfaction problem, i.e. the set of all configurations satisfying a random k-SAT formula. Beyond the satisfiability threshold, there are several other thresholds that shed light on the behavior of $\mathscr{S}$ [53]. One crucial threshold relevent to this thesis is α_{cond} called the *condensation* threshold where a new phase called 1RSB (1-Replica Symmetry Breaking) is realized (See [67] for 1RSB phase in k-SAT and k-XORSAT).

We say that a pair of solutions is connected if its Hamming distance equals 1 and call the set of connected solutions a *cluster*. On $0 < \alpha < \alpha_{clus}$ where α_{clus} stands for *clustering threshold*, most of the solutions are in one cluster. Some smaller clusters appear but they comprise only an exponentially small fraction of solutions while most solutions belong to one giant cluster. This phase is called the *replica symmetric* (RS) phase. On $\alpha_{clus} < \alpha < \alpha_{cond}$, the solutions are disconnected among exponentially many exponentially small clusters. Within this phase, the size of clusters continues to decrease as the solution space continues to shatter. However, since each cluster weighs a negligible mass compared to the total, as $n \to \infty$ it is as if there are no clusters [53]. That is why this phase is sometimes called the *dynamic replica symmetric breaking* phase or included in the replica symmetric phase. For $\alpha_{cond} < \alpha < \alpha_{sat}$, $\mathscr{S}$ is dominated by a few clusters. This is where the 1RSB occurs. This phase is called the *static replica symmetric breaking* phase. Finally, $\alpha_{sat} < \alpha \leq 1$, $\mathscr{S}$ is empty (see Figure 1.1).

What do these physics terms mean? Replica symmetry means that in RS phase ($\alpha < \alpha_{cond}$) factor graphs can basically be treated as though they were acyclic [60, Chapter 14]. This implies that BP produces a fixed point that results in the correct value for the free energy. Physicists conjectured that

RS ansatz applies if the random factor graph model enjoys a certain pairwise decorrelation property [53]. This conjecture was proven; that the asymptotic independence is enough to make RS ansatz work [31].

1.2.3 2-SAT

Now we focus on the 2-SAT problem. There are n variable nodes and $\boldsymbol{m} = \mathrm{Po}(dn/2)$ many check nodes. As before, let V, F denote the sets of variables and checks respectively. For each $a \in F$, it has two distinct neighbors $x_1, x_2 \in V$ so it has $n(n-1)$ many options of pairs to choose from. Furthermore, it can choose a relation among the four following disjunctions

$$x_1 \vee x_2, \quad x_1 \vee \neg x_2, \quad \neg x_1 \vee x_2, \quad \neg x_1 \vee \neg x_2,$$

so each check is one disjunction among $4n(n-1)$. Then an instance of 2-SAT would be a conjunction of disjunctions

$$\boldsymbol{\Phi} = a_1 \wedge \cdots \wedge a_{\boldsymbol{m}}.$$

The random 2-SAT problem was the first rCSP where α_{sat} was pinned down, independently by Chvátal and Reed [75] and Goerdt [46] in 1992. Other works on 2-SAT followed since. Bollobás, Borgs, Chayes, Kim and Wilson [20] succeeded in finding the scaling window of the satisfiability threshold which also matched the scaling window of the giant component phase transition of the ER random graph [19, 56]. These previous results paved the way for more discoveries regarding variations of the 2-SAT model such as the random 2-SAT formulas with given literal degrees [33], the random MAX 2-SAT problem where the target is to maximize the number of satisfied constraints above α_{sat} [34].

Despite many milestones regarding 2-SAT variants, finding the number of solutions of a random 2-SAT had remained open. Just as in the k-SAT problem, physicists' input was crucial in making discoveries about the 2-SAT problem. Their modus operandi derived from the aforementioned cavity method is a message passing algorithm called *Belief Propagation* (BP). As we shall see in 2.1.1, BP calculates the marginal probability that a random variable takes a Boolean value. By way of BP, we show that the Bethe free entropy, $\phi(\beta)$ gives the number of satisfying assignment of 2-SAT. The fact that $\phi(\beta)$ is the tight upper bound on $\frac{1}{n}\log Z(\Phi)$ had been known via the so-called interpolation method [44, 71, 47]. Thus, we find a lower bound of the number of solution which is also tight, thereby proving the conjecture made by Monasson and Zecchina [66]. The proof relies on finding a solution to a stochastic fixed point equation and applying it to the Bethe free density. It also relies on the fast convergence of the fixed point equation. Similar to (1.2.1), we can express the 2-SAT formula using the idea of factor graph as follows. With the inverse temperature $\beta > 0$,

$$Z_\beta(\boldsymbol{\Phi}) = \sum_{\sigma \in \{\pm 1\}^n} \prod_{i=1}^{\boldsymbol{m}} \exp\left(-\beta \mathbb{1}\{\sigma \text{ violates clause } a_i\}\right). \tag{1.2.4}$$

The challenge is in driving the limit $\beta \to \infty$ to satisfy the 'hard' constraints condition. Montanari

and Shah [68], Panchenko [70] and Talagrand [78] investigated 'soft' versions of the partition function. For instance, Montanari and Shah [68] obtained $\lim_{n\to\infty}\frac{1}{n}\mathbb{E}[\log Z_\beta(\mathbf{\Phi})]$ for all finite β under the assumption $d < 1.16\ldots$ thus not all the way to the threshold $d = 2$.

In order to prove the conjecture albeit with some conditions on d, all three works [68, 70, 78] use the Gibbs uniqueness property, that is, the Boltzmann distribution is the unique fixed point of BP. While the Gibbs uniqueness is also our main driver, we develop a more accurate method for verifying the Gibbs uniqueness property based on the explicit construction of an extremal boundary condition that is unique to the case of 2-SAT. In terms of a local structure of a Galton Watson branching process, one can come up with extremal boundary conditions on the leaves to conjure up the maximum bias for the marginal distribution for a root because there are only two variables connected to one constraint.

For $d < 1$ the random digraph of the 2-SAT formula is sub-critical and the free energy density can be calculated by counting arguments. On $1 < d < 2$, a weak giant component will appear so it is not trivial to compute the partition function. Finally, as mentioned above, $d = 2$ is the satisfiability threshold. Thus from now on, we assume $0 < d < 2$. We will further discuss how these ideas fit together to compute the number of solutions of a random 2-SAT in 3.1.

1.2.4 k-XORSAT

A k-XORSAT instance is composed of m linear equations in $\mathbb{F}_2$ over n variables. Each equation gets k variables and is equal to either 0 or 1. Equivalently, it is a linear system $Ax = b \mod 2$ in which $A \in \mathbb{M}_{m\times n}(\mathbb{F}_2)$ is a matrix, each row in which gets k non-zero entries and $b \in \mathbb{F}_2^n$. A random k-XORSAT instance then would be made of a random matrix $\boldsymbol{A}$ and a random vector $\boldsymbol{b}$.

Just as in the case of k-SAT Section 1.2.1, the solution space $\mathscr{S}$ of a k-XORSAT goes through a phase transition as the constraint density $c = m/n$ passes through a certain critical ratio c^*. Namely, as $m, n \to \infty$, if $\lim c < c^*$, the probability that a random instance $\mathbb{F}_{n,m}$ is satisfiable is 1 w.h.p.while if $\lim c > c^*$ the probability approaches 0 [53].

Dubois and Mandler considered a constrained random k-XORSAT model, where $\boldsymbol{b}$ is uniformly random, but $\boldsymbol{A}$ is uniformly random over the subset of matrices in which each column sum has at least two non-zero entries so that each variable shows up at least twice in the system. They showed that its threshold for m/n in the constrained 3-XORSAT is 1 [38]. They used this result to derive the result for an unconstrained 3-XORSAT. They did it through a process called *Unit Clause Propagation* (UCP) which reduces the unconstrained model to the constrained model and by showing that UCP does not alter the threshold. Pittel and Sorkin identified the satisfiability threshold for k-XORSAT over $\mathbb{F}_2$ for all k, followed by results on $\mathbb{F}_3, \mathbb{F}_4$ [72]. However, their methods do not cover other fields [5, 36, 38, 49, 72]. This question is directly linked to finding the rank of the matrix. We shall continue on this topic in the next Section 1.3 and say few more words about UCP in Section 2.1.2.

1.3 Combinatorial Random Matrices

1.3.1 Studying rCSP via CRM

rCSP and CRM are intertwined in various implications. Thus understandably combinatorial matrices have made impact in many applications including powerful error correcting codes called low-density parity check codes [76], data compression [4, 85] and hashing [36].

CRM can be large divided into *dense* and *sparse* kinds. By sparse, we mean that it has a bounded average number of non-zero entries per row or column. We know more about the dense kinds than we do about the sparse ones because concentration techniques apply more easily in the dense case [83, 84]. Another clue about the difficulty in analyzing the sparse matrices is highlighted in the close connection between the sparse random matrices and random satisfaction problems which are known to be notoriously difficult [7].

Especially relevant for the thesis is the k-XORSAT model as discussed the previous Section 1.2.4. The constraints will take the role of rows and the variables will occupy the columns. For each constraint, the connected variables will take 1 and others 0. Solving the rCSP would then be equal as solving the system of linear equations. From the matrix point of view, solvability would also imply whether the matrix is full rank or not. Thus we are dealing with the rank of random matrices as well the satisfiability threshold.

Here we introduce the notion of the *fraction of frozen variables* [26]. In an instance of $\boldsymbol{A}x = \boldsymbol{y}$, consider the solution set. Equivalently, we can consider the kernel of A since the solution set would be a translation of the kernel. Let $[t]$ denote $\{1,2,\ldots,t\}$ for a positive integer t. We denote the kernel of a matrix T as $\ker T$. Then we call the variable $i \in [n]$ *frozen* if all the vectors in the kernel set take 0 in the ith entry. In addition, we denote the fraction of frozen variables by

$$f(\boldsymbol{A}) = |\{i \in [n] : \forall x \in \ker \boldsymbol{A} : x_i = 0\}| / n. \tag{1.3.1}$$

As discussed in Section 1.2.4, a random k-XORSAT has a sharp satisfiability threshold [36, 38, 72]. What is peculiar about its satisfiability threshold is that it is strictly smaller than the obvious point $m/n = 1$ beyond which the corresponding $\mathbb{F}_2$-matrix has more rows than columns and is no longer full row rank. Indeed, the satisfiability threshold occurs when a linear number of variables freeze which is strictly less than 1 [38]. Thus, the notion of $f(\boldsymbol{A})$ plays a major role in studying the rank of $\boldsymbol{A}$.

1.3.2 Nullity and Rank

Here we introduce an important theorem regarding the rank and nullity in terms of $f(\boldsymbol{A})$. Theorem 1.1 in [26] yields an asymptotic formula for the normalized nullity of a sparse random linear system in terms of a parameter α that heuristically equals $f(\boldsymbol{A})$. This theorem will be used in both papers regarding CRM [24, 27] thus we write down the general form here. The following setup largely follows the one from [27].

Let $\boldsymbol{d} \geq 0$, $\boldsymbol{k} \geq 3$ be independent integer-valued random variables such that $\mathbb{E}[\boldsymbol{d}^{2+\eta}] + \mathbb{E}\left[\boldsymbol{k}^{2+\eta}\right] < \infty$ for an arbitrarily small $\eta > 0$. Let $(\boldsymbol{d}_i, \boldsymbol{k}_i)_{i\geq 1}$ be independent copies of $(\boldsymbol{d}, \boldsymbol{k})$ and set $d = \mathbb{E}[\boldsymbol{d}], k = \mathbb{E}[\boldsymbol{k}]$. Moreover, let $\mathfrak{d} = \gcd\{\mathrm{supp}(\boldsymbol{d})\}$ and $\mathfrak{k} = \gcd\{\mathrm{supp}(\boldsymbol{k})\}$. Let n be integer divisible by $\mathfrak{k}$ and $\boldsymbol{m} = \mathrm{Po}(dn/k)$, independent of $(\boldsymbol{d}_i, \boldsymbol{k}_i)_i$. It can be shown

$$\sum_{i=1}^{n} \boldsymbol{d}_i = \sum_{j=1}^{\boldsymbol{m}} \boldsymbol{k}_j, \tag{1.3.2}$$

that is, the sums of degrees match with probability at least $\Omega(n^{-1/2})$ [26, Proposition 1.7]. Given (1.3.2) let $\mathbb{G} = \mathbb{G}_n(\boldsymbol{d}, \boldsymbol{k})$ denote a simple random bipartite graph on a set of checks $\{a_1 \ldots, a_{\boldsymbol{m}}\}$ and a set of variables $\{x_1, \ldots, x_n\}$ such that $|\partial a_i| = \boldsymbol{k}_i$ and the degree of $\left|\partial x_j\right| = \boldsymbol{d}_j$ for all i, j. The edges of $\mathbb{G}$ denote the positions of the non-zero entries of the associated matrix $\mathbb{A}$, which can be from a finite field or $\{0,1\}$ regarded as rational numbers. Let us focus on a matrix over a finite field $\mathbb{F}_q$ where $q = p^\ell$ for p prime. Let $\boldsymbol{\chi}$ be a random variable in $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. Let $\mathrm{rk}(\mathbb{A})$ and $\mathrm{nul}(\mathbb{A})$ denote the rank and nullity of $\mathbb{A}$ respectively. We tacitly mention that $\mathrm{rk}(\mathbb{A}) + \mathrm{nul}(\mathbb{A}) = n$. Then $\mathbb{A} = \mathbb{A}_n(\boldsymbol{d}, \boldsymbol{k}, \boldsymbol{\chi})$ is the $\boldsymbol{m} \times n$-matrix with entries

$$\mathbb{A}_{i,j} = \mathbb{1}\{a_i x_j \in E(\mathbb{G})\} \cdot \boldsymbol{\chi}_{i,j}$$

where $\boldsymbol{\chi}_{i,j}$ are copies of $\boldsymbol{\chi}$. We remark that the i-th row of $\mathbb{A}$ contains $\boldsymbol{k}_i$ non-zero entries and the j-th column contains $\boldsymbol{d}_j$ non-zero entries.

We denote the probability generating functions of $\boldsymbol{d}$ and $\boldsymbol{k}$ as $D(x)$ and $K(x)$, respectively.

Define

$$\Phi : [0,1] \to \mathbb{R}, \qquad \alpha \mapsto D\left(1 - K'(\alpha)/k\right) - \frac{d}{k}\left(1 - K(\alpha) - (1-\alpha)K'(\alpha)\right). \tag{1.3.3}$$

The following theorem determines the *normalised* rank of $\mathbb{A}$:

Theorem 1.3.1 ([26, Theorem 1.1])**.**

$$\frac{\mathrm{rk}(\mathbb{A})}{n} \xrightarrow{\mathbb{P}} 1 - \max_{\alpha \in [0,1]} \Phi(\alpha) \qquad \text{as } n \to \infty. \tag{1.3.4}$$

Full Rank

We already mentioned that a satisfiability threshold in a k-XORSAT corresponds to the analogous random matrix being full rank. Indeed, the question of whether the random matrix matrix model at hand is likely full rank or not is of a fundamental importance. In the second paper on the rank [27], we consider this question for a broader class of sparse combinatorial random matrices of dimension $\boldsymbol{m} \times n$. Note that Theorem 1.3.1 concerns the normalized rank of $\mathbb{A}$. This implies that we still get an error of $o(n)$ for $\mathrm{rk}(\mathbb{A})$. Thus, in [27] we study the rank directly and draw a conclusion about a sufficient condition for the matrix to be full rank which is described in terms of (1.3.4). The condition turns out to be essentially necessary too.

We proceed to set the basic premises for the main results in our second paper on rank [27] in the current section. Proving them requires ascertaining two other relations; once we prove them, the main results can be readily proven. Thus, this section works to convince the reader why we take the detour to the other lemmas. In Section 3.4, we will mainly focus on the proof strategy of the lemmas.

Annealed vs Quenched

This section follows [27, Section 2.1] closely. We first describe an *annealed* computation and show that it overshoots the actual value we are seeking. In order to reduce fluctuations we condition on the σ-algebra $\mathfrak{A}$ generated by $\boldsymbol{m}, (\boldsymbol{k}_i)_{i\geq 1}, (\boldsymbol{d}_i)_{i\geq 1}$ and by the numbers $\boldsymbol{m}(\chi_1,\dots,\chi_\ell)$ of checks of degree $\ell \geq 3$ with coefficients $\chi_1,\dots,\chi_\ell \in \mathbb{F}_q^*$. We use $\mathbb{P}_{\mathfrak{A}} = \mathbb{P}[\cdot \mid \mathfrak{A}]$ and $\mathbb{E}_{\mathfrak{A}} = \mathbb{E}[\cdot \mid \mathfrak{A}]$ for brevity.

The second moment method has been a staple tool to find the satisfiability thresholds for rCSP [6, 7]. Indeed, it was one of the key ideas used to solve the random 3-XORSAT problem [38]. It boils down to finding the full rank threshold over $\mathbb{F}_2$. Let us discuss the random 3-XORSAT for a moment. We apply the second moment method to the number of solutions, $\boldsymbol{Z} = \boldsymbol{Z}(\mathbb{A}, \boldsymbol{y})$ to $\mathbb{A}x = \boldsymbol{y}$, where the field is $\mathbb{F}_2, \boldsymbol{d} = \mathrm{Po}(d), d > 0, \boldsymbol{k} = 3$. Note that $\boldsymbol{y}$ is random and independent of $\mathbb{A}$. Thus, the probability of any fixed vector $x \in \mathbb{F}_2^n$ being a solution to $\mathbb{A}x = \boldsymbol{y}$ is $2^{-\boldsymbol{m}}$. There are 2^n possible vectors so we have [27, Eq. 2.1]

$$\mathbb{E}_{\mathfrak{A}}[\boldsymbol{Z}] = 2^{n-\boldsymbol{m}}.$$

It is apparent from this relation that the satisfiability threshold is at when $n = \boldsymbol{m}$, which implies $d < 3$. The second moment method works when $\mathbb{E}_{\mathfrak{A}}\left[\boldsymbol{Z}^2\right] \sim \mathbb{E}_{\mathfrak{A}}[\boldsymbol{Z}]^2$ in which case Chebyshev's inequality comes to rescue to pin down $\boldsymbol{Z}$ in the vicinity of the expected value. Since $\boldsymbol{Z}$ is either empty or a translation of the kernel, we obtain [[27, Eq. 2.2]]

$$\mathbb{E}_{\mathfrak{A}}[\boldsymbol{Z}^2] = \sum_{\sigma,\tau\in\mathbb{F}_q^n} \mathbb{P}_{\mathfrak{A}}\left[\mathbb{A}\sigma = \mathbb{A}\tau = \boldsymbol{y}\right] = \sum_{\sigma,\tau\in\mathbb{F}_q^n} \mathbb{P}_{\mathfrak{A}}\left[\mathbb{A}\sigma = \boldsymbol{y}\right] \mathbb{P}_{\mathfrak{A}}[\sigma - \tau \in \ker \mathbb{A}] = \mathbb{E}_{\mathfrak{A}}[\boldsymbol{Z}]\,\mathbb{E}|\ker \mathbb{A}|. \tag{1.3.5}$$

We calculate the expected kernel size, observing that the probability that a vector x is in the kernel depends on its Hamming weight, w. Indeed, for a vector x with w we get

$$\mathbb{P}_{\mathfrak{A}}[x \in \ker \mathbb{A}] \sim \left(\frac{1+\left(1-\frac{2w}{n}\right)^3}{2}\right)^{\boldsymbol{m}}.$$

Furthermore, since there are $\binom{n}{w}$ many vectors with Hamming weight w, we have [27, Eq. 2.3]

$$\mathbb{E}_{\mathfrak{A}}|\ker \mathbb{A}| = \sum_{w=0}^{n} \binom{n}{w} \left(\frac{1+\left(1-\frac{2w}{n}\right)^3}{2}\right)^{\boldsymbol{m}}. \tag{1.3.6}$$

Stirling's formula and parametrizing $w = zn$ simplify (1.3.6) to [27, Eq. 2.4]

$$\log \mathbb{E}_{\mathfrak{A}}|\ker \mathbb{A}| \sim n \cdot \max_{z\in[0,1]} -z\log z - (1-z)\log(1-z) + \frac{\boldsymbol{m}}{n}\log\frac{1+(1-2z)^3}{2} \tag{1.3.7}$$

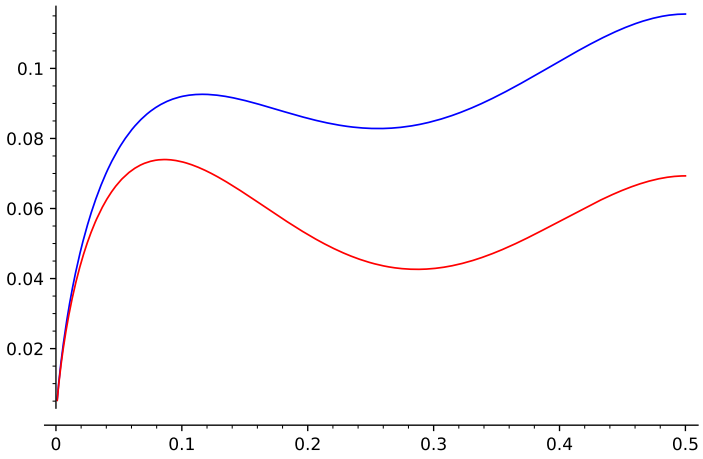

FIGURE 1.2: [27, Figure 3]. The r.h.s. of (1.3.7) for $d = 2.5$ (blue) and $d = 2.7$ (red).

Imagine x is a *balanced* vector such that its Hamming weight is about $n/2$. If $z = 1/2$ is applied to (1.3.7), then the result simplifies to $(n - \boldsymbol{m})\log 2$ and the second moment method works well. However, if the maximum is attained at another value $z \neq 1/2$, then (1.3.7) yields $\mathbb{E}_{\mathfrak{A}}|\ker \mathbb{A}| \gg 2^{n-\boldsymbol{m}}$ and the second moment method fails. Figure 1.2 displays (1.3.7) for $d = 2.5$ and $d = 2.7$. For $d = 2.5$ the function takes the maximum at $z = 1/2$. However, for $d = 2.7$ the maximum is at $z \approx 0.085$ which nullifies the second moment method's analysis. However, the true random 3-XORSAT threshold is $d \approx 2.75$ [38]. Thus, applying the second moment calculation directly to $\boldsymbol{Z}$ fails.

This example highlights the distinction between *annealed* and *quenched* moment computations. It boils down to which action is taken first, log or $\mathbb{E}_{\mathfrak{A}}$. Because $\boldsymbol{Z}$ is a potentially exponential value, it is often possible that

$$\log \mathbb{E}_{\mathfrak{A}}[\boldsymbol{Z}] \nsim \mathbb{E}_{\mathfrak{A}}\left[\log \boldsymbol{Z}\right]. \tag{1.3.8}$$

The l.h.s. of (1.3.8) is called the annealed moment and the r.h.s. is called the quenched moment (See [61] for a deeper look at these different moments). The bottom line is that the annealed moment is too susceptible to large deviation effects where some pathological events bias the calculation. For the random 3-XORSAT Dubois and Mandler were successful in identifying the precise large deviations effect by considering a minor obtained by UCP (See Section 2.1.2) and came up with a more intricate optimization problem than (1.3.7) [38]. We consider a similar optimization problem but their methods of keeping track of the large deviation effects cannot work in our general setting of $\boldsymbol{d}, \boldsymbol{k} \geq 3, \mathbb{F}_q$. Therefore, we proceed with a quenched argument, i.e. we work out moment calculation in the benign case of *equitable* or *balanced* solutions. This proof strategy generalizes the methods developed in [11, 26].

Let us now set the premise. The optimization problem we consider comes in terms of variables $(z_i)_{i \in \mathrm{supp}\boldsymbol{d}}$ that range over the space $\mathscr{P}(\mathbb{F}_q)$ of probability distributions on $\mathbb{F}_q$. We also consider a second set of variables $(\hat{z}_{\chi_1,\ldots,\chi_\ell})_{\ell \in \mathrm{supp}\boldsymbol{k}, \chi_1,\ldots,\chi_\ell \in \mathrm{supp}\boldsymbol{\chi}}$, those which range over probability distributions on solutions to the linear equation $\chi_1\sigma_1 + \cdots + \chi_\ell\sigma_\ell = 0$. Thus these variables are related to the rows of

$\mathbb{A}$. In terms of these variables we need to optimize the following [27, Eq. 2.5].

$$\begin{aligned}
\max \quad & \sum_{\sigma\in\mathbb{F}_q} \mathbb{E}\left[(\boldsymbol{d}-1)z_{\boldsymbol{d}}(\sigma)\log z_{\boldsymbol{d}}(\sigma)\right] \\
& -\frac{d}{k}\mathbb{E}\left[\sum_{\substack{\sigma_1,\dots,\sigma_{\boldsymbol{k}}\in\mathbb{F}_q \\ \boldsymbol{\chi}_{1,1}\sigma_1+\cdots+\boldsymbol{\chi}_{1,\boldsymbol{k}}\sigma_{\boldsymbol{k}}=0}} \hat{z}_{\boldsymbol{\chi}_{1,1},\dots,\boldsymbol{\chi}_{1,\boldsymbol{k}}}(\sigma_1,\dots,\sigma_{\boldsymbol{k}})\log\hat{z}_{\boldsymbol{\chi}_{1,1},\dots,\boldsymbol{\chi}_{1,\boldsymbol{k}}}(\sigma_1,\dots,\sigma_{\boldsymbol{k}})\right] \qquad (1.3.9) \\
& \text{s.t.} \quad \mathbb{E}[\boldsymbol{d}z_{\boldsymbol{d}}(\tau)] = \mathbb{E}\left[\sum_{\substack{\sigma_1,\dots,\sigma_{\boldsymbol{k}}\in\mathbb{F}_q \\ \boldsymbol{\chi}_{1,1}\sigma_1+\cdots+\boldsymbol{\chi}_{1,\boldsymbol{k}}\sigma_{\boldsymbol{k}}=0}} \boldsymbol{k}\mathbb{1}\{\sigma_1=\tau\}\,\hat{z}_{\boldsymbol{\chi}_{1,1},\dots,\boldsymbol{\chi}_{1,\boldsymbol{k}}}(\sigma_1,\dots,\sigma_{\boldsymbol{k}})\right] \qquad \text{for all } \tau\in\mathbb{F}_q.
\end{aligned}$$

Similar to the random 3-XORSAT, the balanced solution [27, Eq. 2.6]

$$z_i(\sigma) = q^{-1} \qquad \hat{z}_{\chi_1,\dots,\chi_\ell}(\sigma_1,\dots,\sigma_\ell) = q^{1-\ell} \qquad \text{for all } i,\chi_1,\dots,\chi_\ell \qquad (1.3.10)$$

gets the value $(1-d/k)\log q$ when applied in (1.3.9). This value matches the normalized first moment $\frac{1}{n}\log\mathbb{E}_{\mathfrak{A}}[\boldsymbol{Z}]$.

So how do we use the quenched calculation to prove the main result? Applying log to $\boldsymbol{Z}$ and then calculating expectation amounts to finding the mean of $\dim\ker\mathbb{A}$. This quenched average is of order $O(n)$ and it is not affected by large deviations effects. Yet computing the quenched average alone does not solve away the sizeable error $o(n)$. To that end, let us consider a suitable event and explain what that entails. First let $\boldsymbol{x}_{\mathbb{A}} = (\boldsymbol{x}_{\mathbb{A},i})_{i\in[n]} \in \mathbb{F}_q^n$ be a random vector in $\ker\mathbb{A}$. We define the event [27, Eq. 2.7]

$$\mathfrak{O} = \left\{\sum_{\sigma,\tau\in\mathbb{F}_q}\sum_{i,j=1}^{n}\left|\mathbb{P}\left[\boldsymbol{x}_{\mathbb{A},i}=\sigma,\ \boldsymbol{x}_{\mathbb{A},j}=\tau\mid\mathbb{A}\right]-q^{-2}\right| = o(n^2)\right\}, \qquad (1.3.11)$$

which implies asymptotic independence among entries in the kernel vectors. Then Chebyshev's inequality on $\mathfrak{O}$ w.h.p. shows [[27, Section 2.2]]

$$\sum_{i=1}^{n}\mathbb{1}\left\{\boldsymbol{d}_i=\ell,\boldsymbol{x}_{\mathbb{A},i}=\sigma\right\} = \mathbb{P}\left[\boldsymbol{d}=\ell\right]n/q+o(n) \qquad \text{for all } \sigma\in\mathbb{F}_q,\ \ell\in\operatorname{supp}\boldsymbol{d}.$$

This implies for every ℓ the only meaningful values to consider for optimizing (1.3.9) is the almost balanced vectors with the uniform distribution among $\mathbb{F}_q^*$ elements. Thus the following relations make sense, [27, Eq. 2.8], [27, Eq. 2.9],

$$\mathbb{E}_{\mathfrak{A}}\left[\boldsymbol{Z}\cdot\mathbb{1}\{\mathbb{A}\in\mathfrak{O}\}\right] \sim \mathbb{E}_{\mathfrak{A}}\left[\boldsymbol{Z}\right] \sim q^{n-\boldsymbol{m}} \qquad (1.3.12)$$

$$\mathbb{E}_{\mathfrak{A}}\left[\boldsymbol{Z}^2\cdot\mathbb{1}\{\mathbb{A}\in\mathfrak{O}\}\right] \sim \mathbb{E}_{\mathfrak{A}}\left[\boldsymbol{Z}\right]^2, \qquad (1.3.13)$$

Given that a key assumption for the main Theorem 3.4.1 is satisfied, we can show that (1.3.12), (1.3.13) are true w.h.p. Theorem (3.4.1) will turn out to be an easy consequence of (1.3.12)–(1.3.13), and two other theorems.

The task now is to prove (1.3.12) and (1.3.13). Regarding (1.3.12), the first asymptotic equality is where we use a quenched average and a matrix with few extra rows. The second asymptotic equality is as easy as in the random 3-XORSAT. As for (1.3.13), this is where we expand the second moment around the uniform solution. This expansion involves looking at the lattices generated by certain integer vectors that encode nearly equitable solutions. This method generalizes Huang's argument for the adjacency matrices of random d-regular graphs [48] and uses a local limit theorem to be introduced in Section 2.3.3. The basic strategy will be laid out in Section 3.4 and we refer the reader to [27] for detail.

2 Methods

2.1 Message Passing Algorithms - BP and WP

When faced with solving for a marginal distribution of a variable i among n particles which draw values from a finite space Ω, one might consider summing over all possible configurations. That would take $|\Omega|^n$ units of time. A message passing algorithm can be an efficient tool to reduce the time of computations when the graphical model fits certain nice features [60]. Imagine a factor graph G. A message passing is applied to messages on the edges which contain certain directed messages, from a variable to a factor and from a factor to a variable. Then a message passing algorithm updates these messages according to the neighboring messages. The update rule depends on the types of problems the algorithm works on and on the choice of algorithm. BP is the most well-known message passing algorithm. It computes marginal distributions exactly on tree factor graphs. But even more surprising, BP is successful in finding the right marginals on loopy graphs as well, as long as they have the appearance of a tree when viewed locally [60]. After we discuss BP further in 2.1.1, we also delve into discrete message passing algorithm such as UCP and *Warning Propagation* WP in 2.1.2.

2.1.1 BP

This section follows [60, Chapter 14] closely. As alluded in 1.1.2, we are after the free energy of a factor graph. BP paves the way to make this computation possible.

Let $G = (V, F, (\partial a)_{a\in F}, (\psi_a)_{a\in F})$ be a factor graph. For a configuration $\tau \in \Omega^{\partial a}$, let $\tau_x, x \in V$ denote the value on x given by τ. Let the message space $\mathscr{M}(G)$ be defined as the set of all families

$$\nu = (\nu_{x\to a}, \nu_{a\to x})_{x\in V, a\in F, x\in\partial a} \quad \text{with} \quad \nu_{x\to a}, \nu_{a\to x} \in \mathscr{P}(\Omega).$$

The *Belief Propagation operator*

$$\mathrm{BP} : \mathscr{M}(G) \to \mathscr{M}(G)$$

updates $\nu \in \mathscr{M}(G)$ with $\hat{\nu} \in \mathscr{M}(G)$ defined by

$$\hat{\nu}_{a\to x}(\sigma) = \frac{\sum_{\tau\in\Omega^{\partial a}} \mathbf{1}\{\{\}\tau_x = \sigma\}\psi_a(\tau)\prod_{y\in\partial a\setminus x}\nu_{y\to a}(\tau_y)}{\sum_{\tau\in\Omega^{\partial a}}\psi_a(\tau)\prod_{y\in\partial a\setminus x}\nu_{y\to a}(\tau_y)} \qquad \hat{\nu}_{x\to a}(\sigma) = \frac{\prod_{b\in\partial x\setminus a}\hat{\nu}_{b\to x}(\sigma)}{\sum_{\tau\in\Omega}\prod_{b\in\partial x\setminus a}\hat{\nu}_{b\to x}(\tau)}, \quad (2.1.1)$$

where $\sigma \in \Omega$. The idea of cavity ansatz is embedded in BP. The interpretation of $\hat{\nu}_{a\to x}(\sigma)$ is that it is the marginal distribution of x receiving σ in a graphical model where all the factors in ∂x except

a are deemed deleted. Analogously, $\hat{\nu}_{x\to a}(\sigma)$ is the marginal distribution of x sending σ in a graphical model where a is deemed deleted. BP recursively updates the messages so we can inductively define the messages after ℓ iterations. Let $\hat{\nu}^{(\ell)}_{a\to x}, \hat{\nu}^{(\ell)}_{x\to a}$ be the outputs of BP after ℓ iterations. Furthermore, for a point $\nu \in \mathscr{M}(G)$ and a variable node x and $\sigma \in \Omega$ we define the BP *marginal distribution estimates* after $\ell+1$ iterations.

$$\nu^{(\ell+1)}_x(\sigma) = \frac{\prod_{b\in\partial x}\hat{\nu}^{(\ell)}_{b\to x}(\sigma)}{\sum_{\tau\in\Omega}\prod_{b\in\partial x}\hat{\nu}^{(\ell)}_{b\to x}(\tau)}, \tag{2.1.2}$$

and similarly for a constraint node a,

$$\nu^{(\ell+1)}_a(\sigma) = \frac{\psi_a(\sigma)\prod_{y\in\partial a}\hat{\nu}^{(\ell)}_{y\to a}(\sigma_y)}{\sum_{\tau\in\Omega^{\partial a}}\psi_a(\tau)\prod_{y\in\partial a}\hat{\nu}^{(\ell)}_{y\to a}(\tau_y)} \qquad (\sigma\in\Omega^{\partial a}). \tag{2.1.3}$$

Helpful expositions on BP can be found in [60, 88]. With these terms, we can write down the estimate of the free energy in (1.1.6) which is the logarithm of the partition function, called the *Bethe Free Energy*.

Bethe Free Energy

The estimate of free energy $\log Z(G)$ from (1.1.6) after $\ell-1$ iterations is given by

$$\mathscr{B}_\ell(\nu) = \sum_{x\in V} H(\nu^{(\ell)}_x) - \sum_{a\in F}\left[D_{\mathrm{KL}}\left(\nu^{(\ell)}_a \| \otimes_{x\in\partial a}\nu^{(\ell)}_x\right) - \langle \ln\psi_a, \nu^{(\ell)}_a\rangle\right] \tag{2.1.4}$$

We call this functional *Bethe free energy* [16]. In acyclic graphs or graphs with no long correlation, BP gets unique fixed points, ν_x, ν_a which match the correct marginal distributions of the system, $(\mu_x)_{x\in V}, (\mu_{\partial a})_{a\in F}$ respectively [60]. Then the Bethe free energy evaluated at the fixed points correctly estimates the free energy

$$\log Z(G) = \mathscr{B}(\nu) = \sum_{x\in V} H(\nu_x) - \sum_{a\in F}\left[D_{\mathrm{KL}}(\nu_a \| \otimes_{x\in\partial a}\nu_x) - \langle \ln\psi_a, \nu_a\rangle\right] \tag{2.1.5}$$

This is one of the main ideas used in [3] to calculate the free energy of the random 2-SAT model. The idea of a unique fixed point will be discussed in detail in Section 3.1. We can express the Bethe free energy in an alternative way as well. We define

$$\begin{aligned}
&\mathscr{B}(\mu) = \sum_{a\in F} F_a + \sum_{x\in V} F_x - \sum_{x\in V, a\in\partial x} F_{a,x}, \quad \text{where} \\
&F_a = \log \sum_{\tau\in\Omega^{\partial a}} \psi_a(\tau) \prod_{x\in\partial a} \mu_{x\to a}(\sigma_x), \quad F_x = \log \sum_{\sigma\in\Omega} \prod_{b\in\partial x} \mu_{b\to x}(\sigma), \quad F_{a,x} = \log \sum_{\sigma\in\Omega} \mu_{x\to a}(\sigma)\mu_{a\to x}(\sigma)
\end{aligned} \tag{2.1.6}$$

where $\sum_{a\in F} F_a$ stands for the entropy on the factors and $\sum_{x\in V} F_x$, the entropy on the variables and $\sum_{x\in V, a\in\partial x} F_{a,x}$ for the interaction between the variables and the factors. A detailed derivation of Bethe free energy equation can be found in [60, Chapter 14], [89].

2.1.2 WP

Now we turn to a message passing algorithm of discrete nature. Whereas BP updates the probability distributions on the directed messages, WP updates the messages themselves in reaction to their neighbors' messages. Suppose we have an instance of a rCSP, Φ and let G_Φ denote its factor graph. On each edge, there are directed messages, $\mu_{x\to a}$ and $\mu_{a\to x}$. If we initialize each message to be Boolean and run WP, then WP updates the messages to either 0 or 1 according to the following warnings [60, Section 14.3.3]. Here σ is Boolean.

- $\mu_{x\to a}(\sigma) = 1$ means *according to the demand of the constraints $b \in \partial x \setminus a$, x should not take the value σ.*
- $\mu_{x\to a}(\sigma) = 0$ means *according to the demand of the constraints $b \in \partial x \setminus a$, x can take the value σ.*

Therefore, WP makes direct implications for the messages. However, the messages are not required to be Boolean nor the number of types of the vertices is limited to 2. Here we define WP in full generality. This portion follows [[32, Section 1.3]] closely.

Given a graph G, let $\mu_{v\to w}, \mu_{w\to v}, vw \in E(G)$ be the messages drawn from a finite set Ω. We define $\mathscr{M}(G)$ to be the set of all vectors $\left(\mu_{v\to w}\right)_{(v,w)\in V(G)^2 : vw\in E(G)} \in \Omega^{2|E(G)|}$ where $V(G)$ is the set of all vertices of all types involved. To define the update function for the messages, for $d \in \mathbb{N}$ let $\left(\!\binom{\Omega}{d}\!\right)$ be the set of all d-ary multisets with elements from Ω and let [[32, Eq. 1.1]]

$$\varphi : \bigcup_{d\geq 0} \left(\!\binom{\Omega}{d}\!\right) \to \Omega \tag{2.1.7}$$

be an *update rule* that, given any multiset of input messages, determines an output message. In other words, we define the WP operator on G by

$$\mathrm{WP}_G : \mathscr{M}(G) \to \mathscr{M}(G), \qquad \mu = \left(\mu_{v\to w}\right)_{vw} \mapsto \left(\varphi\left(\{\!\{\mu_{u\to v} : u \in \partial v \setminus w\}\!\}\right)\right)_{vw},$$

where $\{\!\{a_1, \ldots, a_r\}\!\}$ denotes the multiset with $a_1, \ldots, a_r \in \Omega$. Thus to update a directed message, WP ignores the target while reacting to all other neighbors in a similar way to BP in 2.1.1.

Let us discuss two examples of WP. Consider UCP on a rCSP. Any clause with one variable in its neighbor is called a unit clause. Starting on any unit clause, one can set the value on the literal so that it satisfies the unit clause. Those other clauses in which the variable appears with the same sign are now also satisfied so the propagation effect stops but the clauses with the opposite sign will carry the effect further. Eventually this process would stop, either with an empty set or with clauses that contain at least two variables. Unit Propagation was successfully used to get results on k-SAT problems [1, 45].

There is also the peeling process for the *k-core*. It starts on vertices of degree less than k and delete them along with the connecting edges. One such round might expose more vertices with less than k. The process continues until a subgraph with all vertices with k or more neighbors, the k-core which might be empty (See e.g. [73, 64]).

WP is a general model of such discrete message passing algorithms that recursively update the messages along the edges. As we have seen in the two examples, the update rule, the types of messages and the types of vertices are determined according to the particular problems WP deals with.

There have been many different approaches to analyzing such recursive processes. One classical tool is the differential equations method [86], where the asymptotic number of vertices of varying degrees is the main function of time. Pittel, Spencer and Wormald used this method to discover results regarding $k-$core in [73]. More results on k-core followed using branching processes [77], enumerative methods [25], or birth-death processes [50, 51].

Similarly as in BP, for WP to be useful, it would be helpful if the recursive process converges to a fixed point quickly after a bounded number of recursions. Moreover, even after reaching the fixed point, in case of any change in messages, there should not be global changes in response to that. The main results of [32] exactly accomplish these goals in studying various models such as ER binomial random graph model $G(n,p)$, $k-$partite graphs, random regular graphs, random graphs with a particular degree sequence, the stochastic block model, and factor graphs of random hypergraphs. Indeed, we show that for any specific recursive processes which can be fitted in the forms of Theorem 3.2.9 we only need to study the recursion on a multi-type Galton-Watson tree that resembles the local structure of the respective model. We mention that this work was inspired by our need to understand a recursive process in the context of CRM to be discussed in Section 3.3.

Our goal is to study the fixed points of WP and in particular the rate of convergence on the random graph $\mathbb{G}$ of various models with k types of vertices. A crucial premise on $\mathbb{G}$ is that locally it has the structure of a multi-type Galton-Watson tree. Under mild assumptions on φ, we prove that this local structure completely characterizes the WP fixed point. The recursive nature of the Galton-Watson tree ascertains that our fixed point will just be a collection of probability distributions on Ω of each type of directed edge so that if the children of a vertex v send messages to v independently according to these distributions, then the message from v to its parent would also reflect the same distributions of messages of each type. The distributions of messages between vertices of k types can be efficiently expressed as a matrix. For a matrix M and $i,j\in[k]$ types of vertices, we denote by $M[i,j]$ the ij entry in the matrix and by $M[i]$ the i-th row $\left(M[i,j]\right)_{j\in[k]}$.

Given a finite set Ω, a *probability distribution matrix* on Ω is a $k\times k$ matrix Q in which each entry $Q[i,j]$ of Q is a probability distribution on Ω. In other words, $Q[i,j]$ denotes the probability distribution on directed messages from a type i to a type j drawn from Ω such that $\sum_{j\in[k]}Q[i,j]=1$. We initialize the messages independently.

Definition 2.1.1 ([32, Definition 1.2])**.** *For a graph G and a probability distribution matrix Q on Ω, we refer to* initialising messages in G according to Q *to mean that we initialise the message $\mu_{u\to v}(0)$ for each directed edge (u,v) independently at random according to $Q[i,j]$, where i and j are the types of u and v respectively.*

Upon initializing the messages independently, we update the distribution according to WP rule and

the current distribution. More precisely, for a directed edge vw of type (i,j), we consider the messages from the other neighbors of v according to the current probability distribution on each pair of types. This process generates an updated probability distribution for messages between i and j types. Repeating this for all $i,j \in [k]$ gives the updated matrix. In addition, it now makes sense to consider the limit of updating process. We need Q to converge to a matrix with respect to a metric of our choice. This process is described more formally in [32, Section 2.1]. We shall pick up on this point in Section 3.2 when we discuss the main result of [32].

2.2 Rank and Intuition from Physics

2.2.1 Overlap and Replica Symmetry

When a vector $\boldsymbol{y}$ is randomly drawn from the column space of $\boldsymbol{A} \in [0,1]_{m\times n}$, solving the random linear system $\boldsymbol{A}x = \boldsymbol{y}$ is a rCSP. Recall that a random k-XORSAT is a random linear system over $\mathbb{F}_2$ where every row contains k ones. We can also look at this problem from $\boldsymbol{x}$'s point of view. Let $\hat{\boldsymbol{x}} \in \mathbb{F}_2^n$ denote a random vector (ground truth) and $\boldsymbol{y}$ be the noisy observation of $\hat{\boldsymbol{x}}$ via $\boldsymbol{y} = \boldsymbol{A}\hat{\boldsymbol{x}}$. An *inference problem* asks how well one can recover $\hat{\boldsymbol{x}}$ given $\boldsymbol{A}$ and $\boldsymbol{y}$. Here we see the connection between rCSP and inference problem since the posterior distribution of a random fixed vector x matching the ground truth is the uniform distribution among the vectors x that solve the linear system [24, Eq. 1.3]

$$\mathbb{P}\left[\hat{\boldsymbol{x}} = x \mid \boldsymbol{A}, \boldsymbol{y}\right] = \frac{\mathbb{1}\{\boldsymbol{A}x = \boldsymbol{y}\}}{|\ker \boldsymbol{A}|}, \qquad (x \in \mathbb{F}_2^n). \tag{2.2.1}$$

We can also think about what fraction of variables in $\hat{\boldsymbol{x}}$ we can match with a random vector x. This is the idea of the *overlap*.

Definition 2.2.1 ([24, Section 1.3])**.** *[Overlap]*

$$R(\boldsymbol{x}, \hat{\boldsymbol{x}}) = \frac{1}{n}\sum_{i=1}^{n} \mathbb{1}\{\boldsymbol{x}_i = \hat{\boldsymbol{x}}_i\}.$$

We are also interested in the overlap given $\boldsymbol{A}, \boldsymbol{y}$. The average of $R(\boldsymbol{x}, \hat{\boldsymbol{x}})$ given $\boldsymbol{A}, \boldsymbol{y}$ is a value independent of $\boldsymbol{y}$ given by

$$\bar{R}(\boldsymbol{A}) = \mathbb{E}\left[R(\boldsymbol{x}, \hat{\boldsymbol{x}}) \mid \boldsymbol{A}, \boldsymbol{y}\right] = \frac{1}{|\ker \boldsymbol{A}|^2} \sum_{x, x' \in \ker \boldsymbol{A}} R(x, x').$$

We discussed previously the idea of replica symmetry in terms of geometry of solution space where two independently drawn solutions belong to one cluster. Another way to express the idea of replica symmetry involves the overlap. We say the linear system is replica symmetric when the overlap converges to a single value, given the disorder which in this case being $\boldsymbol{A}, \boldsymbol{y}$ [90],

$$\lim_{n\to\infty} \mathbb{E}\left[\left|R(\boldsymbol{x}, \hat{\boldsymbol{x}}) - \bar{R}(\boldsymbol{A})\right|\right] \to 0.$$

Surprisingly perhaps, most of studies in inference problems show that the overlap converges to a deterministic value, independent of the given condition $\boldsymbol{A}, \boldsymbol{y}$ [13]. We call this phenomenon *Strong Replica Symmetry* and express it as

$$\lim_{n\to\infty} \mathbb{E}\left[\left|R(\boldsymbol{x},\hat{\boldsymbol{x}}) - \mathbb{E}\left[\bar{R}(\boldsymbol{A})\right]\right|\right] \to 0.$$

The object of study in [24] is a square matrix with each entry having a Bernoulli distribution with $p = d/n, d > 0$. This matrix $\boldsymbol{A}$ belongs to the rare case where the fraction of frozen variables $f(\boldsymbol{A})$ and the conditional overlap $\bar{R}(\boldsymbol{A})$ are both strongly replica symmetric when $0 < d <$ e but only replica symmetric when $d >$ e.

We will state these main results in the section 3.3 and lay out the proof strategy.

2.3 Algebraic Detour, Local Limit Theorem

2.3.1 Short linear relations

Let the *support* of a vector $\xi \in \mathbb{F}^U$ be defined as $\mathrm{supp}(\xi) = \{i \in U : \xi_i \neq 0\}$.

Definition 2.3.1 ([26, Definition 2.1])**.** *Let A be an $m \times n$ matrix over a field $\mathbb{F}$.*

- *A set $\emptyset \neq I \subseteq [n]$ is a* relation *of A if there exists a row vector $y \in \mathbb{F}^{1\times m}$ such that $\emptyset \neq \mathrm{supp}(yA) \subseteq I$.*
- *If $I = \{i\}$ is a relation of A, then we call i* frozen *in A. Let $\mathfrak{F}(A)$ be the set of all frozen $i \in [n]$.*
- *A set $I \subseteq [n]$ is a* proper relation *of A if $I \backslash \mathfrak{F}(A)$ is a relation of A.*
- *For $\delta > 0, \ell \geq 1$ we say that A is $(\delta,\ell)-$*free *if there are no more than δn^ℓ proper relations $I \subseteq [n]$ of size $|I| = \ell$.*

In other words, a relation is a subset of column indices in which the support of non-zero linear combinations yA is contained for some row vector y of A. We note that every row of A induces a relation on the column indices where it has non-zero values. We are particularly interested in the singleton relation for we know if $I = \{i\}$ is a relation, then $x_i = 0$ for all $x \in \ker A$. Note that this is the same definition as in (1.3.1). A proper relation is a relation composed of at least one non-frozen relation. Lastly, we aim to use bounded ℓ and small $\delta > 0$. We say A is $(\delta,\ell)-$*free* when A has relatively few relations. The following observation will aid the Aizenman-Sims-Starr coupling argument, in which we study the effect of adding a few extra rows and columns to a random matrix. The Aizenman-Sims-Starr argument is discussed in Section 2.3.2.

The Pinning Operation

We use this notion of $(\delta,\ell)-$*free* to perform an operation called *pinning* with a view of having a good control of the nullity of A as we attach one more variable along with bounded number of checks in keeping with the original distribution of A. Probing the change of nullity as we introduce extra bits to A entails the so-called *Aizenman-Sims-Starr* scheme which was inspired by the *cavity method* [8,

61]. First we define the pinning operation. The point of pinning operation is that we can reduce the number of short relations by freezing a few random variables [10, 28, 31, 74].

Let A be an $m \times n$ matrix and let $\eta \geq 0$ be an integer. Let $\boldsymbol{i}_1, \boldsymbol{i}_2, \dots, \boldsymbol{i}_\eta \in [n]$ be uniformly random and mutually independent column indices. Then we define $A[\eta]$ as A with η new rows so that for each $j \in [\eta]$ the j-th new row has precisely one non-zero entry, namely 1 in the $\boldsymbol{i}_j$-th column, thereby pinning variables at $\boldsymbol{i}_1, \boldsymbol{i}_2, \dots, \boldsymbol{i}_\eta$ to the frozen state [26, Definition 2.3]. Pinning enables a $(\delta, \ell) - \textit{free}$ event to be likely as the following proposition shows.

Proposition 2.3.2 ([26, Proposition 2.3])**.** *For any $\delta > 0, \ell > 0$ there exists $\mathcal{T} = \mathcal{T}(\delta, \ell) > 0$ such that that for any matrix A over any field $\mathbb{F}$ the following is true. With $\boldsymbol{\eta} \in [\mathcal{T}]$ chosen uniformly at random we have*

$$\mathbb{P}\left[A[\boldsymbol{\eta}] \textit{ is } (\delta, \ell) - \textit{free}\right] > 1 - \delta.$$

Proposition 2.3.2 produces a very useful application. Namely, if pinning operation to a random matrix over a finite field leaves a few frozen variables, then a de-correlation condition similar to $\mathfrak{O}$ from (1.3.11) will be achieved, effectively making the system replica symmetric. Let $\boldsymbol{x}_A$ denote a random vector in $\ker A$.

Corollary 2.3.3 ([26, Lemma 4.2])**.** *For any $\zeta > 0$ and any prime power $q > 0$ there exist $\xi > 0$ and $\Theta_0 > 0$ such that for any $\Theta > \Theta_0$ for large enough n the following is true. Let A be a $m \times n$-matrix over $\mathbb{F}_q$. Suppose that for a uniformly random $\boldsymbol{\theta} \in [\Theta]$ we have $\mathbb{E}|\mathfrak{F}(A[\boldsymbol{\theta}])| < \xi n$. Then*

$$\sum_{\sigma,\tau \in \mathbb{F}_q} \sum_{i,j=1}^{n} \mathbb{E}\left|\mathbb{P}\left[\boldsymbol{x}_i = \sigma, \boldsymbol{x}_j = \tau \mid A[\boldsymbol{\theta}]\right] - q^{-2}\right| < \zeta n^2.$$

The pinning operation was used in three of our papers [3, 24, 27] and will be be discussed further in Chapter 3.

2.3.2 Aizenman Sims Starr

The Aizenman-Sims-Starr scheme embodies the essence of the cavity method [8]. The cavity method works like induction [78]. To measure the change of the system or a certain value of interest as n increases, the cavity method considers the system with a cavity, one less variable to gauge the actions of the rest, just as we have seen in BP and WP. We can think of the Aizenman-Sims-Starr scheme as going one step further and accommodating the ensuing change in order to keep the distribution of the system equivalent as before. We will present this scheme as it is applied to the nullity of the matrix $\boldsymbol{A}_n$ from [26] due its simpler form than the one in [27]. The key difference between [26] and our second paper on rank [27] is that for arbitrary $\varepsilon, \delta > 0$ and for an integer $\Theta(\varepsilon)$, in addition to pinning $\boldsymbol{\theta}$ many variable as in [26], we also add $\mathrm{Po}(\delta n)$ ternary equations (rows), each of which involves three variables chosen uniformly at random. We refer the reader to [27, Section 8] for a detailed proof on the upper bound of the nullity.

Recall the distributions of non-zero entries in rows and columns of the random matrix presented in Section 1.3.2. In order to derive the desired upper bound on the nullity we write a telescoping sum [26, Eqs. 2.5, 2.6],

$$\limsup_{n\to\infty}\frac{1}{n}\mathbb{E}\left[\mathrm{nul}(\boldsymbol{A}_n)\right]=\limsup_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N-1}\mathbb{E}\left[\mathrm{nul}(\boldsymbol{A}_{n+1})\right]-\mathbb{E}\left[\mathrm{nul}(\boldsymbol{A}_n)\right]\le\limsup_{n\to\infty}\mathbb{E}\left[\mathrm{nul}(\boldsymbol{A}_{n+1})\right]-\mathbb{E}\left[\mathrm{nul}(\boldsymbol{A}_n)\right].$$

Then we should attempt to couple $\boldsymbol{A}_{n+1}$ and $\boldsymbol{A}_n$ such that we can write a single expectation [[26, Eq. 2.7]]

$$\mathbb{E}\left[\mathrm{nul}(\boldsymbol{A}_{n+1})\right]-\mathbb{E}\left[\mathrm{nul}(\boldsymbol{A}_n)\right]=\mathbb{E}\left[\mathrm{nul}(\boldsymbol{A}_{n+1})-\mathrm{nul}(\boldsymbol{A}_n)\right] \tag{2.3.1}$$

Here we follow the argument in [26, Section 2]. We want to calculate $\mathbb{E}[X_n]$ as $n\to\infty$. Then we can think about summing the differences as n increases. In other words, we calculate $\mathbb{E}[X_{n+1}]-\mathbb{E}[X_n]$ and make a telescoping sum up to $n+1$. In doing so, we would like to couple X_n and X_{n+1} such that X_{n+1} results from X_n by adding a bounded number of elements [26, Section 2]. Authors of [26] applied this approach to $X_n=\mathrm{nul}\,\boldsymbol{A}_n$. We observe that Aizenman-Sims-Starr was also used in our 2-SAT paper when it was applied to the free energy density $\frac{1}{n}\log Z_n$ [3].

The coupling will be such that X_{n+1} is the nullity of a random matrix made from $\boldsymbol{A}_n$ by adding a few rows and columns. We need to calculate the change in nullity upon the addition. The new rows will take some non-zero elements. Depending on the locations of the non-zero elements, their linear dependence and the fraction of frozen variables, we might face a big drop in nullity. However, the random locations of the non-zero elements and the pinning operation save the day to show that the linear dependencies among the non-zero entries of the new rows turn out to be negligible (See Lemma 2.3.3).

In both [3] and [27], one side of the inequality is already given by previous works of others. Regarding the result in [27] , the lower bound on nul A is already given in [21, 55, 26]. As for [3], the upper bound on the free energy $\frac{1}{n}\log Z_G$ by interpolation method in [44, 71].

Half-edges and Configuration Model

This section follows the argument in [26, Section 2.2]. To couple $\mathrm{nul}(\boldsymbol{A}_{n+1})-\mathrm{nul}(\boldsymbol{A}_n)$ requires more than adding one column and few rows according to the current distributions because that alone cannot guarantee the same distributions. For one, the condition $\boldsymbol{m}=\mathrm{Po}(dn/k)$ might mean that A_{n+1} cannot even exist with the current distributions. To overcome this issue, we come up with a *contiguous* model that is more manageable to control. First let $G=G(V,F)$ denote the graphical model of $\boldsymbol{A}_n$ with V taking the role of the columns while F being the rows. Now we choose $\varepsilon>0$ as small as we like and choose a large number $\mathscr{T}=\mathscr{T}(\varepsilon)$. Then for any $n\ge\mathscr{T}$, we make $\boldsymbol{A}_{\varepsilon,n}$ as follows. Let $\boldsymbol{m}_{\varepsilon,n}=\mathrm{Po}((1-\varepsilon)dn/k)$ be the number of rows for $\boldsymbol{A}_{\varepsilon,n}$. Next we choose $\theta\in[\mathscr{T}]$ uniformly at random. Recall the definitions of the random variables for the degrees of each row and column $(\boldsymbol{d}_i)_{i\in[n]},(\boldsymbol{k}_j)_{j\in[\boldsymbol{m}]}$, all copies of $\boldsymbol{d},\boldsymbol{k}$ respectively. Instead of starting with a connected graph G, we look at each vertex with its degree as one node with *half-edges* attached to it. For instance, let $x_i\in V$ and $d_i=|\partial x_i|$. Then we make d_i many *clones* of x_i and we do that for every vertex. That gives us two

vertex classes

$$\cup_{i=1}^{\boldsymbol{m}_{\varepsilon,n}}\{a_i\}\times[\boldsymbol{k}_i] \text{ and } \cup_{j=1}^{n}\{x_j\}\times[\boldsymbol{d}_j].$$

Finally we let $\boldsymbol{\Gamma}_{\varepsilon,n}$ denote an uniformly and randomly chosen maximal matching of the complete bipartite graph between two vertex classes of half-edges. This is a well-known model of random graphs called the *configuration model*, first devised by Bollobás and effectively used by Molloy, Reed, and Wormald [18, 65, 87]. On top of $\boldsymbol{\Gamma}_{\varepsilon,n}$ we place additional checks $p_i, i\in[\theta]$ connected with a randomly chosen variable clone. However, because we are missing about $\varepsilon dn/k$ rows, we expect about εdn variable clones not being matched. These are called *cavities*. it is this cavity that creates wiggle room to make auxiliary models. In [27], we show that a similar matrix to $\boldsymbol{A}_{\varepsilon,n}$ resembles $\boldsymbol{A}_n$. Additionally, $p_i, i\in[\theta]$ freeze the connected variables in order to make Corollary 2.3.3 work. Finally, on the back of the contiguity result, we carry out the expectation in (2.3.1) by using this auxiliary matrix along with two other auxiliaries. We refer the reader to [27, Section 8] for detail.

2.3.3 Local Limit Theorem

Here we briefly discuss a variant of Central Limit Theorem called Local Limit Theorem (LLT). To keep it light we will write down a version for sums of independent random variables mirroring the lecture note [80].

Let $X_1, X_2, \ldots$ be i.i.d. copies of an integer random variable X with mean μ and variance σ^2. Let $S_n = X_1 + X_2 + \cdots + X_n$. Suppose there is no arithmetic progression of the form $a + q\mathbb{Z}$ with $q > 1$ for which $X \equiv a \bmod q$ almost surely. Then we have $\mathbb{P}[S_n = m] = \frac{1}{\sqrt{2\pi n\sigma}}\mathrm{e}^{-(m-n\mu)^2/2n\sigma^2} + o(1/n^{1/2})$ for all $n \geq 1$ and all integers m. Thus, whether X belongs to a sub-lattice or not is an important criteria in using LLT. Later when we discuss LLT in Section 3.4, the main question boils down to whether a *balanced* vector belongs to a sub-lattice or whether a uniform vector belongs to the full integer lattice, as alluded in Section 1.3.2. A key Claim 3.4.13 is a case in point. A vector version of LLT is presented in [35]. This version requires a special assumption about increments of vectors being realized in every direction of the dimension. This assumption cannot be established in our key Claim 3.4.13. We will pick up on this topic as we discuss the results of [27]. We refer the reader to [[27, Appendix]] for the proof of Claim 3.4.13.

3 Results

3.1 The Number of Satisfying Assignments of Random 2-SAT Formulas

In addition to the set up in Section1.2.3, few more premises are necessary in order to state the main result. Let $\mathscr{P}(0,1)$ be the set of all Borel probability measures on $(0,1)$, endowed with the weak topology. We define an operator $\mathrm{BP}_d : \mathscr{P}(0,1) \to \mathscr{P}(0,1)$, $\pi \mapsto \hat{\pi}$ as follows.

Let $\boldsymbol{d}^+, \boldsymbol{d}^- = \mathrm{Po}(d/2)$ stand for the number of 'true' and 'false' messages respectively from the variable's neighbors. Furthermore, let $\boldsymbol{\mu}_{\pi,1}, \boldsymbol{\mu}_{\pi,2}, \ldots$ denote random variables with distribution π, all mutually independent and let $\hat{\pi}$ be the distribution of the random variable [3, Eq. 1.1]

$$\frac{\prod_{i=1}^{\boldsymbol{d}^-} \boldsymbol{\mu}_{\pi,i}}{\prod_{i=1}^{\boldsymbol{d}^-} \boldsymbol{\mu}_{\pi,i} + \prod_{i=1}^{\boldsymbol{d}^+} \boldsymbol{\mu}_{\pi,i+\boldsymbol{d}^-}} \in (0,1). \tag{3.1.1}$$

Notice that this equation takes a similar form as in (2.1.2) and (2.1.3). Let $\delta_{1/2} \in \mathscr{P}(0,1)$ mean the atom at $1/2$ and write $\mathrm{BP}_d^\ell(\cdot)$ for the ℓ-fold recursion of the operator BP_d.

Theorem 3.1.1 ([3, Theorem 1.1]). *For any $d < 2$ the limit $\pi_d = \lim_{\ell\to\infty} \mathrm{BP}_d^\ell(\delta_{1/2})$ exists and*

$$\lim_{n\to\infty} \frac{1}{n} \log Z(\boldsymbol{\Phi}) = \mathbb{E}\left[\log\left(\prod_{i=1}^{\boldsymbol{d}^-} \boldsymbol{\mu}_{\pi_d,i} + \prod_{i=1}^{\boldsymbol{d}^+} \boldsymbol{\mu}_{\pi_d,i+\boldsymbol{d}^-}\right) - \frac{d}{2}\log\left(1 - \boldsymbol{\mu}_{\pi_d,1}\boldsymbol{\mu}_{\pi_d,2}\right)\right] \quad \textit{in probability.} \tag{3.1.2}$$

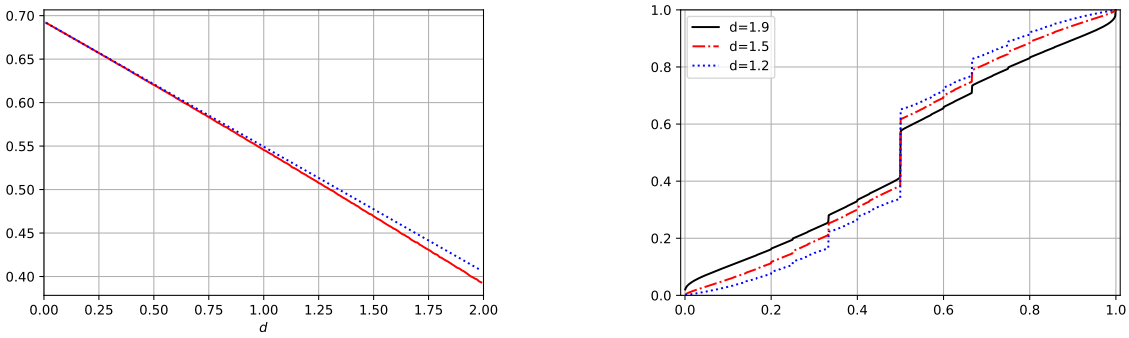

FIGURE 3.1: [3, Figure 1]. *Left:* the red line depicts a numerical approximation to the r.h.s. of (3.1.2) after 24 iterations of $\mathrm{BP}_d(\cdot)$. The dotted blue line displays the first moment bound. *Right:* the cumulative density functions of numerical approximations to $\mathrm{BP}_d^{24}(\delta_{1/2})$ for various d.

By the definition of π_d, it is a solution to the stochastic fixed point equation [3, Eq. 1.3]

$$\pi_d = \mathrm{BP}_d(\pi_d). \tag{3.1.3}$$

The equation (3.1.3) is known as the *density evolution* equation in physics, while the expression on the r.h.s. of (3.1.2) is the *Bethe free entropy* introduced in (2.1.6) [60]. Theorem 3.1.1 confirms the conjecture from [66] that the free energy density is equal to the Bethe free entropy evaluated at the fixed point of (3.1.1). The proof shows that the fixed point iteration $\mathrm{BP}_d^{\ell}(\delta_{1/2})$ converges in some metric as Figure 3.1 illustrates.

3.1.1 Applying BP on 2-SAT

As discussed in section 2.1.1, BP is a message passing algorithm with the goal of approximating the marginal probability that in the setting of 2-SAT a specific variable takes the value 'true' under a random satisfying assignment. Notice that in 2-SAT, $\Omega = \{\text{true}, \text{false}\} = \{+1, -1\}$. Finding satisfying assignments of a given 2-SAT formula can be done by a typical SAT solver algorithm but narrowing down these marginals is not trivial. In fact, the problem is #P-hard [81]. In this paper we show that BP recovers the marginals well on a random formula w.h.p. Recall the setup done in Section 2.1.1. Given a 2-SAT formula $\Phi = \Phi(n, m)$, we associate a bipartite graph $G(\Phi)$. The variable set $V = V(\Phi) = \{x_1, \ldots, x_n\}$ and the clause set $F = F(\Phi) = \{a_1, \ldots, a_m\}$ are as before, with each clause node a_i having two variable nodes as its neighbors. Moreover, for a vertex v, let $\partial^{\ell} v$ for $\ell \geq 1$ denote the set of all vertices at distance precisely ℓ from v. We also define $\nabla^{\ell}(\Phi, v)$ to be the sub-formula from Φ by deleting all the clauses and variables at distance greater than ℓ from v. This sub-formula may contain clauses of length less than two depending on whether $v \in V$ or $v \in F$ and ℓ is even or odd. Furthermore, for a clause a and a variable x of Φ we let $\mathrm{sign}(x, a) = \mathrm{sign}_{\Phi}(x, a) \in \{\pm 1\}$ be the sign with which x appears in a.

We initialize all messages by [3, Eq. 1.5]

$$\nu^{(0)}_{\mathbf{\Phi}, a \to x}(\pm 1) = \nu^{(0)}_{\mathbf{\Phi}, x \to a}(\pm 1) = 1/2 \tag{3.1.4}$$

and for $\ell \geq 1$ the messages $\nu^{(\ell)}_{\mathbf{\Phi}, a \to x}, \nu^{(\ell)}_{\mathbf{\Phi}, x \to a}$ are defined inductively as ℓ-fold operations of (3.1.1). Let us write down BP update functions (2.1.2), (2.1.3) in the case of 2-SAT in detail. Let $a \in F$ and $\partial a = \{x, y\}$ and let $r, s \in \{\pm 1\}$ indicate whether x, y appear as positive or negative literals in a. Then for $t = \pm 1$ (2.1.2), (2.1.3) take the following forms [3, Eq. 1.6]

$$\nu^{(\ell)}_{\mathbf{\Phi}, a \to x}(t) = \frac{1 - \mathbb{1}\{r \neq t\}\, \nu^{(\ell-1)}_{\mathbf{\Phi}, y \to a}(-s)}{1 + \nu^{(\ell-1)}_{\mathbf{\Phi}, y \to a}(s)}, \qquad \nu^{(\ell)}_{\mathbf{\Phi}, x \to a}(t) = \frac{\prod_{b \in \partial x \setminus \{a\}} \nu^{(\ell)}_{\mathbf{\Phi}, b \to x}(t)}{\prod_{b \in \partial x \setminus \{a\}} \nu^{(\ell)}_{\mathbf{\Phi}, b \to x}(1) + \prod_{b \in \partial x \setminus \{a\}} \nu^{(\ell)}_{\mathbf{\Phi}, b \to x}(-1)}. \tag{3.1.5}$$

Furthermore, let the Belief Propagation estimate of the marginal of a variable x after ℓ iterations reads [3, Eq. 1.7]

$$\nu^{(\ell)}_{\mathbf{\Phi},x}(t) = \frac{\prod_{a\in\partial x}\nu^{(\ell)}_{\mathbf{\Phi},a\to x}(t)}{\prod_{a\in\partial x}\nu^{(\ell)}_{\mathbf{\Phi},a\to x}(1)+\prod_{a\in\partial x}\nu^{(\ell)}_{\mathbf{\Phi},a\to x}(-1)}. \tag{3.1.6}$$

Let $S(\mathbf{\Phi})$ be the set of all satisfying assignments of $\mathbf{\Phi}$ and let $\mu_{\mathbf{\Phi}}(\sigma)$ denote the uniform distribution on $S(\mathbf{\Phi})$. Additionally, let $\boldsymbol{\sigma}_\Phi = (\boldsymbol{\sigma}_{\Phi,x})_{x\in V(\Phi)}$ mean a uniformly random configuration from $S(\mathbf{\Phi})$. For $\tau_{\mathbf{\Phi}}$ and $\ell \geq 1$ the conditional distribution $\mu_{\mathbf{\Phi}}(\cdot \mid \boldsymbol{\sigma}_{\partial^{2\ell}x_1} = \tau_{\partial^{2\ell}x_1}) = \mu_{\mathbf{\Phi}}(\cdot \mid \forall y \in \partial^{2\ell}x_1 : \boldsymbol{\sigma}_y = \tau_y)$ means all configurations with the values of the leaves at 2ℓ distance from x being determined by τ. We can show that BP withstands any boundary conditions such that it approximates the conditional marginals as well as unconditional ones as the following theorem states.

Theorem 3.1.2 ([3, Theorem 1.2])**.** *If $d < 2$, then*

$$\lim_{\ell\to\infty}\limsup_{n\to\infty}\mathbb{E}\left[\max_{\tau\in S(\mathbf{\Phi})}\left|\mu_{\mathbf{\Phi}}(\boldsymbol{\sigma}_{x_1}=1 \mid \boldsymbol{\sigma}_{\partial^{2\ell}x_1}=\tau_{\partial^{2\ell}x_1}) - \nu^{(\ell)}_{\mathbf{\Phi},x_1}(1)\right| \mid Z(\mathbf{\Phi})>0\right] = 0. \tag{3.1.7}$$

Since $\nu^{(\ell)}_{\mathbf{\Phi},x_1}$ does not depend on τ, averaging (3.1.7) on the boundary condition $\tau \in S(\mathbf{\Phi})$ yields [3, Eq. 1.10]

$$\lim_{\ell\to\infty}\limsup_{n\to\infty}\mathbb{E}\left[\left|\mu_{\mathbf{\Phi}}(\boldsymbol{\sigma}_{x_1}=\pm 1) - \nu^{(\ell)}_{\mathbf{\Phi},x_1}(\pm 1)\right| \mid Z(\mathbf{\Phi})>0\right] = 0. \tag{3.1.8}$$

Since the distribution of $\mathbf{\Phi}$ is invariant under permutations of the variables $x_1,\dots,x_n$, (3.1.8) it is implied that the marginals of all but $o(n)$ variables x_i are within $\pm o(1)$ of BP approximation w.h.p. .

We apply the triangle inequality to (3.1.7) and (3.1.8) to see [3, Eq. 1.11]

$$\lim_{\ell\to\infty}\limsup_{n\to\infty}\mathbb{E}\left[\max_{\tau\in S(\mathbf{\Phi})}\left|\mu_{\mathbf{\Phi}}(\boldsymbol{\sigma}_{x_1}=1 \mid \boldsymbol{\sigma}_{\partial^{2\ell}x_1}=\tau_{\partial^{2\ell}x_1}) - \mu_{\mathbf{\Phi}}(\boldsymbol{\sigma}_{x_1}=1)\right| \mid Z(\mathbf{\Phi})>0\right] = 0. \tag{3.1.9}$$

This means that any boundary condition will be forgotten in the marginal of x_1 as $\ell, n \to \infty$. This spatial mixing property is known as *Gibbs uniqueness* [53].

Furthermore, (3.1.9) nullifies the issue of extensive long-range correlations; since for any fixed ℓ the distance between the first two variables x_1, x_2 is greater than 4ℓ in $G(\mathbf{\Phi})$, (3.1.9) implies that for all $d < 2$, [3, Eq. 1.12]

$$\lim_{n\to\infty}\sum_{s,t\in\{\pm 1\}}\mathbb{E}\left[\left|\mu_{\mathbf{\Phi}}(\boldsymbol{\sigma}_{x_1}=s,\boldsymbol{\sigma}_{x_2}=t) - \mu_{\mathbf{\Phi}}(\boldsymbol{\sigma}_{x_1}=s)\cdot\mu_{\mathbf{\Phi}}(\boldsymbol{\sigma}_{x_2}=t)\right| \mid Z(\mathbf{\Phi})>0\right] = 0. \tag{3.1.10}$$

Thus, without loss of generality, by permutation invariance, (3.1.10) implies that asymptotic independence extends to all but $o(n^2)$ pairs of variables x_i, x_j w.h.p. Recall that the decorrelation property (3.1.10) known as *replica symmetry* was discussed in Section 1.2.2.

By the *depth* of $x \in V(\Phi)$ we mean the maximum distance between x and a leaf of $G(\Phi)$. For any Φ we set up BP as in (3.1.4)–(3.1.6). It was already discussed in Section 2.1.1 that BP computes the correct marginals if $G(\Phi)$ is acyclic. Then we have the following theorem that says for a tree, BP estimate of the marginal of x after ℓ iterations correctly matches the marginal of x for ℓ which is greater than or equal to the depth of x.

Proposition 3.1.3 ([60, Theorem 14.1]). *If $G(\Phi)$ is a tree and $x \in V(\Phi)$, then for any ℓ greater than or equal to the depth of x we have $\mu_\Phi(\boldsymbol{\sigma}_x = \pm 1) = \nu^{(\ell)}_{\Phi,x}(\pm 1)$.*

The proof of Theorem 3.1.1 proceeds in four steps.

Third, building upon these preparations, we will prove that the truncated mean $n^{-1}\mathbb{E}[\log(Z(\boldsymbol{\Phi}) \vee 1)]$ converges to the r.h.s. of (3.1.2). The truncation is necessary to deal with the unlikely event that $Z(\boldsymbol{\Phi}) = 0$. Finally, we will show that $\log(Z(\boldsymbol{\Phi}) \vee 1)$ concentrates about its mean to obtain convergence in probability, thus completing the proof of Theorem 3.1.1.

3.1.2 Step 1: Density evolution

First we prove that the limit π_d from Theorem 3.1.1 exists and π_d satisfies a tail bound as the following proposition describes.

Proposition 3.1.4 ([3, Proposition 2.1]). *The weak limit $\pi_d = \lim_{\ell\to\infty} \mathrm{BP}_d^\ell(\delta_{1/2})$ exists and*

$$\mathbb{E}\left[\log^2 \frac{\boldsymbol{\mu}_{\pi_d}}{1-\boldsymbol{\mu}_{\pi_d}}\right] < \infty. \tag{3.1.11}$$

Moreover, $\boldsymbol{\mu}_{\pi_d}$ and $1-\boldsymbol{\mu}_{\pi_d}$ are identically distributed and

$$\mathbb{E}\left|\log\left(\prod_{i=1}^{\boldsymbol{d}^-}\boldsymbol{\mu}_{\pi_d,i} + \prod_{i=1}^{\boldsymbol{d}^+}\boldsymbol{\mu}_{\pi_d,i+\boldsymbol{d}^-}\right)\right| < \infty, \qquad \mathbb{E}\left|\log\left(1-\boldsymbol{\mu}_{\pi_d,1}\boldsymbol{\mu}_{\pi_d,2}\right)\right| < \infty. \tag{3.1.12}$$

The proof of Proposition 3.1.4 is based on showing that BP is a contraction and that the fixed point iteration converges quickly to π_d. The following corollary clarifies the combinatorial meaning of the distribution π_d from Theorem 3.1.1. Namely, π_d is the limit of the empirical distribution of the marginal probabilities $\mu_{\boldsymbol{\Phi}}(\boldsymbol{\sigma}_{x_i} = 1)$.

Corollary 3.1.5 ([3, Corollary 1.3]). *For any $0 < d < 2$ the random probability measure*

$$\pi_{\boldsymbol{\Phi}} = \frac{1}{n}\sum_{i=1}^{n} \delta_{\mu_{\boldsymbol{\Phi}}(\boldsymbol{\sigma}_{x_i}=1)} \tag{3.1.13}$$

converges to π_d weakly in probability.

3.1.3 Step 2: Gibbs uniqueness

Next we prove (3.1.7) that BP approximates the conditional marginals well, which will verify the Gibbs uniqueness (3.1.9) and the convergence of the empirical marginals (3.1.13) to π_d.

We recall that $\mathbf{\Phi}$ locally looks like a tree so we analyze a bipartite Galton-Watson tree $\boldsymbol{T}$ that mimics $G(\mathbf{\Phi})$. Let $\boldsymbol{T}^{(\ell)}$ be the finite tree obtained from $\boldsymbol{T}$ and $\partial^{2\ell} o = \partial^{2\ell}(\boldsymbol{T}, o)$ denote the set of all variables within the distance of 2ℓ from the root variable o.

The following proposition is the heart of the proof which derives the Gibbs uniqueness for the tree formula $\boldsymbol{T}^{(2\ell)}$, which in turn by the contiguity of the tree and the graph, proves the Gibbs uniqueness for the graph as well.

Proposition 3.1.6 ([3, Proposition 2.2])**.** *We have*

$$\lim_{\ell\to\infty} \mathbb{E}\left[\max_{\tau\in S(\boldsymbol{T}^{(2\ell)})} \left|\mu_{\boldsymbol{T}^{(2\ell)}}(\boldsymbol{\sigma}_o = 1 \mid \boldsymbol{\sigma}_{\partial^{2\ell} o} = \tau_{\partial^{2\ell} o}) - \mu_{\boldsymbol{T}^{(2\ell)}}(\boldsymbol{\sigma}_o = 1)\right|\right] = 0. \tag{3.1.14}$$

We prove Proposition 3.1.6 by a subtle contraction argument in combination with construction of extreme boundary conditions of the tree formula $\boldsymbol{T}^{(2\ell)}$. Specifically, we will construct boundary conditions $\boldsymbol{\sigma}^{\pm}$ that maximize or minimize the conditional probability that the root gets "truth" value [3, Eq. 2.4]

$$\mu_{\boldsymbol{T}^{(2\ell)}}(\boldsymbol{\sigma}_o = 1 \mid \boldsymbol{\sigma}_{\partial^{2\ell} o} = \boldsymbol{\sigma}^{\pm}_{\partial^{2\ell} o}), \tag{3.1.15}$$

respectively. This is a unique feature of 2-SAT. We illustrate the maximum boundary condition $\boldsymbol{\sigma}^{+}_{\partial^{2\ell} o}$.

Let $C_x(+)$ be the set of check nodes that are children of the variable node x that impose truth value for x and $C_x(-)$ the opposite. All the checks in $C_x(+)$ are satisfied with $\boldsymbol{\sigma}_o = 1$ and in order to push the marginal toward 1, we set the values of the children variables of $C_x(+)$ to opposite of what the check nodes impose. Concerning $C_x(-)$, we set their children variables to what the check nodes impose in order to give a positive probability for x to receive 1 from those checks. Starting from the root variable o, we repeat setting the children variables according to this scheme down to the leaves at ℓ distance away.

Let $\boldsymbol{\sigma}^{+}$ denote the satisfying configuration on $\boldsymbol{T}^{(2\ell)}$ that maximizes the marginal on o being 1. Thus $\boldsymbol{\sigma}^{+}$ depends on the tree $\boldsymbol{T}^{(2\ell)}$. It seems untenable to work down the tree to set the values on the variables and go up on the now-fixed tree to calculate the marginal using the boundary conditions from $\boldsymbol{\sigma}^{+}$. In order to circumvent this issue, for each variable node $x \in \partial^{2k} o$, $k > 0$, of $\boldsymbol{T}^{(2\ell)}$, we define a quantity $\boldsymbol{\eta}_x \in \mathbb{R}\cup\{\pm\infty\}$ that features the Markov property of the random tree. Specifically, $\boldsymbol{\eta}_x$ measures how strongly x can nudge its grandparent variable y toward the truth value mandated by $\boldsymbol{\sigma}^{+}_y$ and is defined as the log-likelihood ratio [3, Eq. 5.1]

$$\boldsymbol{\eta}^{(\ell)}_x = \log \frac{Z(\boldsymbol{T}^{(2\ell)}_x, \boldsymbol{\sigma}^{+}, \boldsymbol{\sigma}^{+}_x)}{Z(\boldsymbol{T}^{(2\ell)}_x, \boldsymbol{\sigma}^{+}, -\boldsymbol{\sigma}^{+}_x)} \in \mathbb{R}\cup\{\pm\infty\} \qquad (x \in V(\boldsymbol{T}^{(2\ell)})), \tag{3.1.16}$$

where $Z(\boldsymbol{T}^{(2\ell)}_x, \boldsymbol{\sigma}^{+}, \boldsymbol{\sigma}^{+}_x)$ denotes the number of satisfying assignments of $\boldsymbol{T}^{(2\ell)}_x$ that agree with $\boldsymbol{\sigma}^{+}$ on the boundary and assign value $\boldsymbol{\sigma}^{+}_x$ to x. We find that $\boldsymbol{\eta}^{(\ell)}_o$ can be approximated by the k-fold recursion

of a suitable operator that turns out to be a W_1-contraction. Taking the limits as $k, \ell \to \infty$ finishes the proof.

3.1.4 Step 3: the Aizenman-Sims-Starr scheme

We briefly discussed how the Aizenman-Sims-Starr scheme in Section 2.3.2 can be applied to the free energy $\frac{1}{n}\log Z_n$ in order to derive the tight lower bound. It involves coupling the random formula $\boldsymbol{\Phi}_n$ with n variables and $\mathrm{Po}(dn/2)$ clauses and the random formula $\boldsymbol{\Phi}_{n+1}$ with $n+1$ variables and $\mathrm{Po}(d(n+1)/2)$ clauses. This coupling involves delicate moves. Introducing a new variable x_{n+1} along with a few random adjacent clauses that get attached to random variables already in $\boldsymbol{\Phi}_n$ can cause nullifying all the previously satisfying configurations by one new troublesome check node. To get around this issue, we introduce a third object as a liaison. Namely, let $\boldsymbol{\Phi}'$ be a 2-SAT with n variables and $\boldsymbol{m} = \mathrm{Po}(dn/2 - d/2)$ checks. Next, we get $\boldsymbol{\Phi}''$ from $\boldsymbol{\Phi}'$ by adding $\Delta'' = \mathrm{Po}(d/2)$ uniformly random and independent checks. Furthermore, we get $\boldsymbol{\Phi}'''$ from $\boldsymbol{\Phi}'$ by adding one variable x_{n+1} and $\Delta''' = \mathrm{Po}(d)$ checks.

The goal is to show

Corollary 3.1.7 ([3, Corollary 2.5])**.** *For any $d < 2$ we have*

$$\lim_{n\to\infty}\frac{1}{n}\mathbb{E}[\log(Z(\boldsymbol{\Phi})\vee 1)] = \mathbb{E}\left[\log\left(\prod_{i=1}^{\boldsymbol{d}^-}\boldsymbol{\mu}_{\pi_d,i} + \prod_{i=1}^{\boldsymbol{d}^+}\boldsymbol{\mu}_{\pi_d,i+\boldsymbol{d}^-}\right) - \frac{d}{2}\log\left(1-\boldsymbol{\mu}_{\pi_d,1}\boldsymbol{\mu}_{\pi_d,2}\right)\right].$$

Observing that $\boldsymbol{\Phi}''$ and $\boldsymbol{\Phi}'''$ have the same distributions as $\boldsymbol{\Phi}_n$ and $\boldsymbol{\Phi}_{n+1}$ respectively, we see the following fact immediately, [3, Fact 6.1]

$$\mathbb{E}[\log(Z(\boldsymbol{\Phi}_{n+1})\vee 1)] - \mathbb{E}[\log(Z(\boldsymbol{\Phi}_n)\vee 1)] = \mathbb{E}\left[\log\frac{Z(\boldsymbol{\Phi}''')\vee 1}{Z(\boldsymbol{\Phi}')\vee 1}\right] - \mathbb{E}\left[\log\frac{Z(\boldsymbol{\Phi}'')\vee 1}{Z(\boldsymbol{\Phi}')\vee 1}\right]. \tag{3.1.17}$$

Also helpful is to notice [3, Corollary 2.5]

$$\lim_{n\to\infty}\frac{1}{n}\mathbb{E}[\log(Z(\boldsymbol{\Phi})\vee 1)] = \lim_{n\to\infty}\frac{1}{n}\sum_{N=2}^{n-1}\mathbb{E}[\log(Z(\boldsymbol{\Phi}_{n+1})\vee 1)] - \mathbb{E}[\log(Z(\boldsymbol{\Phi}_n)\vee 1)]. \tag{3.1.18}$$

as the telescoping sum only retains the last summannd. Therefore the proof of Corollary 3.1.7 comes down to showing [3, Propositions 6.2, 6.3]

$$\mathbb{E}\left[\log\frac{Z(\boldsymbol{\Phi}''')\vee 1}{Z(\boldsymbol{\Phi}')\vee 1}\right] = \mathbb{E}\left[\log\left(\prod_{i=1}^{\boldsymbol{d}^-}\boldsymbol{\mu}_{\pi_d,i} + \prod_{i=1}^{\boldsymbol{d}^+}\boldsymbol{\mu}_{\pi_d,i+\boldsymbol{d}^-}\right)\right]$$
$$\mathbb{E}\left[\log\frac{Z(\boldsymbol{\Phi}'')\vee 1}{Z(\boldsymbol{\Phi}')\vee 1}\right] = \mathbb{E}\left[-\frac{d}{2}\log\left(1-\boldsymbol{\mu}_{\pi_d,1}\boldsymbol{\mu}_{\pi_d,2}\right)\right]$$

Careful argument is necessary to rule out rogue constraints ruining the already satisfying assignments. Detail is given in [3, Section 6].

3.1.5 Step 4: concentration

The final step to prove Theorem 3.1.1 is to show that $\log(Z(\mathbf{\Phi}) \vee 1)$ concentrates about its mean. In other words, the annealed computation equals the quenched one. However, because Z_n is exponential value, due to hard constraints, a small change in constraint can drive a large change in the partition function. Thus, a routine tool like the Azuma-Hoeffding inequality would not be sufficient. To get around this issue, we first consider the non-zero temperature case (1.2.4), as discussed in Section 1.2.3. From [68, 70, 78], we know $\log Z_\beta(\mathbf{\Phi})$ concentrates around its mean. By its loose restriction, $Z_\beta(\mathbf{\Phi}) \geq Z(\mathbf{\Phi})$. [78] also showed that $\lim_{n\to\infty} \frac{1}{n}\mathbb{E}\left[\log Z_\beta(\mathbf{\Phi})\right] \leq \mathfrak{B}_\beta(p)$ for any $p \in \mathscr{P}(0,1)$ where $\mathfrak{B}_\beta(p)$ stands for the corresponding Bethe functional. Combining these two facts we can show the following Corollary,

Corollary 3.1.8 ([3, Corollary 7.3]). *For any $\beta > 0$ we have* $\lim_{n\to\infty} \mathbb{P}\left[\log Z(\mathbf{\Phi}) > n\mathfrak{B}_\beta(\pi_d) + n^{2/3}\right] = 0$.

Finally, we can show that $\lim_{\beta\to\infty} \mathfrak{B}_\beta(\pi_d)$ exists and is finite such that $\log Z(\mathbf{\Phi})$ does not deviate more than εn from the mean, thereby concluding the proof.

3.2 Warning Propagation: stability and subcriticality

3.2.1 Basic Notions and Assumptions

Before we state the main theorem, we set some parametrs and assumptions. We define $\mathbb{G}$ to be a k-type graph (possibly a multigraph), i.e. $V(\mathbb{G}) = \{V_i\}_{i=1}^k$ where V_i the set of vertices of type i with (deterministic or random) cardinality $n_i := |V_i|$. For a vertex in V_i, let $\mathscr{Z}_i \in \mathbb{N}_0^k$ denote the asymptotic distribution of the numbers of neighbors of each type $j \in [k]$ such that the j-th entry, $\mathscr{Z}_{ij}$ describes the numbers of neighbors of type j connected to a vertex of type i. Furthermore, we denote a simple k-type graph by G. We denote the largest degree of $\mathbb{G}$ as $\Delta(\mathbb{G})$.

Definition 3.2.1 ([32, Definition 2.2]). *Let $\mathscr{Z}_1, \ldots, \mathscr{Z}_k \in \mathscr{P}\left(\mathbb{N}_0^k\right)$. For each $(i,j) \in \mathscr{K}$, define $\mathscr{Y}_{j,i} = \mathscr{Y}_{j,i}(\mathscr{Z}_i) \in \mathscr{P}\left(\mathbb{N}_0^k\right)$ to be the probability distribution such that for $(a_1, \ldots, a_k) \in \mathbb{N}_0^k$ we have*

$$\mathbb{P}\left(\mathscr{Y}_{j,i} = (a_1, \ldots, a_k)\right) := \frac{\mathbb{P}\left(\mathscr{Z}_i = \left(a_1, \ldots, a_{j-1}, a_j + 1, a_{j+1}, \ldots, a_k\right)\right)}{\mathbb{P}\left(\mathscr{Z}_{ij} \geq 1\right)}.$$

The point of $\mathscr{Y}_{j,i}$ is to compute the marginal distribution of a message from type i to type j. For this to happen, we need to have a positive probability of having such an edge.

Definition 3.2.2 ([32, Definition 2.3]). *Given $\mathscr{D} \in \mathscr{P}\left(\mathbb{N}_0^k\right)$ and a vector $\boldsymbol{q} = \left(q_1, \ldots, q_k\right) \in (\mathscr{P}(\Omega))^k$ of probability distributions on Ω, let us define a multiset $\mathscr{M}\left(\mathscr{D}, \boldsymbol{q}\right)$ of elements of Ω as follows.*

- *Generate a vector $(a_1, \ldots, a_k)$ according to $\mathscr{D}$.*
- *For each $j \in [k]$ independently, select a_j elements of Ω independently according to q_j. Call the resulting multiset $\mathscr{M}_j$.*
- *Define $\mathscr{M}\left(\mathscr{D}, \boldsymbol{q}\right) := \biguplus_{j=1}^k \mathscr{M}_j$.*

This definition is to take care of multiple types, each type of connected edges with differing message distributions. Thus we first determine the number of neighbors and draw message distributions for each type of neighbors. Then we can define the update function on message as a probability distribution matrix (PDM) R on Ω with

$$R[i,j] := \varphi\left(\mathscr{M}\left(\mathscr{Y}_{j,i}, Q[i]\right)\right)$$

where ϕ_φ stands for the collective operator on Q, gathering each entry as a result of φ. Further, let $\phi_\varphi^t(Q) = \phi_\varphi\left(\phi_\varphi^{t-1}(Q)\right)$ denote the t^{th} iterated function of ϕ_φ evaluated at Q.

Definition 3.2.3 ([32, Definition 2.5])**.** *The total variation distance of two $k\times k$ probability distribution matrices Q and R on the same set S is defined as $d_{\mathrm{TV}}(Q,R) := \sum_{i,j\in[k]} d_{\mathrm{TV}}\left(Q[i,j], R[i,j]\right)$.*

Definition 3.2.4 ([32, Definition 2.6])**.** *Let P be a PDM on Ω and $\varphi : \bigcup_{d\geq 0}\left(\!\!\binom{\Omega}{d}\!\!\right) \to \Omega$ be a WP update rule.*

1. *We say that P is a* fixed point *if $\phi_\varphi(P) = P$.*
2. *A fixed point P is* stable *if ϕ_φ is a contraction on a neighbourhood of P with respect to the total variation distance d_{TV} as defined in Definition 3.2.3.*
3. *We say that P is the* stable WP limit *of a PDM Q_0 on Ω if P is a stable fixed point, and furthermore the limit $\phi_\varphi^*(Q_0) := \lim_{t\to\infty}\phi_\varphi^t(Q_0)$ exists and equals P.*

Definition 3.2.5 ([32, Definition 2.7])**.** *For a k-type graph G, the type-degree of a vertex $v\in V(G)$, which we denote by $\boldsymbol{d}(v)$, is the sequence $(i,d_1,\ldots,d_k)\in[k]\times\mathbb{N}_0^k$ where i is the type of v and where d_j is the number of neighbours of v of type j. Moreover, the* type-degree sequence *$\boldsymbol{D}(G)$ of G is the sequence $(\boldsymbol{d}(v))_{v\in V(G)}$ of the type-degrees of all the vertices of G.*

Definition 3.2.6 ([32, Definition 2.8])**.** *Let $\mathscr{Z}_1,\ldots,\mathscr{Z}_k\in\mathscr{P}\left(\mathbb{N}_0^k\right)$ and for all $(i,j)\in\mathscr{K}$, let $\mathscr{Y}_{j,i}$ be as in Definition 3.2.1. For each $i\in[k]$, let $\mathscr{T}_i := \mathscr{T}_i(\mathscr{Z}_1,\ldots,\mathscr{Z}_k)$ denote a k-type Galton-Waltson process defined as follows:*

1. *The process starts with a single vertex u of type i.*
2. *Generate children of u with types according to $\mathscr{Z}_i$.*
3. *Subsequently, starting from the children of u, further vertices are produced recursively according to the following rule: for every vertex w of type h with a parent w' of type ℓ, generate children of w with types according to $\mathscr{Y}_{\ell,h}$ independently.*

Moreover, for $r\in\mathbb{N}_0$ we denote by $\mathscr{T}_i^r$ the branching process $\mathscr{T}_i$ truncated at depth r.

Definition 3.2.7 ([32, Definition 2.9])**.** *Let G be a k-type graph with parts $V_1(G),\ldots,V_k(G)$, let $i\in[k]$ and $r\in\mathbb{N}_0$. Then for a graph $H\in\mathscr{G}_\star$, we define*

$$\mathfrak{U}_{i,r}^G(H) := \frac{1}{|V_i(G)|}\sum_{u\in V_i(G)}\mathbf{1}\{B_G(u,r)\cong H\}.$$

In other words, $\mathfrak{U}_{i,r}^{G}$ defines a probability distribution on the class of k-type graphs H rooted at type i vertex of depth at most r, Thus, we can compare it with the truncated branching processes $\mathscr{T}_i^r$ (see **A4**). Now we state the assumptions for $\mathbb{G}$.

Assumption 3.2.8 ([32, Assumption 2.10])**.** *There exist functions*

$$1 \ll \Delta_0 = \Delta_0(n) \ll n^{1/10} \tag{3.2.1}$$

and $\zeta = \zeta(x) \xrightarrow{x\to\infty} \infty$ *and a probability distribution vector* $\mathscr{Z} := (\mathscr{Z}_1, \ldots, \mathscr{Z}_k) \in \left(\mathscr{P}\left(\mathbb{N}_0^k\right)\right)^k$ *such that for all* $i \in [k]$ *and for all* $x \in \mathbb{R}$*, we have*

$$\mathbb{P}\left(\|\mathscr{Z}_i\|_1 > x\right) \le \exp\left(-\zeta(x)\cdot x\right), \tag{3.2.2}$$

and such that the random graph $\mathbb{G}$ *satisfies the following properties:*

- ***A1*** *For all* $i \in [k]$ *we have* $\mathbb{E}(n_i) = \Theta(n)$ *and* $\mathrm{Var}(n_i) = o\left(n^{8/5}\right)$.
- ***A2*** *For any two simple* k*-type graphs* G *and* H *satisfying* $\boldsymbol{D}(G) = \boldsymbol{D}(H)$*, we have* $\mathbb{P}(\mathbb{G} = G) = (1 + o(1))\,\mathbb{P}(\mathbb{G} = H)$.
- ***A3*** *W.h.p.* $\Delta(\mathbb{G}) \le \Delta_0$*;*
- ***A4*** *For any* $i \in [k]$ *and* $r \in \mathbb{N}_0$ *we have*

$$d_{\mathrm{TV}}\left(\mathfrak{U}_i^r(\mathbb{G}), \mathscr{T}_i^r(\mathscr{Z})\right) \ll \frac{1}{\Delta_0^2} \quad \textit{w.h.p.}$$

The meaning of the assumptions 3.2.8 is as follows.

- **A1** - All vertex classes have the same order of magnitude and not too large variance.
- **A2** - The graph $\mathbb{G}$ is uniformly random given its type-degree sequence.
- **A3** - There are few vertices of high degree.
- **A4** - The local structure is described by the branching process $\mathscr{T}_i(\mathscr{Z}_1, \ldots, \mathscr{Z}_k)$.

We observe that **A4** states that the local structure of $\mathbb{G}$ is the branching processes $(\mathscr{T}_i)_{i\in[k]}$ with fast convergence. Usually, the main difficulty lies in bounding the speed of convergence of the local structure.

3.2.2 Main Result

Given a PDM Q_0 on Ω, we want to pin down how quickly WP will converge on $\mathbb{G}$ from a random initialization with Q_0. We will use $\varphi_{v\to w}^t\left(\mu^{(0)}\right)$ to denote the message from v to w in $\mathbb{G}$ after t iterations of warning propagation φ with initialization $\mu^{(0)}$.

Theorem 3.2.9 ([32, Theorem 1.3]). *Let $\mathbb{G}$ be a random graph model satisfying Assumption 3.2.8 and let P, Q_0 be probability distributions on Ω such that P is the stable WP limit of Q_0. Then for any $\delta > 0$ there exists $t_0 = t_0(\delta, \mathscr{Z}, \varphi, Q_0)$ such that the following is true.*

Suppose that $\mu^{(0)} \in \mathscr{M}(\mathbb{G})$ is an initialization according to Q_0. Then w.h.p. for all $t \geq t_0$ we have

$$\sum_{v,w:vw\in E(\mathbb{G})} \mathbb{1}\{\varphi^t_{v\to w}(\mu^{(0)}) \neq \varphi^{t_0}_{v\to w}(\mu^{(0)})\} < \delta n.$$

The main theorem states that after a bounded number of rounds t_0, the WP messages will stay unchanged except for at most δn many directed edges. It is crucial to note that t_0 does not depend on n or $\mathbb{G}$ but only subject to change regarding the desired accuracy δ, $\mathscr{Z}$, φ and Q_0.

Rather than generating $\mathbb{G}$ and applying WP directly, we use another model $\hat{\mathbb{G}}$ that resembles $\mathbb{G}$ yet allows more freedom so we can wield it to prove the main result. Namely, $\hat{\mathbb{G}}$ begins by having half-edges with messages and matching is performed. This idea of using half-edges first and matching next to draw a model that emulates the original model was briefly discussed in Section 2.3.2 and used in all four papers in this thesis.

This approximation by $\hat{\mathbb{G}}$ is what enables to show that very few changes occur between $\mathrm{WP}^{t_0-1}_{\mathbb{G}}(\mu^{(0)})$ and $\mathrm{WP}^{t_0}_{\mathbb{G}}(\mu^{(0)})$. Even so, these few changes could cause cascade effects later on. At this point, we use the local structure of a branching process $\mathfrak{T}$ to estimate the possible cascade effect and show that this branching process is subcritical.

The proof is done in two steps. First, we define the $\hat{\mathbb{G}}_{t_0}$ model and introduce Lemma 3.2.10, which states that this model is a good approximation for Warning Propagation on $\mathbb{G}$. Second, we introduce the branching process $\mathfrak{T}$ and prove that it is subcritical in Proposition 3.2.11. We combines these two steps to show after t_0 iterations of WP, very few further changes will be made and prove Theorem 3.2.9.

3.2.3 Message histories

We employed two distinct ways to keep up with the updates on directed messages. First a message contains the information on which two types are connected. Second, rather than looking at the current messages, we keep track of the entire history of directed messages. For two adjacent vertices u, v, we define the *t-history from u to v* to be the vector [[32, Section 3.1]]

$$\boldsymbol{\mu}_{u\to v}(\leq t) := \left(\mu_{u\to v}(0), \ldots, \mu_{u\to v}(t)\right) \in \Omega^{t+1}.$$

We denote by $\mathscr{G}^{(t)}_n$ the set of Ω^{t+1}-messaged graphs on vertex set $[n]$ with each directed edge having t-histories. Let $\mathbb{G}_t \in \mathscr{G}^{(t)}_n$ be the random Ω^{t+1}-messaged graph germinated by iterations of φ on $\mathbb{G}$ from the initial distribution Q_0. We also define $\mathbb{G}_* := \lim_{t\to\infty} \mathbb{G}_t$, if this limit exists (see [[32, Definition 3.1]]).

As discussed previously, we define $\hat{\mathbb{G}}_{t_0}$ as a configuration model that resembles $\mathbb{G}_{t_0}$ (see [[32, Definition 3.4]]). We note that the matching of the half-edges are maximum subject to the two conditions. One, the matching is consistent such that a half-edge with incoming $\boldsymbol{a}$ and outgoing $\boldsymbol{b}$ message histories is connected with a half-edge with incoming $\boldsymbol{b}$ and outgoing $\boldsymbol{a}$ message histories. Two, the resulting graph is simple with no multi-edges while we accept unmatched half-edges.

3.2.4 Step 1: Contiguity

Lemma 3.2.10 ([32, Lemma 3.7])**.** *For any integer $t_0 \in \mathbb{N}$ and real number $\delta > 0$, the random Ω^{t_0+1}-messaged graphs $\hat{\mathbb{G}}_{t_0}, \mathbb{G}_{t_0}$ can be coupled in such a way that w.h.p. $\hat{\mathbb{G}}_{t_0} \sim_\delta \mathbb{G}_{t_0}$.*

Note that $\sim_\delta$ means two compared objects are close to each other except for δn edges. Then Lemma 3.2.10 states that $\hat{\mathbb{G}}_{t_0}$ and $\mathbb{G}_{t_0}$ have approximately the same distribution.

The proof of Lemma 3.2.10 is detailed in [32, Section 5].

3.2.5 Step 2: Subcriticality

Given a probability distribution matrix Q on Ω and a pair $(\sigma_0, \tau_0) \in \mathscr{P}(Q)$, we define a branching process $\mathfrak{T} = \mathfrak{T}(\sigma_0, \tau_0, Q)$ as follows. We generate an instance of $\mathscr{T}_{ij}$, where $(i, j) = \bar{g}(\sigma_0)$, in particular including messages upwards to the directed root edge (v, u), so u is the parent of v. We then also initialize two messages downwards along this root edge, $\mu^{(1)}_{u\to v} = \sigma_0$ and $\mu^{(2)}_{u\to v} = \tau_0$. We track further messages down the tree based on the message that a vertex receives from its parent and its children according to the WP update rule φ. Given a vertex y with parent x, let $\mu^{(1)}_{x\to y}$ be the resultant message when the input at the root edge is $\mu^{(1)}_{u\to v} = \sigma_0$, and similarly $\mu^{(2)}_{x\to y}$ the resulting message when the input is $\mu^{(2)}_{u\to v} = \tau_0$. Finally, delete all edges (x, y) for which $\mu^{(1)}_{x\to y} = \mu^{(2)}_{x\to y}$, so we keep only edges at which messages change (along with any subsequently isolated vertices). It is an elementary consequence of the construction that $\mathfrak{T}$ is necessarily a tree.

Intuitively, $\mathfrak{T}$ approximates the cascade effect that a single change in a message from time $t_0 - 1$ to time t_0 subsequently causes (this is proved more precisely in [[32, Section 7]]). Therefore while much of this paper is devoted to showing that $\mathfrak{T}$ is indeed a good approximation, the following result is the essential heart of the proof of Theorem 3.2.9.

Proposition 3.2.11 ([32, Proposition 6.3])**.** *If P is a stable fixed point, then for any $(\sigma_0, \tau_0) \in \mathscr{P}(P)$, the branching process $\mathfrak{T} = \mathfrak{T}(\sigma_0, \tau_0, P)$ is subcritical.*

In the proof of Proposition 3.2.11 we define the transition matrix T of the change process $\mathfrak{T}$, which is a $|\Omega|^2 \times |\Omega|^2$ matrix where the entry $T[\boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2]$ is the expected number of changes of type $\boldsymbol{\sigma}_1$ that come from a change of type $\boldsymbol{\sigma}_2$. We note that the subcriticality of the branching process can be interpreted as $T^n \xrightarrow{n\to\infty} 0$. That happens if and only if all eigenvalues of T are strictly less than 1 (in absolute value).

As a result, we obtain the following corollary.

Corollary 3.2.12 ([32, Corollary 7.1]). *There exist a constant $\gamma > 0$ and a positive real $|\Omega|^2$-dimensional vector $\boldsymbol{\alpha}$ (with no zero entries) such that*

$$T\boldsymbol{\alpha} \leq (1-\gamma)\boldsymbol{\alpha}$$

(where the inequality is understood pointwise). We may further assume that $\|\boldsymbol{\alpha}\|_1 = 1$.

Lastly, the next corollary shows that when Q is close enough to P, we enjoy the similar result as in the previous corollary.

Corollary 3.2.13 ([32, Corollary 7.2]). *There exists $\delta_0 > 0$ sufficiently small that for any probability distribution Q on Ω which satisfies $d_{\mathrm{TV}}(P,Q) \leq \delta_0$, the following holds. Let $\mathfrak{T}_1 = \mathfrak{T}(\sigma_0, \tau_0, Q)$ and let T_1 be the transition matrix of $\mathfrak{T}_1$. Then there exist a constant $\gamma > 0$ and a positive real $|\Omega|^2$-dimensional vector $\boldsymbol{\alpha}$ (with no zero entries) such that*

$$T_1\boldsymbol{\alpha} \leq (1-\gamma)\boldsymbol{\alpha}$$

(where the inequality is understood pointwise).

That is, the same statement holds for T_1, the transition matrix of this slightly perturbed process, as for T. In particular, $\mathfrak{T}_1$ is also a subcritical branching process.

Let δ be fixed as in Theorem 3.2.9 and a constant $\delta_0 \ll \delta$ small enough that Corollary 3.2.13 holds. We can now complete the proof of our main theorem.

Proof of Theorem 3.2.9. We find that edges on which messages change when moving from $\mathrm{WP}^{t_0}(\mathbb{G}_0)$ to $\mathrm{WP}^*(\mathbb{G}_0)$ are numbered at most $\sqrt{\delta_0}n$. Furthermore, we can choose $\delta_0 \ll \delta$, the statement of Theorem 3.2.9 is proven. □

3.3 The Sparse Parity Matrix

Recall the definition of $f(\boldsymbol{A})$, the fraction of frozen variables. Then a variable v chosen uniformly at random would have about $f(\boldsymbol{A})$ probability of being frozen. Furthermore, due to the local tree structure of G, we observe that for the root v to be frozen, it would require that v has at least one check whose children variables are frozen. Then the following equation contains this information about $f(\boldsymbol{A})$.

$$\phi_d : [0,1] \to [0,1], \qquad \alpha \mapsto 1 - \exp\left(-d\exp\left(-d(1-\alpha)\right)\right); \tag{3.3.1}$$

that is, the fixed points of 3.3.1 are the plausible fractions of frozen variables. It turns out that there are possibly three fixed points in ϕ, two of which are stable fixed points denoted by $\alpha_* \leq \alpha^*$ and an unstable fixed point α_0 and they have the following hierarchy, $0 \leq \alpha_* \leq \alpha_0 \leq \alpha^* \leq 1$. Now we state the first main result of the paper.

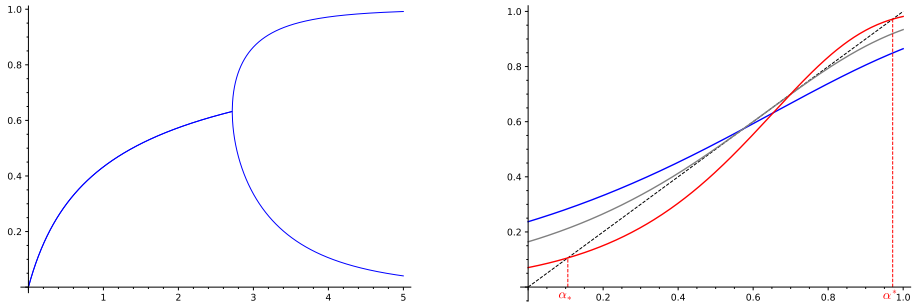

FIGURE 3.2: [24, Figure 1]. Left: the two fixed points $\alpha_* = \alpha_*(d)$ and $\alpha^* = \alpha^*(d)$ of ϕ_d. Right: the function ϕ_d for $d = 2.5$ (blue) possesses a unique fixed point, while for $d = 3$ (red) there are two stable fixed points and an unstable one in between.

Theorem 3.3.1 ([24, Theorem 1.1])**.** *1. For $d \le$ e the function ϕ_d has a unique fixed point and*

$$\lim_{n\to\infty} f(\boldsymbol{A}) = \alpha_* = \alpha^* \qquad \text{in probability.}$$

2. For $d >$ e we have $\alpha_* < \alpha^*$ and for all $\varepsilon > 0$,

$$\lim_{n\to\infty} \mathbb{P}\left[|f(\boldsymbol{A}) - \alpha_*| < \varepsilon\right] = \lim_{n\to\infty} \mathbb{P}\left[|f(\boldsymbol{A}) - \alpha^*| < \varepsilon\right] = \frac{1}{2}.$$

Recall the definition of the overlap 2.2.1. Here we state the second main result of the paper.

Theorem 3.3.2 ([24, Theorem 1.2])**.** *1. If $d <$ e then $\lim_{n\to\infty} R(\boldsymbol{x}, \hat{\boldsymbol{x}}) = (1 + \alpha_*)/2$ in probability.*

2. For all $d >$ e we have $\lim_{n\to\infty} \mathbb{E}\left|R(\boldsymbol{x}, \hat{\boldsymbol{x}}) - \bar{R}(\boldsymbol{A})\right| = 0$ while

$$\lim_{n\to\infty} \mathbb{P}\left[\left|\bar{R}(\boldsymbol{A}) - \frac{1+\alpha_*}{2}\right| < \varepsilon\right] = \lim_{n\to\infty} \mathbb{P}\left[\left|\bar{R}(\boldsymbol{A}) - \frac{1+\alpha^*}{2}\right| < \varepsilon\right] = \frac{1}{2} \qquad \text{for any } \varepsilon > 0.$$

Observe that Theorem 3.3.2 is the expression of Theorem 3.3.1 in terms of the overlap. Theorem 3.3.1 implies that an optimal algorithm such as Gaussian elimination can pin down $f(\boldsymbol{A}) \in \{\alpha_*, \alpha^*\}$ fraction among n variables. Regarding the complement $1 - f(\boldsymbol{A})$, a random guess would have to do, offering $\frac{1-f(\boldsymbol{A})}{2}$ chance to get the right values for the variables. Then the sum gives us the fraction of variables we can expect to retrieve: $\frac{1+f(\boldsymbol{A})}{2}$, which shows up in Theorem 3.3.2 with equal probability for each α_*, α^*.

Proofs of the two main results come by three steps. First, we show that $f(\boldsymbol{A})$ concentrates on the fixed points of ϕ_d, either on α_*, α^* or α_0. Second, we ascertain that the unstable fixed point α_0 is an unlikely outcome. Lastly, we conclude that α_* and α^* are equally likely.

3.3.1 Step 1: Fixed points of (3.3.1) and $f(\boldsymbol{A})$ match

Recall Theorem 1.3.1 from Section 1.3 regarding the nullity of $\boldsymbol{A}$ and the maximum of $\Phi(\alpha)$ where α can be interpreted as the fraction of frozen variables? It takes a bit of calculus to find that the stable fixed points of $\phi(\alpha)$ are the maximizers of $\Phi(\alpha)$. The left figure in Figure 3.2 shows the relationship

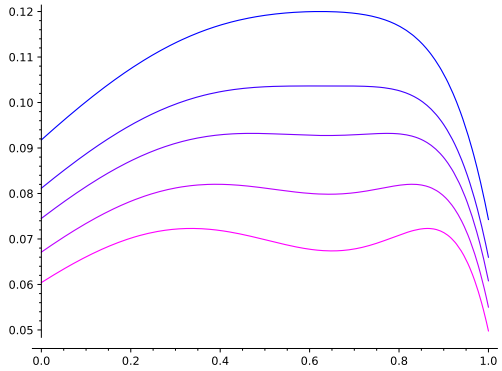

FIGURE 3.3: *Unused Figure from [24].* Φ_d for various d values where the second from the top is Φ_e.

between d and the stable fixed points of ϕ. If $d \le e$ then ϕ_d has a unique fixed point, which is the unique global maximizer of Φ_d, as in the case of the top curve in Figure 3.3. If $d > e$ then the function ϕ_d has precisely two stable fixed points, namely $0 < \alpha_* < \alpha^* < 1$, and

$$\Phi_d(\alpha_*) = \Phi_d(\alpha^*) > \Phi_d(\alpha) \qquad \text{for all } \alpha \in [0,1] \setminus \{\alpha_*, \alpha^*\}$$

i.e. α_*, α^* are the maximizers [[24, Proposition 2.3]].

Furthermore, for any $d > 0$ we have [[24, Lemma 2.2]]

$$\lim_{t\to\infty} \phi_d^{\circ t}(x) = \alpha_* \quad \text{for any } x < [0, \alpha_0), \qquad \lim_{t\to\infty} \phi_d^{\circ t}(x) = \alpha^* \quad \text{for any } x \in (\alpha_0, 1].$$

Now that we know the fixed points of $\phi(\alpha)$ and the maximizers of $\Phi(\alpha)$ math, how do we prove that the fixed points of ϕ_d are $f(\boldsymbol{A})$? WP helps to analyze the local structure of $G(\boldsymbol{A})$.

Enhanced Warning Propagation

Recall from Section 2.1.2 that WP is a scheme to update directed messages of {true, false} on the edges according to the neighbors' information. In our setting, the messages would carry either *unfrozen* or *frozen*. How do we initialize the messages? If initialized with the assumption of all being unfrozen, then because of local branching process, WP reduces to iteration of ϕ_d. Since $\lim_{t\to\infty} \phi_d^{\circ t}(0) = \alpha_*$, WP predicts $f(\boldsymbol{A}) = \alpha_*$. If initialized with the assumption of all being unfrozen, then by the same reasoning, $\lim_{t\to\infty} \phi_d^{\circ t}(1) = \alpha^*$ and WP predicts $f(\boldsymbol{A}) = \alpha^*$. Thus we run an enhanced version of Warning Propagation with three values, $\mathtt{f}, \mathtt{u}, \mathtt{s}$ (standing for *slush* to mean the uncertain status on the verge of freezing) as introduced in Section 3.2 for the paper [32]. We initialize all the messages as $\mathtt{s}$.

Our enhanced WP algorithm associates a pair of $\{\mathtt{f}, \mathtt{s}, \mathtt{u}\}$-valued messages with every edge of $G(A)$. Hence, let $\mathscr{W}(A)$ be the set of all vectors

$$w = (w_{v\to a}, w_{a\to v})_{v\in V(A), a\in C(A): a\in\partial v} \qquad \text{with entries } w_{v\to a}, w_{a\to v} \in \{\mathtt{f}, \mathtt{s}, \mathtt{u}\}.$$

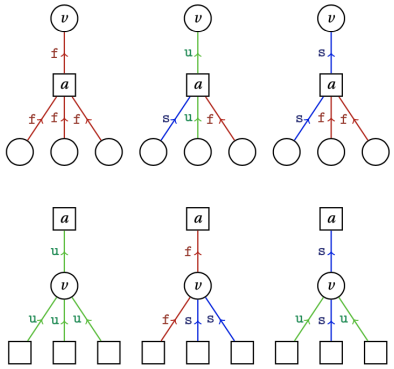

FIGURE 3.4: [24, Figure 2]. A local snapshot of the Warning Propagation rules. The check and variable nodes are represented by squares and circles respectively.

We define the WP operator $\varphi : \mathscr{W}(A) \to \mathscr{W}(A)$, $w \mapsto \hat{w}$, encoding one round of the message updates, by letting [[24, Eq. 2.2]]

$$\hat{w}_{a\to v} = \begin{cases} \mathtt{f} & \text{if } w_{y\to a} = \mathtt{f} \text{ for all } y \in \partial a \setminus \{v\}, \\ \mathtt{u} & \text{if } w_{y\to a} = \mathtt{u} \text{ for some } y \in \partial a \setminus \{v\}, \\ \mathtt{s} & \text{otherwise,} \end{cases} \tag{3.3.2}$$

$$\hat{w}_{v\to a} = \begin{cases} \mathtt{u} & \text{if } \hat{w}_{b\to v} = \mathtt{u} \text{ for all } b \in \partial v \setminus \{a\}, \\ \mathtt{f} & \text{if } \hat{w}_{b\to v} = \mathtt{f} \text{ for some } b \in \partial v \setminus \{a\}, \\ \mathtt{s} & \text{otherwise} \end{cases} \tag{3.3.3}$$

Furthermore, we define a *message distribution* to be a vector [[24, Section 4.1]]

$$\boldsymbol{q} = \left(\boldsymbol{q}^{(v)}, \boldsymbol{q}^{(c)}\right) \quad \text{with} \quad \boldsymbol{q}^{(v)} = \left(q^{(v)}_{\mathtt{f}}, q^{(v)}_{\mathtt{s}}, q^{(v)}_{\mathtt{u}}\right), \quad \boldsymbol{q}^{(c)} = \left(q^{(c)}_{\mathtt{f}}, q^{(c)}_{\mathtt{s}}, q^{(c)}_{\mathtt{u}}\right) \in [0,1]^3$$

Intuitively, $q^{(v)}, q^{(c)}$ model the probability distribution of an incoming message at a check/variable node, so for example $q^{(v)}_{\mathtt{f}}$ is the probability that an incoming message at a variable node is $\mathtt{f}$.

Note that given a message distribution $\boldsymbol{q}$, the local tree structure tells us that at a u.a.r. vertex the distribution of half-edges with incoming messages is given by $\mathrm{Po}(d\boldsymbol{a})$. Specifically, at a variable node, this generates $\mathrm{Po}\left(dq^{(v)}_{\mathtt{f}}\right)$ half-edges whose in-message is $\mathtt{f}$ and similarly (and independently) generates half-edges whose in-message is $\mathtt{s}$ or $\mathtt{u}$. At a check node, the generation of half-edges with

incoming messages is analogous. Define the conjectured limiting distribution [[24, Section 4.1]]

$$\boldsymbol{q}_* := \left(\boldsymbol{q}_*^{(v)}, \boldsymbol{q}_*^{(c)}\right) \quad \text{with} \quad \boldsymbol{q}_*^{(v)} = \left(q_{*,\mathtt{f}}^{(v)}, q_{*,\mathtt{s}}^{(v)}, q_{*,\mathtt{u}}^{(v)}\right) := \left(1-\alpha^*, \alpha^*-\alpha_*, \alpha_*\right), \tag{3.3.4}$$

$$\boldsymbol{q}_*^{(c)} = \left(q_{*,\mathtt{f}}^{(c)}, q_{*,\mathtt{s}}^{(c)}, q_{*,\mathtt{u}}^{(c)}\right) := \left(\alpha_*, \alpha^*-\alpha_*, 1-\alpha^*\right). \tag{3.3.5}$$

Let $\varphi(\boldsymbol{q})$ be the message update function and let $\varphi^*(\boldsymbol{q}) := \lim_{t\to\infty}\varphi^{\circ t}(\boldsymbol{q})$ if this limit exists. Note that $\boldsymbol{q}_0 = ((0,1,0),(0,1,0))$. The following two lemmas are verified by our paper on WP [32].

Lemma 3.3.3 ([24, Lemma 4.4])**.** *We have $\varphi^*\left(\boldsymbol{q}_0\right) = \boldsymbol{q}_*$. Furthermore, $\exists\ \varepsilon,\delta > 0$ s.t. for any message distribution $\boldsymbol{q}$ which satisfies $d_{\mathrm{TV}}\left(\boldsymbol{q},\boldsymbol{q}_*\right) \le \varepsilon$, we have $d_{\mathrm{TV}}\left(\varphi\left(\boldsymbol{q}\right),\boldsymbol{q}_*\right) \le (1-\delta)d_{\mathrm{TV}}\left(\boldsymbol{q},\boldsymbol{q}_*\right)$.*

That is, WP on the graph quickly converges nearly to the limit. In addition, we define $w(A,t) = \mathrm{WP}_A^t(\mathtt{s},\ldots,\mathtt{s})$ to be the messages that result after t iterations of WP_A launched from the all-$\mathtt{s}$ message vector $w(A,0)$. Furthermore, let $w(A) = \lim_{t\to\infty} w(A,t)$ be the fixed point to which WP_A converges. Observe that the (pointwise) limit always exists because WP_A only updates an $\mathtt{s}$-message to a $\mathtt{u}$-message or to an $\mathtt{f}$-message, while $\mathtt{u}$-messages and $\mathtt{f}$-messages will never change again.

Lemma 3.3.4 ([24, Lemma 4.5])**.** *For any $d,\delta > 0\ \exists\ t_0 \in \mathbb{N}$ s.t. w.h.p. $w(\boldsymbol{A})$ and $w(\boldsymbol{A},t_0)$ are identical except on a set of at most δn edges.*

This means after a bounded number of iterations, any further does not change much, i.e., it is subcritical. Finally, by the iterations of ϕ_d and WP, we can show the following:

Proposition 3.3.5 ([24, Proposition 2.7])**.** *For all $d \in (\mathrm{e},\infty)$ we have*

$$\lim_{n\to\infty} \mathbb{E}\left[\left|f(\boldsymbol{A})-\alpha_*\right| \wedge \left|f(\boldsymbol{A})-\alpha_0\right| \wedge \left|f(\boldsymbol{A})-\alpha^*\right|\right] = 0.$$

3.3.2 Step 2: Stable fixed points are the only tenable choices

Suppose $f(\boldsymbol{A}) = \alpha_0$. We start with observing that a random $\boldsymbol{x} \in \ker \boldsymbol{A}$ sets about half the unfrozen variables to one. Even if we weigh the variable nodes proportionally by their degrees, the overall weight of the one-entries comes to about half w.h.p. (1.3.4) implies that $\ker \boldsymbol{A}$ contains $2^{\Phi_d(\alpha_*)n+o(n)}$ such *balanced* vectors w.h.p.

We prove this step by contradiction. We show that the existence of that many balanced solutions is actually unlikely if $f(\boldsymbol{A}) \sim \alpha_0$.

First, the expectation of the number of fixed points (*covers*) of a version of WP operator that marks about $\alpha_0 n$ variables to frozen turns out to be of $\mathrm{orderexp}(o(n))$ [24, Proposition 6.3]. Next, a general version of the pinning operation discussed in Section 2.3.1 gives us the following lemma.

Lemma 3.3.6 ([24, Lemma 6.1])**.** *W.h.p. the random matrix $\boldsymbol{A}$ has $2^{\Phi_d(\alpha_*)n+o(n)}$ many $o(1)$-balanced solutions.*

For each cover, we compute the expected number of actual balanced solutions compatible with such a WP fixed point, $f(\boldsymbol{A}) = \alpha_0$. We expect the fractions of unfrozen variables and unfrozen checks to be

[[24, Eqs. 6.19, 6.20]]

$$\frac{1}{n}\sum_{i=1}^{n}\mathbb{1}\{\mathfrak{m}(v_i)=\mathtt{u}\}\sim 1-\alpha_0,$$
$$\frac{1}{n}\sum_{i=1}^{n}\mathbb{1}\{\mathfrak{m}(a_i)=\mathtt{u}\}\sim \alpha_0-d(1-\alpha_0)^2,$$

respectively. Each unfrozen check has about $1/2$ probability to be satisfied and each unfrozen variable has freedom to choose between 2 values.

Combining these items and multiplying the sum by the number of covers, we can expect the number of actual balanced solutions to be [[24, Eq. 6.21]]

$$2^{|\{i\in[n]:\mathfrak{m}(v_i)=\mathtt{u}\}|-|\{i\in[n]:\mathfrak{m}(a_i)=\mathtt{u}\}|+o(n)}\le 2^{n(1-2\alpha_0+d(1-\alpha_0)^2+o(1))}=2^{n\Phi_d(\alpha_0)+o(n)}.$$

However, this value falls short of what (1.3.4) guarantees. In other words, because $\Phi_d(\alpha_0)<\Phi_d(\alpha_*)=\max_\alpha\Phi_d(\alpha)$, we see that $f(\boldsymbol{A})\sim\alpha_0$ creates far fewer balanced vectors in its kernel than (1.3.4) requires. Thus, $f(\boldsymbol{A})\sim\alpha_0$ is unlikely.

3.3.3 Step 3: Both stable fixed points are equally likely

Recall that all messages are initialized as $\mathtt{s}$. As the WP operator φ updates the messages, either $\mathtt{s}$ resists any change or changes to $\mathtt{f}$ or $\mathtt{u}$ and stays that way. Define a minor matrix $\boldsymbol{A}_\mathtt{s}$ of $\boldsymbol{A}$ to be composed of variables and checks that belong to the *slush*. Specifically, for a given matrix A let [[24, Section 7]]

$$V_\mathtt{s}(A)=\{v\in V(A):(\forall a\in\partial v: w_{a\to v}(A)\neq\mathtt{f}),|\{a\in\partial v: w_{a\to v}(A)=\mathtt{s}\}|\ge 2\},\tag{3.3.6}$$
$$C_\mathtt{s}(A)=\{a\in C(A):(\forall v\in\partial a: w_{v\to a}(A)\neq\mathtt{u}),|\{v\in\partial a: w_{v\to a}(A)=\mathtt{s}\}|\ge 2\}.\tag{3.3.7}$$

We already saw in (3.3.4),(3.3.5) that WP shows asymptotically $\alpha^*-\alpha_*$ portion is either all frozen or all unfrozen. Using the symmetry of the model and moment calculations, we have the following two propositions that finalize the proof.

Proposition 3.3.7 ([24, Proposition 2.9])**.** *For any $d_0>\mathrm{e}$ there exists a function $\omega=\omega(n)\gg 1$ such that for all $d>d_0$ we have*

$$\lim_{n\to\infty}\mathbb{P}\left[|V_\mathtt{s}(\boldsymbol{A})|-|C_\mathtt{s}(\boldsymbol{A})|\ge\omega\right]=\lim_{n\to\infty}\mathbb{P}\left[|C_\mathtt{s}(\boldsymbol{A})|-|V_\mathtt{s}(\boldsymbol{A})|\ge\omega\right]=\frac{1}{2}.$$

Proposition 3.3.8 ([24, Proposition 2.10])**.** *For any $d>\mathrm{e}$, $\varepsilon>0$, $\omega=\omega(n)\gg 1$ we have*

$$\limsup_{n\to\infty}\mathbb{P}\left[|f(\boldsymbol{A})-\alpha^*|<\varepsilon,\ |V_\mathtt{s}(\boldsymbol{A})|-|C_\mathtt{s}(\boldsymbol{A})|\ge\omega\right]=0$$
$$\limsup_{n\to\infty}\mathbb{P}\left[|f(\boldsymbol{A})-\alpha_*|<\varepsilon,\ |C_\mathtt{s}(\boldsymbol{A})|-|V_\mathtt{s}(\boldsymbol{A})|\ge\omega\right]=0.$$

Combining Propositions 3.3.7, 3.3.8, we prove that $f(\boldsymbol{A}) = \alpha_*$ or $f(\boldsymbol{A}) = \alpha^*$ with equal probability of $1/2$.

3.4 The Full Rank Condition for Sparse Random Matrices

3.4.1 Main Results

Finite fields

Let $\mathbb{A}$ be defined as before in Section 1.3.2. The first result gives a sufficient condition for $\mathbb{A}$ to have full rank. The second regards the rank of zero-one matrix over rationals, $\mathbb{B}$. Recall the definition of $\boldsymbol{\Phi}$ from (1.3.3) that provides the information on the asymptotic rank of $\mathbb{A}$.

Theorem 3.4.1 ([27, Theorem 1.1])**.** *If q and $\mathfrak{d}$ are coprime and*

$$\Phi(z) < \Phi(0) \qquad \text{for all } 0 < z \leq 1, \tag{3.4.1}$$

then $\mathbb{A}$ has full row rank over $\mathbb{F}_q$ w.h.p.

Since Φ does not depend on q, the condition (3.4.1) is not contingent on the choice q. We will show that the sufficient condition (3.4.1) is generally necessary as well.

Since $\boldsymbol{k} \geq 3$, the definition (1.3.3) ensures that $\Phi(0) = 1 - d/k$ and thus $n\Phi(0) \sim n - \boldsymbol{m}$ w.h.p. Therefore (1.3.4) implies that $\mathrm{rk}(\mathbb{A}) \leq \boldsymbol{m} - \Omega(n)$ w.h.p. unless $\Phi(z)$ attains its maximum at $z = 0$. In other words, $\mathbb{A}$ has full row rank only if $\Phi(z) \leq \Phi(0)$ for all $0 < z \leq 1$. Indeed, in [27, Section 1.3] we show examples that requite a strict inequality as in (3.4.1). The condition that q and $\mathfrak{d}$ be coprime is generally necessary as well, as we show in [27, Example 1.7].

Let us emphasize that (1.3.4) does not guarantee that $\mathbb{A}$ has full row rank w.h.p. even if (3.4.1) is satisfied. Due to normalization on the l.h.s. (1.3.4) only implies the much weaker statement $\mathrm{rk}(\mathbb{A}) = \boldsymbol{m} - o(n)$ w.h.p. Hence, in the case that (3.4.1) is satisfied, Theorem 3.4.1 improves over the asymptotic estimate (1.3.4) substantially. Such a stronger result also requires a more delicate proof strategy.

Zero-one matrices over the rationals

Apart from matrices over finite fields, the rational rank of sparse random $\{0,1\}$-matrices has received a great deal of attention [83, 84]. The random graph $\mathbb{G}$ naturally induces a $\{0,1\}$-matrix, namely the $\boldsymbol{m} \times n$-biadjacency matrix $\mathbb{B} = \mathbb{B}(\mathbb{G})$. Explicitly, $\mathbb{B}_{ij} = \mathbb{1}\{a_i x_j \in E(\mathbb{G})\}$. As an application of Theorem 3.4.1 we obtain the following result.

Corollary 3.4.2 ([27, Corollary. 1.2])**.** *If (3.4.1) is satisfied then the random matrix $\mathbb{B}$ has full row rank over $\mathbb{Q}$ w.h.p.*

Since (1.3.4) holds for random matrices over the rationals as well, Corollary 3.4.2 is optimal to the extent that $\mathbb{B}$ fails to have full row rank w.h.p. if $\max_{x \in [0,1]} \Phi(x) > \Phi(0)$. Moreover, in [27, Example 1.4] we show that $\mathbb{B}$ does not generally have full rank w.h.p. unless $x = 0$ is the unique maximizer of Φ.

The proof of these main results boil down to show the relations (1.3.12), (1.3.13) are true. Theorem 3.4.2 is established once Theorem 3.4.1 is proven so we now focus on the case of $\mathbb{A}$.

3.4.2 Step 1: Proving the first moment relation (1.3.12)

Let us begin with (1.3.12). (1.3.4) alone cannot prove that $\mathfrak{O}$ is a likely event. Thus we consider a perturbed matrix. Specifically, for an integer $t \geq 0$ obtain $\mathbb{A}_{[t]}$ from $\mathbb{A}$ by adding t more rows that contain precisely three non-zero entries. The positions of these non-zero entries are chosen uniformly, mutually independently and independently of everything else, and the non-zero entries themselves are independent copies of $\boldsymbol{\chi}$. We require the following lower bound on the rank of $\mathbb{A}_{[t]}$.

Proposition 3.4.3 ([27, Proposition 2.1])**.** *If* (3.4.1) *is satisfied then there exists* $\delta_0 = \delta_0(\boldsymbol{d}, \boldsymbol{k}) > 0$ *such that for all* $0 < \delta < \delta_0$ *we have*

$$\liminf_{n\to\infty} \frac{1}{n}\mathbb{E}[\operatorname{nul} \mathbb{A}_{[\lfloor \delta n \rfloor]}] \leq 1 - \frac{d}{k} - \delta. \tag{3.4.2}$$

Proposition 3.4.3 leads us to (1.3.12). We first show that Proposition 3.4.3 is only possible when $\mathbb{A} \in \mathfrak{O}$ w.h.p. The implication of Proposition 3.4.3 is that almost every one of the ternary equation lowers the nullity by one. If Proposition 3.4.3 is true on the assumption on (3.4.1) and if Proposition 3.4.3 is only possible when $\mathbb{A} \in \mathfrak{O}$, then (3.4.1) must mean $\mathbb{A} \in \mathfrak{O}$. The proof of Proposition 3.4.3 relies on the Aizenman-Sims-Starr scheme that was discussed in Section 2.3.2. The proof of 3.4.3 is similar to the proof of the rank formula Theorem 1.3.1 in [26] but we take a more delicate care to accommodate the ternary equations. The way of the proof is basically by showing that there cannot be too many frozen variables (1.3.1) and using the pinning operation discussed in Section 2.3.1. The detail is given in [[27, Section 4]].

Finally, by combining the idea of Aizenman-Sim-Starr and sparsity of frozen variables in connection with $\mathfrak{O}$, we have the following proposition; the detail of the proof is found in [[27, Section 5]].

Proposition 3.4.4 ([27, Proposition 2.2])**.** *Assume that* (3.4.1) *is satisfied. Then* (1.3.12) *holds w.h.p.*

3.4.3 Step 2: Proving the second moment relation (1.3.13)

Now that we know the assumption (3.4.1) proves (1.3.12), which in turn implies $\mathbb{A} \in \mathfrak{O}$, we can establish (1.3.13) by expanding (1.3.9) around the uniform distribution (1.3.10).

To estimate $\ker \mathbb{A}$ accurately while allowing general distributions for $\boldsymbol{d}, \boldsymbol{k}$ and $\boldsymbol{\chi} \in \mathbb{F}_q$, we need to investigate the conceivable frequencies of field elements that can lead to solutions. Specifically, for an integer $k_0 \geq 3$ and $\chi_1, \ldots, \chi_{k_0} \in \mathbb{F}_q^*$ let

$$\mathscr{S}_q(\chi_1, \ldots, \chi_{k_0}) = \left\{ \sigma \in \mathbb{F}_q^{k_0} : \sum_{i=1}^{k_0} \chi_i \sigma_i = 0 \right\} \tag{3.4.3}$$

comprise all solutions to a linear equation with coefficients $\chi_1,\dots,\chi_{k_0} \in \mathbb{F}_q$. For each solution k_0-ary vector $\sigma \in \mathscr{S}_q(\chi_1,\dots,\chi_{k_0})$ the vector [[27, Eq. 2.14]]

$$\hat{\sigma} = \left(\sum_{i=1}^{k_0} \mathbb{1}\{\sigma_i = s\}\right)_{s\in\mathbb{F}_q^*} \in \mathbb{Z}^{\mathbb{F}_q^*} \tag{3.4.4}$$

tracks the number of each field element as a $q-1$-ary vector. Depending on the coefficients $\chi_1,\dots,\chi_{k_0}$, the frequency vectors $\hat{\sigma}$ may live in a proper sub-grid of the integer lattice $\mathbb{Z}^{\mathbb{F}_q^*}$. For example, in the case $q = k_0 = 3$ and $\chi_1 = \chi_2 = \chi_3 = 1$ they span the sub-lattice spanned by $\binom{1}{1}$ and $\binom{0}{3}$. The following proposition characterizes the lattice spanned by the $\hat{\sigma}$ for general k_0 and $\chi_1,\dots,\chi_{k_0}$.

Proposition 3.4.5 ([27, Proposition 2.3])**.** *Let $k_0 \geq 3$, let $\chi_1,\dots,\chi_{k_0} \in \mathbb{F}_q^*$ and let $\mathfrak{M}_q(\chi_1,\dots,\chi_{k_0}) \subseteq \mathbb{Z}^{\mathbb{F}_q^*}$ be the $\mathbb{Z}$-module generated by the frequency vectors $\hat{\sigma}$ for $\sigma \in \mathscr{S}_q(\chi_1,\dots,\chi_{k_0})$. Then $\mathfrak{M}_q(\chi_1,\dots,\chi_{k_0})$ has a basis $\mathfrak{b}_1,\dots,\mathfrak{b}_{q-1}$ of non-negative integer vectors with $\|\mathfrak{b}_i\|_1 \leq 3$ for all $1 \leq i \leq q-1$ such that* $\det\left(\mathfrak{b}_1 \cdots \mathfrak{b}_{q-1}\right) = q^{\mathbb{1}\{\chi_1=\cdots=\chi_{k_0}\}}$.

Note that the basis vectors have small ℓ_1-norm. We also show that these basis vectors are combinatorially meaningful in our purpose of counting solutions. The detail of the proof is found in [[27, Section 6]].

In addition to the frequency grid, we also observe another constraint due to $\boldsymbol{d}$. Namely, for any assignment $\sigma \in \mathbb{F}_q^n$ to variables the frequencies of the various field elements $s \in \mathbb{F}_q$ are divisible by the g.c.d. $\mathfrak{d}$ of $\operatorname{supp}(\boldsymbol{d})$, i.e. [[27, Eq. 2.15]]

$$\mathfrak{d} \mid \sum_{i=1}^{n} \boldsymbol{d}_i \mathbb{1}\{\sigma_i = s\} \qquad \text{for all } s \in \mathbb{F}_q. \tag{3.4.5}$$

Thus to compute the expected kernel size we look at the intersection of the sub-grid (3.4.5) with the grid spanned by the frequency vectors $\hat{\sigma}$ for $\sigma \in \mathscr{S}_q(\boldsymbol{\chi}_{1,1},\dots,\boldsymbol{\chi}_{1,\boldsymbol{k}})$. Specifically, by way of estimating the number of assignments represented by each grid point and calculating the ensuing satisfiability probability, we obtain the following.

Proposition 3.4.6 ([27, Proposition 2.4])**.** *Assume that q and $\mathfrak{d}$ are coprime and that (3.4.1) is satisfied. Then (1.3.13) holds w.h.p.*

Combining Propositions 3.4.3–3.4.6, we now establish the main theorem and its corollary.

Proof of Theorem 3.4.1. The assumption (3.4.1) implies that $1 - d/k = \Phi(0) > \Phi(1) = 0$. Combining Propositions 3.4.4 and 3.4.6, we obtain (1.3.12)–(1.3.13). Hence, Chebyshev's inequality implies that $\boldsymbol{Z} \geq q^{n-\boldsymbol{m}} = q^{n(1-d/k+o(1))} > 0$ w.h.p. Consequently, the random linear system $\mathbb{A}x = \boldsymbol{y}$ has a solution w.h.p., and thus $\operatorname{rk}\mathbb{A} = \boldsymbol{m}$ w.h.p. □

Proof of Corollary 3.4.2. Let q be a prime that does not divide $\mathfrak{d}$ and let $\boldsymbol{\chi} = 1$ deterministically. Obtain the matrix $\bar{\mathbb{B}} \in \mathbb{F}_q^{\boldsymbol{m}\times n}$ by reading the $\{0,1\}$-entries of $\mathbb{B}$ as elements of $\mathbb{F}_q$. Then the distribution of $\bar{\mathbb{B}}$ coincides with the distribution of the random $\mathbb{F}_q$-matrix $\mathbb{A}$. Hence, Theorem 3.4.1 implies that $\bar{\mathbb{B}}$ has full row rank w.h.p.

Suppose that indeed $\mathrm{rk}\bar{\mathbb{B}} = \boldsymbol{m}$. We claim that then the rows of $\mathbb{B}$ are linearly independent. Indeed, assume that $z^\top \mathbb{B} = 0$ for some vector $z = (z_1, \ldots, z_{\boldsymbol{m}})^\top \in \mathbb{Z}^{\boldsymbol{m}}$. Factoring out $\gcd(z_1, \ldots, z_{\boldsymbol{m}})$ if necessary, we may assume that the vector $\bar{z} \in \mathbb{F}_q^{\boldsymbol{m}}$ with entries $\bar{z}_i = z_i + q\mathbb{Z}$ is non-zero. Since $z^\top \mathbb{B} = 0$ implies that $\bar{z}^\top \bar{\mathbb{B}} = 0$, the rows of $\bar{\mathbb{B}}$ are linearly dependent, in contradiction to our assumption that $\bar{\mathbb{B}}$ has full row rank. □

The rest of this section we sketch the proofs of Proposition 3.4.5 and Proposition 3.4.6.

Proof of Proposition 3.4.5

We differentiate the cases where the coefficients $\chi_1, \ldots, \chi_{k_0}$ are identical or not. The following two lemmas summarize the analyses of the two cases.

Lemma 3.4.7 ([27, Lemma 6.1])**.** *For any prime power q and any $\chi \in \mathbb{F}_q^*$ the $\mathbb{Z}$-module $\mathfrak{M}_q(\chi, \chi, \chi)$ possesses a basis $(\mathfrak{b}_1, \ldots, \mathfrak{b}_{q-1})$ of non-negative integer vectors $\mathfrak{b}_i \in \mathbb{Z}^{\mathbb{F}_q^*}$ for all $i \in [q-1]$ such that*

$$\|\mathfrak{b}_i\|_1 \le 3 \quad \text{and} \quad \sum_{s \in \mathbb{F}_q^*} \mathfrak{b}_{i,s} s = 0 \quad \text{for all } i \in [q-1], \text{ and} \quad \det\left(\mathfrak{b}_1 \cdots \mathfrak{b}_{q-1}\right) = q.$$

Furthermore, for any $k_0 > 3$ we have $\mathfrak{M}_q\underbrace{(\chi, \ldots, \chi)}_{k_0 \text{ times}} = \mathfrak{M}_q(\chi, \chi, \chi)$.

Lemma 3.4.8 ([27, Lemma 6.2])**.** *Suppose that q is a prime power, that $k_0 \ge 3$ and that $\chi_1, \ldots, \chi_{k_0} \in \mathbb{F}_q^*$ satisfy $|\{\chi_1, \ldots, \chi_{k_0}\}| \ge 2$. Then*

$$\mathfrak{M}_q(\chi_1, \ldots, \chi_{k_0}) = \mathbb{Z}^{\mathbb{F}_q^*}.$$

Furthermore, $\mathfrak{M}_q(\chi_1, \ldots, \chi_{k_0})$ possesses a basis $(\mathfrak{b}_1, \ldots, \mathfrak{b}_{q-1})$ of non-negative integer vectors $\mathfrak{b}_i \in \mathbb{Z}^{\mathbb{F}_q^*}$ such that

$$\|\mathfrak{b}_i\|_1 \le 3 \quad \text{and} \quad \sum_{s \in \mathbb{F}_q^*} \mathfrak{b}_{i,s} s = 0 \quad \text{for all } i \in [q-1].$$

In case of Lemma 3.4.7 we get a proper subgrid while in case of Lemma 3.4.8 we get the whole integer module. Proposition 3.4.5 is an immediate consequence of Lemmas 3.4.7 and 3.4.8.

Remark 3.4.9 (Sketch of Proof of Lemma 3.4.7)**.** *It is easy to come up with $q-1$ linearly independent vectors in $\mathfrak{M}$ with ℓ_1-norms bounded by 3 but not easy to see that they generate $\mathfrak{M}$. To that end, we come up with two different bases for $\mathfrak{M}$, namely $\mathscr{B}_1, \mathscr{B}_2$. It would be easy to see $\mathscr{B}_1$ generates $\mathfrak{M}$ while $\mathscr{B}_2$ comprises of linearly independent vectors in $\mathfrak{M}$ with ℓ_1-norms bounded by 3. We use the following elementary lemma to show that $\mathscr{B}_1$ and $\mathscr{B}_2$ generate the same module by showing the change of basis matrix between $\mathscr{B}_1$ and $\mathscr{B}_2$ has the determinant of one.*

Lemma 3.4.10 ([22, p. 135])**.** *Let $\mathfrak{M} \subseteq \mathbb{R}^\ell$ be a $\mathbb{Z}$-module with basis $b_1, \ldots, b_\ell$. Then*

$$\lim_{r \to \infty} \frac{|\{x \in \mathfrak{M} : \|x\| \le r\}|}{\mathrm{vol}\left(\{x \in \mathbb{R}^\ell : \|x\| \le r\}\right)} = \frac{1}{|\det(b_1 \cdots b_\ell)|}.$$

$$M_p = \begin{array}{c} \\ 1 \\ 2 \\ \\ \\ \\ \\ \\ p-1 \end{array} \begin{array}{c} \begin{array}{ccccccccc} 1 & 2 & & . & . & . & . & & p-1 \end{array} \\ \begin{pmatrix} 1 & & & & & & & & \\ & 1 & & & & & & & \\ & & 1 & & & & & & \\ & & & \ddots & & & & & \\ & & & & & & & & \\ & & & & & \ddots & & & \\ & & & & & & 1 & & \\ 1 & 2 & 3 & & \cdots & & p-2 & & p \end{pmatrix} \end{array}.$$

FIGURE 3.5: [27, Figure 4]. The matrix M_p.

$$A_p = \begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & \vdots & \vdots & & & \iddots & 1 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots & & \iddots & \iddots & 0 \\ \vdots & & \ddots & \ddots & 0 & \vdots & \iddots & \iddots & \iddots & \vdots \\ 0 & \cdots & \cdots & 0 & 1 & 0 & 1 & 0 & \cdots & 0 \\ 0 & \cdots & \cdots & 0 & 1 & 2 & 0 & \cdots & \cdots & 0 \\ \vdots & & \iddots & \iddots & 0 & 0 & 1 & \ddots & & \vdots \\ \vdots & \iddots & \iddots & \iddots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \iddots & \iddots & & \vdots & 0 & \cdots & 0 & 1 & 0 \\ 1 & 0 & \cdots & \cdots & 0 & 1 & \cdots & \cdots & 1 & 2 \end{pmatrix}. \tag{3.4.6}$$

FIGURE 3.6: [27, Figure 6]. The matrix A_p.

We remark that some meticulous ordering of elements of $\mathbb{F}_q = p^\ell$ is necessary to make this calculation easier, namely to make the matrices as "lower triangular" as possible. The final point here is the the determinants of both modules are 1 thereby making the bases equivalent. See Figures 3.5 and 3.6 for an illustration of the case $\mathbb{F}_p$. In case of $\mathbb{F}_q = p^\ell, \ell \geq 2$, M_p and A_p are used ℓ times as blocks. The detailed set up of basis vectors for $\mathscr{B}_1$ and $\mathscr{B}_2$ are given in [[27, Section 6.1]].

Proof of Lemma 3.4.8 entails devising bases for various cases, namely regarding whether p is 2 or odd and the value of the second coefficient χ_2 while holding $\chi_1 = 1$. The end result for each case shows that the bases generate the integer module. The detail is laid out in [[27, Section 6.2]].

Proof of Proposition 3.4.6

Our goal is to bound the expected size of the kernel of $\mathbb{A}$ on $\mathfrak{O}$, namely $|\ker \mathbb{A}| \cdot \mathbb{1}_{\mathfrak{O}}$. Let $\mathfrak{A}$ be the σ-algebra generated by $\boldsymbol{m}, (\boldsymbol{k}_i)_{i\geq 1}, (\boldsymbol{d}_i)_{i\geq 1}$ and by the numbers $\boldsymbol{m}(\chi_1, \ldots, \chi_\ell)$ of equations of degree $\ell \geq 3$ with coefficients $\chi_1, \ldots, \chi_\ell \in \mathbb{F}_q^*$. Thus, the total degree $\boldsymbol{\Delta} = \sum_{i=1}^n \boldsymbol{d}_i$ is $\mathfrak{A}$-measurable.

Let us define the empirical frequency for a vector $\sigma \in \mathbb{F}_q^n$ and $s \in \mathbb{F}_q$ [[27, Eq. 7.1]]

$$\rho_\sigma(s) = \sum_{i=1}^{n} \boldsymbol{d}_i \mathbb{1}\{\sigma_i = s\} \tag{3.4.7}$$

and let $\rho_\sigma = (\rho_\sigma(s))_{s\in\mathbb{F}_q}$. In the event of $\mathfrak{O}$, ρ_σ has nearly uniform entries for most $\sigma \in \ker \mathbb{A}$. Here is a helpful statement that characterizes such uniformity.

Fact 3.4.11 ([27, Fact 7.1]). *For any $\varepsilon > 0$ w.h.p. given $\mathfrak{A}$ we have*

$$\mathbb{1}\mathfrak{O} \cdot |\ker \boldsymbol{A}| \le (1+\varepsilon)\left|\{\sigma \in \ker \boldsymbol{A} : \|\rho_\sigma - q^{-1}\boldsymbol{\Delta}\mathbb{1}\|_1 < \varepsilon\boldsymbol{\Delta}\}\right|.$$

In other words, it suffices to count nearly equitable kernel vectors only. We look into different regimes of nearly equitable frequency vectors and bound their contributions. Let $\mathfrak{P}_q$ be the set of all possible frequency vectors, i.e., [[27, Section 7.1]]

$$\mathfrak{P}_q = \left\{\rho_\sigma : \sigma \in \mathbb{F}_q^n\right\}.$$

For $\varepsilon > 0$ let

$$\mathfrak{P}_q(\varepsilon) = \left\{\rho \in \mathfrak{P}_q : \|\rho - q^{-1}\boldsymbol{\Delta}\mathbb{1}\| < \varepsilon\boldsymbol{\Delta}\right\}.$$

In addition, we introduce

$$\begin{aligned}
\mathcal{Z}_\rho &= \left|\{\sigma \in \ker \boldsymbol{A} : \rho_\sigma = \rho\}\right| && (\rho \in \mathfrak{P}_q),\\
\mathcal{Z}_\varepsilon &= \sum_{\rho\in\mathfrak{P}_q(\varepsilon)} \mathcal{Z}_\rho && (\varepsilon \ge 0),\\
\mathcal{Z}_{\varepsilon,\varepsilon'} &= \mathcal{Z}_{\varepsilon'} - \mathcal{Z}_\varepsilon && (\varepsilon, \varepsilon' \ge 0).
\end{aligned}$$

$\mathfrak{P}_q(\varepsilon)$ can be interpreted as nearly equitable frequency vectors; $\mathcal{Z}_\rho$ is the number of kernel vectors whose frequency vectors match $\rho \in \mathfrak{P}_q$; $\mathcal{Z}_\varepsilon$ is the sum of the number of all the kernel vectors whose frequency vectors are nearly equitable; $\mathcal{Z}_{\varepsilon,\varepsilon'}$ denotes the gap in the numbers when the allowed error changes.

Here is another helpful lemma.

Lemma 3.4.12 ([27, Lemma 7.2]). *For any fixed $\varepsilon > 0$ for large enough $\omega = \omega(\varepsilon) > 1$ w.h.p. we have* $\mathbb{E}\left[\mathcal{Z}_{\omega n^{-1/2},\varepsilon} \mid \mathfrak{A}\right] < \varepsilon q^{n-\boldsymbol{m}}$.

The proof of Lemma 3.4.12 involves an expansion to the second order of the optimisation problem (1.3.9) around the equitable solution, similar to previous work on k-XORSAT (see [7, 11, 38]).

With the particular terms we have defined, it is easy to write the version of a local limit theorem we use in [27], distinct from the version in [35]. We continue to denote by $\boldsymbol{\sigma} \in \mathbb{F}_q^n$ a uniformly random assignment and by $\boldsymbol{I}_{q-1}$ the $(q-1)\times(q-1)$-identity matrix. Recall ρ_σ from (3.4.7) and also consider $\hat{\rho} = (\rho(s))_{s\in\mathbb{F}_q^*}$. The following claim determines the distribution of $\rho_{\boldsymbol{\sigma}}$. Let $\bar{\rho} = q^{-1}\boldsymbol{\Delta}\mathbb{1}_{q-1}$.

Claim 3.4.13 ([27, Claim 7.16])**.** *Let $\mathscr{C}$ be the $(q-1)\times(q-1)$-matrix defined as*

$$\mathscr{C} = q^{-1}\boldsymbol{I}_{q-1} - q^{-2}\mathbb{1}_{(q-1)\times(q-1)}.$$

Then w.h.p. for all $\rho \in \mathfrak{P}_q$ we have

$$\mathbb{P}\left[\rho_{\boldsymbol{\sigma}} = \rho \mid \mathfrak{A}\right] = \frac{q^{q/2}\mathfrak{d}^{q-1}}{(2\mathbb{E}[\boldsymbol{d}^2]\pi n)^{(q-1)/2}}\exp\left(-\frac{(\hat{\rho}-\bar{\rho})^\top \mathscr{C}^{-1}(\hat{\rho}-\bar{\rho})}{2n\mathbb{E}[\boldsymbol{d}^2]}\right) + o(n^{(1-q)/2}).$$

For ρ that are within $O(n^{-1/2}\boldsymbol{\Delta})$ of the equitable solution, we need a more refined argument since the conceivable empirical distributions $\rho_{\boldsymbol{\sigma}}$ given that $\boldsymbol{\sigma} \in \ker \boldsymbol{A}$ are confined to a proper sub-lattice of $\mathbb{Z}^q$. The same is true for $\mathfrak{P}_q$ unless $\mathfrak{d} = 1$. Hence, we need to work out how these lattices intersect.

Moreover, for $\rho \in \mathfrak{P}_q$ we need to calculate the number of assignments σ such that $\rho_\sigma = \rho$ as well as the probability that such an assignment satisfies all $\boldsymbol{m}$ equations. By way of Proposition 3.4.5 and meticulous steps that involve Bayes' rule as well as Claim 3.4.13, we deal with this complication to prove the following lemma.

Lemma 3.4.14 ([27, Lemma 7.2])**.** *For any $\varepsilon > 0$ for large enough $\omega = \omega(\varepsilon) > 1$ we have $\mathbb{E}[\mathcal{Z}_{\omega n^{-1/2}} \mid \mathfrak{A}] \leq (1+\varepsilon)q^{n-\boldsymbol{m}}$ w.h.p.*

Finally, by way of Fact 3.4.11, Lemma 3.4.12 and Lemma 3.4.14, Proposition 3.4.6 follows. Proofs of Lemma 3.4.12 and Lemma 3.4.14 are laid out in [[27, Section 7]] and proof of Claim 3.4.13 is given in [[27, Appendix]].

4 List of Publications and Author's Contribution

4.1 The Number of Satisfying Assignments of Random 2-SAT Formulas

A joint work with D. Achlioptas, A. Coja-Oghlan, M. Hahn-Klimroth, N. Müller, M. Penschuck, and G. Zhou. The title of the Arxiv version is *The random 2-SAT partition function* [2]. The journal version [3] was renamed as above and includes a few minor changes.

We prove a long standing conjecture about a random constrains satisfiability problem called 2-SAT. Specifically, the number of solutions for a random 2-SAT has been predicted to be related to a functional evaluated at the marginal probability resulting from *Belief Propagation* (BP) recursion. This paper is published in *Random Structures and Algorithms* on 17.01.2021 [3].

Author's contribution: JHL worked on showing that the log-likelihood function which succinctly contains the BP update function is a contraction; worked on coming up with the extremal conditions on the leaves to bias the marginal distribution at the root to the extremes; worked on showing some bounded probabilities and bounded conditions regarding the leaves at an arbitrary distance away.

4.2 Warning Propagation: Stability and Subcriticality

A joint work with O. Cooley, J.B. Ravelomanana.

We consider a discrete message passing algorithm called *Warning Propagation* (WP). In particular, we analyze WP on random graphs in a general setting with diverse applications in mind. We show WP converges rapidly on random graphs by reducing the analysis to WP on a multi-type Galton Watson tree. This paper is submitted to a journal and is in the review process [32].

Author's contribution: JHL worked on making reasonable assumptions for the general random graph model to have in order for WP to be successful; worked on making contiguous graph models as well as local tree structure to run WP on and showing the convergence is fast; worked on showing subcritical changes after a bounded number of rounds.

4.3 The Sparse Parity Matrix

A joint work with A. Coja-Oghlan, O. Cooley, M. Kang, and J.B. Ravelomanana.

We study a square matrix with each entry being a Bernoulli distribution with $p = d/n, d > 0$. We prove a particular threshold $d = \mathrm{e}$ at which two behaviors of the matrix change in an unusual way. One regards the *fraction of frozen variables* $f(\boldsymbol{A})$ and the other regards *replica symmetry*. This paper was accepted and presented at the Symposium of Discrete Algorithms (SODA) conference in January 2022. It is also submitted to a journal and in the review process [24].

Author's contribution: JHL worked on showing that $f(\boldsymbol{A})$ converges to the fixed points of a certain function that comes from the local structure of the graph that represents $\boldsymbol{A}$; worked on warning propagation analysis on the bipartite graph to show WP correctly identifies the variable categories with high probability; worked on showing the unstable fixed point is not a feasible value for $f(\boldsymbol{A})$; worked on showing the structure of the minor matrix.

4.4 The Full Rank Condition for Sparse Random Matrices

A joint work with A. Coja-Oghlan, P. Gao, M. Hahn-Klimroth, N. Müller, M. Rolvien.

We provide a sufficient condition for a sparse random matrix to be of full row rank. This condition is applied to matrices over finite fields as well as $\{0,1\}$ matrix over rationals. This paper was submitted to a journal and is in the review process [27].

Author's contribution: JHL worked on examples to signify the main result; worked on the variational formula that comes as an upper bound of the nullity of a perturbed matrix and showing the maximum still lies at 0; worked on the various bases of the module generated by the frequency vectors related to the kernel of $\boldsymbol{A}$ and on the change of bases matrix.

5 Zusammenfassung

Vor etwa 50 Jahren interessierten sich Physiker für ein Objekt, das sie *Spinglas* nannten. Im Gegensatz zum üblichen Verhalten von Partikeln, die sich in die gleiche Richtung ausrichten (Ferromagnetismus) oder sich in unterschiedliche Richtungen ausrichten (Antiferromagnetismus), fanden Physiker heraus, dass ein Spinglas beide Typen aufweist und somit nicht nur in eine der beiden Kategorien fällt. Mit anderen Worten, wir stellen uns vor, dass jedes Teilchen eine Orientierung (Spins) hat, sagen wir $\{\pm 1\}$. Zwischen zwei Teilchen gibt es eine Wechselwirkungsenergie und ein Spinglas weist sowohl positive als auch negative Wechselwirkungsenergien auf. Es ist schwierig, einen Besetzung von Spins zu finden, der die gesamte Wechselwirkungsenergie minimiert. Dies war der Beginn der Theorie des Spinglases [59]. Obwohl ein Spin-Glas als physikalisches Objekt nutzlos ist, zeigten frühe Studien, dass es ein hilfreiches Modell ist, um ein allgemeines ungeordnetes System [61] zu untersuchen. Die von ihnen entwickelten Methoden namens Cavity Method und Replikasymmetrie befassten sich mit dem ungeordneten System eines Spinglases und den Änderungen im makroskopischen Verhalten des Objekts. Dies nennt man *Phasenübergänge*. Solche Methoden hatten große Auswirkungen auf andere Wissenschaftsdisziplinen, insbesondere Informationstheorie, Informatik und Mathematik.

Als mathematische Erfindung von Erdös und Rényiwurde die Theorie der Zufallsgraphen auch zu einem integralen Spielplatz der Mathematik und Physik. Sei V die Menge der Knoten. Kanten sind gemäß der Bernoulli-Verteilung zufällig zwischen Knoten vorhanden. Dies wird als ER-Graph bezeichnet. Die Zufälligkeit hat die Idee vorangetrieben, Eigenschaften zu beweisen, indem man einen Wahrscheinlichkeitsraum schafft und beweist, dass solche Eigenschaften existieren. Sie bewiesen auch das Vorhandensein von Phasenübergängen verschiedener Eigenschaften in diversen Graphenmodellen. Mathematiker und Physiker gleichermaßen nutzten die vorhandenen Ideen des anderen, um in den entsprechenden Disziplinen Fortschritte zu machen.

Eine besondere Art von Problemen, an denen beide Parteien interessiert sind, sind *Probleme der Erfüllbarkeit von Einschränkungen*. Ein Constraint-Satisfaction-Problem (CSP) besteht aus n-Variablen, $x_1 -, \cdots -, x_n$- und m-Constraints $a_1, \ldots, a_m$. Jede Bedingung ist mit einer Menge von Variablen verbunden und erlegt jeder verbundenen Variablen eine bestimmte Bedingung (z. B. einen *Spin*) auf. Das Ziel ist es, eine Konfiguration von Spins für $\{x_1\}_{i\in[n]}$ zu finden, die alle Bedingungen erfüllt. Eine Möglichkeit, die Wechselwirkungen zwischen Variablen gemäß den Einschränkungen auszudrücken, ist das Faktorgraphmodell. Ein Faktorgraph drückt die Wechselwirkungen von Teilchen in einer Konfiguration durch *Faktoren* benachbarter Teilchen aus [54]. Sei Ω eine endliche Menge von Spins. Sei $G = (V, F)$ der bipartite Graph indem V die Menge der n Variablen des Systems und F

die Menge der Faktoren (Constraints) bezeichnet. Wie im ER-Graph sind zufällige Kanten zwischen einer Variablen und einem Faktor vorhanden. Wenn zwischen $v \in V$ und $a \in F$ eine Kante existiert, nennen wir sie Nachbarn. Für $x \in V \cup F$, ∂x bezeichne die Knoten, die Nachbarn von x sind. Der Faktorgraph G benötigt eine weitere Komponente, eine Gewichtsfunktion $\psi_a : \Omega^{\partial a} \to (0,\infty)$. Bei einer Konfiguration $\sigma \in \Omega^v$ bezeichne $\sigma_{\partial a}$ die Spins der Variablen in ∂a. Dann hat G eine Boltzmann-Wahrscheinlichkeitsverteilung auf dem Konfigurationsraum Ω^V: ,

$$\begin{aligned} \mu_G(\sigma) &= \psi_G(\sigma)/Z_G \qquad \text{für } \sigma \in \Omega^V, \text{ wobei} \\ \psi_G(\sigma) &= \prod_{a\in F} \psi_a(\sigma_{\partial a}), \qquad Z_G = \sum_{\sigma\in\Omega^V} \psi_G(\sigma), \end{aligned}$$

Hier ist Z_G die Partitionsfunktion des Systems. In der Physik hat $\psi_a(\sigma_{\partial a})$ normalerweise die Form von $\exp\left[-\beta E_a(\sigma_{\partial a})\right]$ wobei $\beta = 1/T \geq 0$ der Kehrwert der Temperatur ist und $E_a(\sigma_{\partial a})$. Der inverse Temperaturterm β wirkt als Straf-Funktion. Anders ausgedrückt ergibt sich eine geringere Wahrscheinlichkeit für eine höhere Energie $E_a(\sigma_{\partial a}) \geq 0$.

Anstatt sich CSP direkt zu nähern, kamen Forscher in den 1980er Jahren auf die Idee zufällige CSP (rCSP) zu betrachten, um einen effizienten Algorithmus zur Lösung von CSPs [43] zu entwickeln. Unter zahlreichen *Message-Passing-Algorithmen* basierend auf der Cavity-Methode konzentrieren wir uns hier auf zwei dieser Algorithmen, Belief Propagation (BP) und Warning Propagation (WP). Wir werden nun das Faktorgraphmodell verwenden, um den zufälligen 2-SAT zu definieren, und BP verwenden, um eins der Hauptresultate zu erhalten.

Jetzt konzentrieren wir uns auf das 2-SAT-Problem. Es gibt n Variablenknoten und $\boldsymbol{m} = \mathrm{Po}(dn/2)$ viele Prüfknoten, somit hat jede Variable die Gradverteilung von $\mathrm{Po}(d)$. Jede Variable bekommt einen Spin in $\Omega = \{\pm 1\}$. Für jedes $a \in F$ hat es zwei unterschiedliche Nachbarn $x_1, x_2 \in V$ und es wählt unter 4 verschiedenen Beziehungen mit den Literalen aus, sodass es $4n(n-1)$ viele Optionen von Paaren zur Auswahl hat . Dann ist eine Instanz von 2-SAT eine Konjunktion von Disjunktionen

$$\boldsymbol{\Phi} = a_1 \wedge \cdots \wedge a_{\boldsymbol{m}}.$$

Wenn $\boldsymbol{m}$ zunimmt, ist natürlich die Wahrscheinlichkeit geringer, dass $\boldsymbol{\Phi}$ erfüllt wird, daher war der Begriff des Phasenübergangs bei steigendem $\boldsymbol{m}$ ein wichtiges Barometer bei der Untersuchung von k-SAT und anderen rCSP . Das zufällige 2-SAT-Problem war das erste rCSP, dessen Erfüllbarkeitsschwelle 1992 aufgedeckt wurde [46, 75]. Zahlreiche Fragen zu 2-SAT wurden beantwortet [19, 20, 33, 34, 56] . Das Finde der Anzahl von Lösungen eines zufälligen 2-SAT war jedoch noch offen. Insbesondere Monasson und Zecchina untersuchten dieses Problem. Anstatt die Zustandssumme $Z(\boldsymbol{\Phi})$ direkt zu berechnen, stellten sie eine Vermutung über den normalisierten Logarithmus von $Z(\boldsymbol{\Phi})$, der als *freie Energiedichte* bezeichnet wird, auf. In [3] haben wir diese Vermutung bewiesen, die wir nun als Satz formulieren.

Seien $\boldsymbol{d}^+, \boldsymbol{d}^- = \mathrm{Po}(d/2)$ die Verteilungen der Anzahl von 'wahren' bzw. 'falschen' Nachrichten, die von

den Nachbarn einer uniform zufällig gewählten Variablen kommen. Weiterhin seien $\boldsymbol{\mu}_{\pi,1}, \boldsymbol{\mu}_{\pi,2}, \ldots$ Zufallsvariablen mit Verteilung π, alle voneinander unabhängig, und $\hat{\pi}$ sei die Verteilung der Zufallsvariable [3, Eq. 1.1]

$$\frac{\prod_{i=1}^{\boldsymbol{d}^-} \boldsymbol{\mu}_{\pi,i}}{\prod_{i=1}^{\boldsymbol{d}^-} \boldsymbol{\mu}_{\pi,i} + \prod_{i=1}^{\boldsymbol{d}^+} \boldsymbol{\mu}_{\pi,i+\boldsymbol{d}^-}} \in (0,1).$$

Dies ist der BP-Operator, der π (die Verteilung von Nachrichten) aktualisiert, die eine Variable empfängt. Sei $\delta_{1/2} \in \mathscr{P}(0,1)$ das Atom bei $1/2$ und wir schreiben $\mathrm{BP}_d^\ell(\cdot)$ für die ℓ-fache Rekursion des Operators BP_d.

Theorem 5.0.1 ([3, Theorem 1.1])**.** *Für $d < 2$ existiert die Grenze $\pi_d = \lim_{\ell\to\infty} \mathrm{BP}_d^\ell(\delta_{1/2})$ und*

$$\lim_{n\to\infty} \frac{1}{n} \log Z(\boldsymbol{\Phi}) = \mathbb{E}\left[\log\left(\prod_{i=1}^{\boldsymbol{d}^-} \boldsymbol{\mu}_{\pi_d,i} + \prod_{i=1}^{\boldsymbol{d}^+} \boldsymbol{\mu}_{\pi_d,i+\boldsymbol{d}^-}\right) - \frac{d}{2}\log\left(1 - \boldsymbol{\mu}_{\pi_d,1}\boldsymbol{\mu}_{\pi_d,2}\right)\right] \quad \textit{in Wahrscheinlichkeit.} \tag{5.0.1}$$

Die rechte Seite von (5.0.1) heißt die *Bethe Free Entropie*. BP berechnet die marginale Wahrscheinlichkeit, dass eine Zufallsvariable einen Spin annimmt. Somit zeigen wir durch die BP-Rekursion, dass die Bethe-Free Entropie $\phi(\beta)$ die Anzahl der erfüllenden Lösungen für ein zufälliges 2-SAT-Problen angibt. Dass $\phi(\beta)$ die obere Schranke von $\frac{1}{n}\log Z(\Phi)$ scharf ist, wurde durch das sogenannte Interpolationsverfahren [44, 47, 71] bewiesen. Daher hebt unser Ergebnis die scharfe untere Grenze der Zahl der Lösungen hervor und beweist damit die Vermutung von Monasson und Zecchina [66]. Der Beweis beruht darauf, einen Fixpunkt einer stochastischen Gleichung zu finden und ihn auf die Bethe-Free-Entropie anzuwenden. Insbesondere der Fixpunkt ist eindeutig und passt zur Boltzmann-Verteilung. Diese Eigenschaft wird *Gibbs Uniqueness* genannt. Wir verwenden die Tatsache, dass $\boldsymbol{\Phi}$ die lokale Struktur eines Galton-Watson-Verzweigungsprozesses hat, und beweisen die Gibbs-Uniqueness, indem wir extreme Randbedingungen auf den Blättern konstruieren. Es beruht auch auf der schnellen Konvergenz der Fixpunktgleichung. Wir stellen auch fest, dass der Faktorgraph, damit BP erfolgreich ist, einem Galton-Watson-Verzweigungsprozess ähneln muss, sodass er keine Zyklen oder langen Korrelationen [60] enthält. Diese Bedingung hängt auch mit dem Begriff der Replikasymmetrie zusammen. Für Einzelheiten verweisen wir den Leser auf [3].

Nun wenden wir uns einem anderen Message-Passing-Algorithmus namens *Warning Propagation* zu. Während BP die Wahrscheinlichkeitsverteilungen der gerichteten Nachrichten aktualisiert, aktualisiert WP die Nachrichten (Spins) mit anderen Nachrichten als Reaktion auf die Nachrichten ihrer Nachbarn. Angenommen, wir haben eine Instanz von rCSP, Φ und G_Φ bezeichne seinen Faktorgraphen. Jede Kante ist mit zwei Nachrichten versehen, $\mu_{x\to a}$ und $\mu_{a\to x}$. Wenn wir jede Nachricht als boolesch initialisieren und WP ausführen, dann aktualisiert WP die Nachrichten mit einem anderen booleschen Wert gemäß den folgenden Warnungen [60, Section 14.3.3]. Für σ ein boolescher Wert,

- $\mu_{x\to a}(\sigma) = 1$ bedeutet *nach der Forderung der Constraints $b \in \partial x \backslash a$ soll x nicht den Wert σ annehmen.*

- $\mu_{x\to a}(\sigma) = 0$ bedeutet *je nach Forderung der Constraints $b \in \partial x \setminus a$ kann x den Wert annehmen σ.*

Natürlich müssen die Nachrichten nicht boolesch sein. Wir könnten WP auch auf ein Modell mit mehreren Knoten anwenden. Hier definieren wir WP in voller Allgemeinheit.

Gegeben sei ein Graph G, $\mu_{v\to w}, \mu_{w\to v}, vw \in E(G)$ seien die Nachrichten aus einer endlichen Menge Ω. Wir definieren $\mathscr{M}(G)$ als die Menge aller Vektoren $\left(\mu_{v\to w}\right)_{(v,w)\in V(G)^2 : vw\in E(G)} \in \Omega^{2|E(G)|}$ wobei $V(G)$ die Menge aller Knoten der beteiligten Typen ist. Um die Aktualisierungsfunktion für die Nachrichten zu definieren, sei für $d \in \mathbb{N}$ $\left(\!\binom{\Omega}{d}\!\right)$ die Menge aller d-arischen Multimenge mit Elementen aus Ω. [[32, Eq. 1.1]],

$$\varphi : \bigcup_{d\geq 0} \left(\!\binom{\Omega}{d}\!\right) \to \Omega$$

sei eine *Aktualisierungsregel*, die bei gegebener beliebiger Menge von Eingabenachrichten eine Ausgabenachricht bestimmt. Mit anderen Worten, wir definieren den WP-Operator auf G durch

$$\mathrm{WP}_G : \mathscr{M}(G) \to \mathscr{M}(G), \qquad \mu = \left(\mu_{v\to w}\right)_{vw} \mapsto \left(\varphi\left(\{\!\{\mu_{u\to v} : u \in \partial v \setminus w\}\!\}\right)\right)_{vw},$$

wobei $\{\!\{a_1, \ldots, a_r\}\!\}$ die Multimenge mit $a_1, \ldots, a_r \in \Omega$ bezeichnet. Um also eine gerichtete Nachricht zu aktualisieren, ignoriert WP das Ziel, während es auf alle anderen Nachbarn in einer ähnlichen Weise wie BP reagiert.

Hier ist ein Beispiel für WP. *Propagierung von Einheitsklauseln* (UCP) beginnt bei jeder Klausel mit einer Variablen in ihrem Nachbarn (*Einheitsklausel*). Wir können den Wert der Variablen entsprechend der Forderung der Klausel setzen, sodass die Klausel erfüllt ist. Durch das Anheften der Variablen wären andere Klauseln betroffen, die mit dieser Variablen verbunden sind. Die Klauseln, die durch den Wert der Variablen erfüllt werden, propagieren keinen Effekt, also werden sie gelöscht, aber jede Klausel, die nicht erfüllt wird, propagiert den Effekt, dass sie durch andere verbundene Variablen erfüllt werden müssen. UCP wird rekursiv angewendet. Irgendwann würde dieser Prozess aufhören, entweder mit einer leeren Menge oder mit Klauseln, die mindestens zwei Variablen enthalten. UCP wurde erfolgreich verwendet, um Ergebnisse zu k-SAT-Problemen zu erhalten [1, 45]. Andere bemerkenswerte Arbeiten wurden mit WP durchgeführt, insbesondere der Peeling-Prozess für den k-Kern [64, 73]).

Wie UCP zeigt, werden die Aktualisierungsregel, die Arten von Nachrichten und die Arten von Scheitelpunkten gemäß den speziellen Problemen bestimmt, mit denen sich WP beschäftigt. Andere bemerkenswerte Ansätze zur Analyse rekursiver Prozesse sind die Methoden der Differentialgleichungen [73, 86], Verzweigungsprozesse [77], Aufzählungsmethoden [25] und Geburts-Tod-Prozesse [50, 51].

Ähnlich wie in BP wäre es für WP hilfreich, wenn der rekursive Prozess nach einer begrenzten Anzahl von Rekursionen schnell zu einem festen Punkt konvergiert, um nützlich zu sein. Außerdem

sollten alle möglichen Änderungen, nachdem der Prozess den Fixpunkt erreicht hat, nicht zu einer makroskopischen Verhaltensänderung führen.

Die Hauptergebnisse von [32] erreichen diese Ziele, sodass WP auf verschiedene Modelle oder Zufallsgraphen angewendet werden kann(wie z.B. das ER binomiale Zufallsgraphenmodell $G(n,p)$, k-partite Graphen, zufällige reguläre Graphen, zufällige Graphen mit einer bestimmten Gradfolge, das stochastische Blockmodell und Faktorgraphen zufälliger Hypergraphen). Tatsächlich haben wir einige Kriterien für Annahmen für ein Zufallsgraphenmodell erarbeitet, sodass WP angewendet werden kann, um die Nachrichten zu einer schnellen Konvergenz zu bringen, sobald das zugrunde liegende Graph-Modell diese eigenschaften erfüllt. Einige der Hauptannahmen ähneln den Eigenschaften, auf die sich BP stützte. Die lokale Struktur eines Modells muss einem Galton-Watson-Baum mit mehreren Typen ähneln.

In gewisser Weise ist das Spiel von WP dasselbe wie in BP; wir wollen die Fixpunkte von WP finden und die Konvergenzrate kontrollieren. In der Tat zeigen wir, dass unser Fixpunkt nur eine Sammlung von Wahrscheinlichkeitsverteilungen auf Ω jeder Art von gerichteter Kante sein wird, so dass, wenn die Kinder eines Knotens v unabhängig von diesen Verteilungen Nachrichten an v senden, dann spiegelt die Nachricht von v an ihre Eltern auch die gleiche Verteilung von Nachrichten jedes Typs wider.

Aufgrund der allgemeinen Formulierung von k-Typen können die Verteilungen von Nachrichten zwischen Scheitelpunkten von k-Typen effizient als Matrix ausgedrückt werden. Ohne viele Details legen wir hier den Hauptsatz nieder.

Theorem 5.0.2 ([32, Theorem 1.3])**.** *Sei $\mathbb{G}$ ein zufälliges Graphenmodell, das [[**?**, Annahmen 2.10]]] und seien P, Q_0 Wahrscheinlichkeitsverteilungsmatrizen auf Ω, so dass P die stabile WP-Grenze von Q_0 ist. Dann existiert für jedes $\delta > 0$ $t_0 = t_0\left(\delta, \mathcal{Z}, \varphi, Q_0\right)$, sodass Folgendes gilt.*

Angenommen, $\mu^{(0)} \in \mathcal{M}\left(\mathbb{G}\right)$ ist eine Initialisierung gemäß Q_0. Dann gilt für alle $t \geq t_0$,

$$\sum_{v,w:vw\in E(\mathbb{G})} \mathbb{1}\left\{\mathbb{G}^t_{v\to w}\left(\mu^{(0)}\right) \neq \ wpf^{t_0}_{v\to w}\left(\mu^{(0)}\right)\right\} < \delta n$$

mit hoher Wahrscheinlichkeit.

Der Hauptsatz besagt, dass nach einer begrenzten Anzahl von Runden t_0 des Ausführens von WP von der anfänglichen Verteilung Q_0 die WP-Nachrichten unverändert bleiben, mit Ausnahme von höchstens δn vielen gerichteten Kanten .

Wir beweisen dieses Theorem, indem wir uns auf einige andere Graphmodelle stützen, die mit dem vorliegenden Modell verwandt sind, und auf denen WP ausgeführt wird. Danach beenden wir den Beweis, indem wir zeigen, dass die stabile Grenze existiert. Wir verweisen den Leser für Einzelheiten auf [32].

In [24] wenden wir das Ergebnis auf WP an, um ein Ergebnis über eine kombinatorische Zufallsmatrix zu beweisen. Mit kombinatorisch meinen wir, dass die Einträge der Matrix aus einer diskreten

Wahrscheinlichkeitsverteilung gezogen werden. Sei $\boldsymbol{A} = \boldsymbol{A}(n, p)$ eine quadratische Matrix, wobei jeder Eintrag eine Bernoulli-Verteilung mit $p = d/n, d > 0$ hat. Hier ist d der Parameter.

Dieses Modell ist eng mit CSP und dem Inferenzproblem verbunden, da unsere Hauptergebnisse für beide Fragen relevant sind. Sei $\boldsymbol{y}$ ein Zufallsvektor im Spaltenraum von $\boldsymbol{A}$ und sei $\boldsymbol{A}x = \boldsymbol{y}$. Natürlich wäre es das Ziel, die Lösungsmenge zu finden. Diese Frage ähnelt der eines rCSP namens k-XORSAT. Eine zufällige k-XORSAT-Instanz besteht aus linearen $\boldsymbol{m}$-Gleichungen in $\mathbb{F}_2$ über n-Variablen. Jede Gleichung erhält k Variablen und ist entweder gleich 0 oder 1. Entsprechend ist es ein lineares System $\boldsymbol{A}x = \boldsymbol{y} \mod 2$ in dem $\boldsymbol{A} \in \mathbb{M}_{\boldsymbol{m}\times n}(\mathbb{F}_2)$ eine Matrix ist, in der jede Zeile k Nicht-Null-Einträge und $b \in \mathbb{F}_2^n$ enthält. Es ist bekannt, dass k-XORSAT eine scharfe Erfüllbarkeitsschwelle hat. Mit zunehmendem Verhältnis m/n fanden Dubois und Mandler sowie Pittel und Sorkin die Schwellenwerte für verschiedene Modelle von k-XORSAT [38, 72]. Überraschend ist, dass diese Schwelle eintritt, bevor m/n eins erreicht, insbesondere dann, wenn eine lineare Anzahl von Variablen *einfrieren*, also in allen Lösungen die gleichen Werte annehmen.

Lassen Sie uns zusätzlich zu den eingefrorenen Variablen den *Anteil der eingefrorenen Variablen* definieren [[24, Section 1.2]]

$$f(\boldsymbol{A}) = |\{i \in [n] : \forall x \in \ker \boldsymbol{A} : x_i = 0\}| / n.$$

Wir können diese Frage auch als Inferenzproblem betrachten. Sei $\hat{\boldsymbol{x}} \in \mathbb{F}_2^n$ ein Zufallsvektor (Grundwahrheit) und $\boldsymbol{y}$ die verrauschte Beobachtung von $\hat{\boldsymbol{x}}$ über $\boldsymbol{y} = \boldsymbol{A}\hat{\boldsymbol{x}}$. Wir können fragen, wie gut wir $\hat{\boldsymbol{x}}$ wiederherstellen können, wenn $\boldsymbol{A}$ und $\boldsymbol{y}$ gegeben sind. Hier sehen wir den Zusammenhang zwischen CSP und dem Inferenzproblem, da die A-posteriori-Verteilung eines zufälligen festen Vektors x, der der Grundwahrheit entspricht, die gleichmäßige Verteilung zwischen den Lösungen ist [24, Eq. 1.3]

$$\mathbb{P}\left[\hat{\boldsymbol{x}} = x \mid \boldsymbol{A}, \boldsymbol{y}\right] = \frac{\mathbb{1}\{\boldsymbol{A}x = \boldsymbol{y}\}}{|\ker \boldsymbol{A}|}, \qquad (x \in \mathbb{F}_2^n). \tag{5.0.2}$$

Wir können auch darüber nachdenken, welchen Bruchteil der Variablen in $\hat{\boldsymbol{x}}$ wir mit einem zufälligen Vektor x abgleichen können. Wir definieren diesen Bruchteil als *overlap*, [[24, Section 1.3]]

$$R(\boldsymbol{x}, \hat{\boldsymbol{x}}) = \frac{1}{n}\sum_{i=1}^{n} \mathbb{1}\{\boldsymbol{x}_i = \hat{\boldsymbol{x}}_i\}.$$

Der erwartete Wert der bedingten Überlappung bei $\boldsymbol{A}, \boldsymbol{y}$ ist das Ziel. Der Durchschnitt der bedingten Überlappung ist ein von $\boldsymbol{y}$ unabhängiger Wert, gegeben durch [[24, Section 1.3]]

$$\bar{R}(\boldsymbol{A}) = \mathbb{E}\left[R(\boldsymbol{x}, \hat{\boldsymbol{x}}) \mid \boldsymbol{A}, \boldsymbol{y}\right] = \frac{1}{|\ker \boldsymbol{A}|^2}\sum_{x, x' \in \ker \boldsymbol{A}} R(x, x').$$

In diesem Zusammenhang können wir nur wenige Worte zur Replikatsymmetrie bezüglich der Überlappung verlieren. Wir sagen, dass das lineare System abbildsymmetrisch ist, wenn die Überlappung

zu einem einzigen Wert konvergiert, angesichts der Unordnung, die in diesem Fall $\boldsymbol{A}, \boldsymbol{y}$ [90] ist,

$$\lim_{n\to\infty} \mathbb{E}\left[\left|R(\boldsymbol{x},\hat{\boldsymbol{x}}) - \bar{R}(\boldsymbol{A})\right|\right] \to 0.$$

Viele Inferenzprobleme zeigen, dass die Überlappung unabhängig von der gegebenen Bedingung $\boldsymbol{A}, \boldsymbol{y}$ [13] gegen einen deterministischen Wert konvergiert. Wir nennen dies *Strong Replica Symmetry* und drücke es aus als

$$\lim_{n\to\infty} \mathbb{E}\left[\left|R(\boldsymbol{x},\hat{\boldsymbol{x}}) - \mathbb{E}\left[\bar{R}(\boldsymbol{A})\right]\right|\right] \to 0.$$

Unser Problem mit $\boldsymbol{A}(n,p)$ gehört zu dem seltenen Fall, wo etwas stark replikationssymmetrisch ist, wenn $0 < d <$ e, aber nur replikationssymmetrisch, wenn $d >$ e.

Wir geben nun die wichtigsten Ergebnisse zu $f(\boldsymbol{A})$ und $R(\boldsymbol{x},\hat{\boldsymbol{x}})$ an. Eine gleichmäßig zufällig gewählte Variable v hat etwa eine Wahrscheinlichkeit von $f(\boldsymbol{A})$, eingefroren zu werden. Die lokale Baumstruktur von G, die $\boldsymbol{A}$ darstellt, würde das Einfrieren der Wurzel v erfordern, dass v mindestens eine Klausel hat, deren untergeordnete Variablen eingefroren sind. Dann enthält die folgende Gleichung diese Information [[24, Eq. 1.1]]

$$\phi_d : [0,1][0,1], \qquad \alpha \mapsto 1 - \exp\left(-d\exp\left(-d(1-\alpha)\right)\right); \tag{5.0.3}$$

das heißt, die Fixpunkte von 5.0.3 sind die plausiblen Brüche eingefrorener Variablen. Es stellt sich heraus, dass es möglicherweise drei Fixpunkte in ϕ gibt, von denen zwei stabile Fixpunkte sind, die mit $\alpha_* \le \alpha^*$ bezeichnet sind, und ein instabiler Fixpunkt α_0 und $0 \le alpha_* \le \alpha_0 \le \alpha^* \le 1$.

Hier ist das erste Hauptergebnis zu $f(\boldsymbol{A})$.

Theorem 5.0.3 ([24, Theorem 1.1])**.**

- *Für $d \le$ e hat die Funktion ϕ_d einen eindeutigen Fixpunkt und*

$$\lim_{n\to\infty} f(\boldsymbol{A}) = \alpha_* = \alpha^* \qquad \textit{in Wahrscheinlichkeit.}$$

- *Für $d >$ e haben wir $\alpha_* < \alpha^*$ und für alle $\varepsilon > 0$,*

$$\lim_{n\to\infty} \mathbb{P}\left[|f(\boldsymbol{A}) - \alpha_*| < \varepsilon\right] = \lim_{n\to\infty} \mathbb{P}\left[|f(\boldsymbol{A}) - \alpha^*| < \varepsilon\right] = \frac{1}{2}.$$

Somit durchläuft $f(\boldsymbol{A})$ den Phasenübergang bei $d =$ e, aber sein Verhalten in $d >$ e ist unentschieden und nimmt mit gleicher Wahrscheinlichkeit $1/2$ entweder α_* oder α^* an. Das nächste Hauptergebnis zeigt ein ähnliches unentschlossenes Verhalten bezüglich der bedingten Überlappung.

Theorem 5.0.4 ([24, Theorem 1.2])**.**

- *Wenn $d <$ e dann gilt $\lim_{n\to\infty} R(\boldsymbol{x},\hat{\boldsymbol{x}}) = (1+\alpha_*)/2$ in Wahrscheinlichkeit.*

- *Für alle* $d > \mathrm{e}$ *gilt* $\lim_{n\to\infty} \mathbb{E}\left|R(\boldsymbol{x},\hat{\boldsymbol{x}}) - \bar{R}(\boldsymbol{A})\right| = 0$ *mit*

$$\lim_{n\to\infty} \mathbb{P}\left[\left|\bar{R}(\boldsymbol{A}) - \frac{1+\alpha_*}{2}\right| < \varepsilon\right] = \lim_{n\to\infty} \mathbb{P}\left[\left|\bar{R}(\boldsymbol{A}) - \frac{1+\alpha^*}{2}\right| < \varepsilon\right] = \frac{1}{2} \qquad \textit{für alle } \varepsilon > 0.$$

Auch hier erfährt der Erwartungswert der bedingten Überlappung einen Phasenübergang bei $d = \mathrm{e}$ mit ähnlichem unentschlossenem Verhalten bei $d > \mathrm{e}$.

Beweise für die beiden Hauptergebnisse kommen in drei Schritten. Zunächst zeigen wir, dass sich $f(\boldsymbol{A})$ auf die Fixpunkte von ϕ_d konzentriert, entweder auf α_*, α^* oder α_0. Zweitens stellen wir fest, dass der instabile Fixpunkt α_0 ein unwahrscheinliches Ergebnis ist. Schließlich schließen wir, dass α_* und α^* gleich wahrscheinlich sind. Der erste und der zweite Schritt verwenden mehrfach das WP-Theorem, das wir in [32] bewiesen haben. Besonders der Multityp WP ist hier nützlich, da wir zwei Arten von Knoten haben, von denen einer Klauseln und der andere Variablen sind. Ebenfalls nützlich ist die Tatsache, dass sich dieses Modell in einem konstanten Schwebezustand befindet, sodass wir nicht alle Variablen als eingefroren oder nicht eingefroren initialisieren können. Daher erstellen wir einen dritten Nachrichtentyp namens *slush* und initialisieren alle gerichteten Nachrichten als slush. Indem wir verschiedene Versionen von WP auf der lokalen baumähnlichen Struktur ausführen, können wir zeigen, dass $f(\boldsymbol{A})$ zu $\alpha_*, \alpha_0, \alpha^*$ konvergiert und dass α_0 ein unwahrscheinlicher Wert ist. Ein weiteres wichtiges Element, um den zweiten Teil zu zeigen, ist ein Satz von [26], den wir hier angeben. Dazu bedarf es einiger Einarbeitung, da dieser Satz auch in der letzten Arbeit [27] verwendet wird. Das folgende Setup folgt genau [27]. Seien $\boldsymbol{d} \geq 0$, $\boldsymbol{k} \geq 3$ unabhängige ganzzahlige Zufallsvariablen, sodass $\mathbb{E}[\boldsymbol{d}^{2+\eta}] + \mathbb{E}\left[\boldsymbol{k}^{2+\eta}\right] < \infty$ für ein beliebig kleines $\eta > 0$. Seien $(\boldsymbol{d}_i, \boldsymbol{k}_i)_{i\geq 1}$ unabhängige Kopien von $(\boldsymbol{d}, \boldsymbol{k})$ und setze $d = \mathbb{E}[\boldsymbol{d}], k = \mathbb{E}[\boldsymbol{k}]$. Außerdem sei $\mathfrak{d} = \gcd\{\mathrm{supp}(\boldsymbol{d})\}$ und $\mathfrak{k} = \gcd\{\mathrm{supp}(\boldsymbol{k})\}$. Sei n ganzzahlig teilbar durch $\mathfrak{k}$ und $\boldsymbol{m} = \mathrm{Po}(dn/k)$, unabhängig von $(\boldsymbol{d}_i, \boldsymbol{k}_i)_i$. Es kann gezeigt werden, dass die Gradsummen übereinstimmen [[26, Eq. 1.1]],

$$\sum_{i=1}^{n} \boldsymbol{d}_i = \sum_{j=1}^{\boldsymbol{m}} \boldsymbol{k}_j,$$

mit Wahrscheinlichkeit mindestens $\Omega(n^{-1/2})$ [26, Proposition 1.7]. Unter der Voraussetzung, dass die Gradsummen übereinstimmen, bezeichne $\mathbb{G} = \mathbb{G}_n(\boldsymbol{d}, \boldsymbol{k})$ einen einfachen zufälligen bipartiten Graphen auf einer Menge von Klauseln $\{a_1 \ldots, a_{\boldsymbol{m}}\}$ und ein Satz von Variablen $\{x_1, \ldots, x_n\}$, so dass $\boldsymbol{k}_i$ den Grad von a_i und $\boldsymbol{d}_j$ den Grad von x_j bezeichnet, wobei $\boldsymbol{k}_i$ und $\boldsymbol{d}_j$ sind jeweils unabhängige Kopien von $\boldsymbol{k}$ und $\boldsymbol{d}$. Die Kanten von $\mathbb{G}$ bezeichnen die Positionen der Nicht-Null-Elemente von $\mathbb{A} = \mathbb{A}(G)$, die endliche Körperelemente oder rationale Zahlen sein können. Für diese Diskussion sei das Feld $\mathbb{F}_q$, wobei $q = p^\ell$ für p prim ist. Sei $\boldsymbol{\chi}$ eine Zufallsvariable in $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$. Lassen Sie $\mathrm{rk}(\mathbb{A})$ und $\mathrm{nul}(\mathbb{A})$ den Rang bzw. die Dimension des Kerns von $\mathbb{A}$ bezeichnen.

Wir bezeichnen die wahrscheinlichkeitserzeugenden Funktionen von $\boldsymbol{d}$ und $\boldsymbol{k}$ als $D(x)$ bzw. $K(x)$.

Definiere [[26, Eq. 1.2]]

$$\Phi : [0,1] \to \mathbb{R}, \qquad \alpha \mapsto D\left(1 - K'(\alpha)/k\right) - \frac{d}{k}\left(1 - K(\alpha) - (1-\alpha)K'(\alpha)\right).$$

Der folgende Satz bestimmt den *normalisierten* Rang von $\mathbb{A}$:

Theorem 5.0.5 ([26, Theorem 1.1])**.**

$$\frac{\mathrm{rk}(\mathbb{A})}{n} \xrightarrow{\mathbb{P}} 1 - \max_{\alpha \in [0,1]} \Phi(\alpha) \qquad \text{as } n \to \infty. \tag{5.0.4}$$

Basierend auf diesem Theorem können Rang und Kern-Dimemsion nur durch den Maximalwert von $\Phi(\alpha)$ erreicht werden. Wir zeigen, dass der instabile Fixpunkt $f(\boldsymbol{A})$ eine viel geringere Lösung des linearen Systems erzeugt, sodass der Satz nicht mehr gilt.

Der dritte Punkt beruht auf der Symmetrie des Modells und der Momentenberechnung. Die Slush-Minor-Matrix, die WP erzeugt, trägt das Ergebnis etwa mit gleicher Wahrscheinlichkeit. Wir verweisen den Leser auf [24].

Theorem 5.0.5 ist die Hauptbedingung für die vierte Arbeit der Dissertation [27]. Wir geben jetzt das Hauptergebnis an.

Theorem 5.0.6 ([27, Theorem 1.1])**.** *Wenn q und $\mathfrak{d}$ Teilerfremde sind und*

$$\Phi(z) < \Phi(0) \qquad \text{für alle } 0 < z \leq 1, \tag{5.0.5}$$

dann hat $\mathbb{A}$ vollen Zeilenrang über $\mathbb{F}_q$ w.h.p.

Das Theorem liefert eine bemerkenswert einfache Bedingung, um zu testen, ob ein Zufallsmatrixmodell vollen Rang hat oder nicht. Lassen Sie uns betonen, dass (5.0.4) nicht garantiert, dass $\mathbb{A}$ den vollen Zeilenrang mit hoher Wahrscheinlichkeit hat, selbst wenn (5.0.5) erfüllt ist. Aufgrund der Normalisierung auf der linken Seite impliziert (5.0.4) nur, dass $\mathrm{rk}(\mathbb{A}) = \boldsymbol{m} - o(n)$ mit hoher Wahrscheinlichkeit, während uns immer noch der Fehler $o(n)$ bleibt. Für den Fall, dass (5.0.5) erfüllt ist, verbessert sich Theorem 5.0.6 gegenüber der asymptotischen Schätzung (5.0.4) enorm.

Um sie zu beweisen, müssen zwei Relationen festgestellt werden, die wiederum das Hauptergebnis beweisen.

Dieser Abschnitt folgt genau [27, Section 2.1]. In Bezug auf rCSP entspricht die Bedingung des vollen Rangs einer Lösung, sodass dieses Problem mit dem Finden der Erfüllbarkeitsschwelle verknüpft ist. Die Methode des zweiten Moments ist eine beliebte Wahl, um die Erfüllbarkeitsschwelle für rCSP [6, 7] zu untersuchen. Es läuft darauf hinaus, den vollen Rangschwellenwert über $\mathbb{F}_2$ zu finden.

Allerdings stieß die Methode an ihre Grenzen, als kompliziertere Modelle getestet wurden [38]. Das Problem tritt auf, wenn das zweite Moment nicht mit dem Quadrat des ersten Moments vergleichbar ist, wodurch die Kraft der Chebyshev-Ungleichung aufgehoben wird.

Diese missliche Lage hebt den Unterschied zwischen *annealed*- und *quenched*-Momentberechnungen hervor. Bezüglich der Anzahl $\boldsymbol{Z}$ der Lösungen des linearen Gleichungssystems bedeuten *annealed*- und *quenched*, welche Aktion zuerst ausgeführt wird, log oder $\mathbb{E}$. Da $\boldsymbol{Z}$ ein potenziell exponentieller

Wert ist, ist es oft möglich, dass

$$\log \mathbb{E}[\boldsymbol{Z}] \not\asymp \mathbb{E}\big[\log \boldsymbol{Z}\big], \tag{5.0.6}$$

die wiederum die Methode des zweiten Moments in diesem aktuellen Zustand unbrauchbar machen. Die linke Seite von (5.0.6) heißt annealed Moment und die r.h.s. wird als quenched Moment bezeichnet (siehe [61] für einen tieferen Einblick in diese verschiedenen Momente). Unter dem Strich ist das annealed Moment zu anfällig für große Abweichungseffekte, wenn einige unwahrscheinliche Ereignisse den Momentwert nach oben treiben. Daher wählen wir das quenched Moment mit *equitable* oder *balanced* Lösungen. Damit meinen wir einen Vektor, der ungefähr die gleiche Menge von jedem der $\mathbb{F}_q^*$-Elemente unter den Einträgen aufnimmt. Diese Beweisstrategie verallgemeinert die in [11, 26] entwickelten Methoden.

Lassen Sie uns nun eine Prämisse festlegen. Das von uns betrachtete Optimierungsproblem besteht aus zwei Sätzen von Vektoren; erstens in Form von Variablen $(z_i)_{i\in\operatorname{supp}\boldsymbol{d}}$, die sich über den Raum $\mathscr{P}(\mathbb{F}_q)$ von Wahrscheinlichkeitsverteilungen auf $\mathbb{F}_q$ erstrecken, und der andere Satz von Variablen $(\hat{z}_{\chi_1,\dots,\chi_\ell})_{\ell\in\operatorname{supp}\boldsymbol{k},\chi_1,\dots,\chi_\ell\in\operatorname{supp}\boldsymbol{\chi}}$, solche, die über Wahrscheinlichkeitsverteilungen von Lösungen der linearen Gleichung $\chi_1\sigma_1+\cdots+\chi_\ell\sigma_\ell=0$ reichen. Somit beziehen sich diese Variablen auf die Zeilen von $\mathbb{A}$. In Bezug auf diese Variablen müssen wir das folgende [27, Eq. 2.5] optimieren.

$$\begin{aligned}\max\quad & \sum_{\sigma\in\mathbb{F}_q}\mathbb{E}\big[(\boldsymbol{d}-1)z_{\boldsymbol{d}}(\sigma)\log z_{\boldsymbol{d}}(\sigma)\big]\\ & -\frac{d}{k}\mathbb{E}\left[\sum_{\substack{\sigma_1,\dots,\sigma_{\boldsymbol{k}}\in\mathbb{F}_q\\ \boldsymbol{\chi}_{1,1}\sigma_1+\cdots+\boldsymbol{\chi}_{1,\boldsymbol{k}}\sigma_{\boldsymbol{k}}=0}}\hat{z}_{\boldsymbol{\chi}_{1,1},\dots,\boldsymbol{\chi}_{1,\boldsymbol{k}}}(\sigma_1,\dots,\sigma_{\boldsymbol{k}})\log\hat{z}_{\boldsymbol{\chi}_{1,1},\dots,\boldsymbol{\chi}_{1,\boldsymbol{k}}}(\sigma_1,\dots,\sigma_{\boldsymbol{k}})\right]\\ \text{s.t.}\quad & \mathbb{E}[\boldsymbol{d}z_{\boldsymbol{d}}(\tau)]=\mathbb{E}\left[\sum_{\substack{\sigma_1,\dots,\sigma_{\boldsymbol{k}}\in\mathbb{F}_q\\ \boldsymbol{\chi}_{1,1}\sigma_1+\cdots+\boldsymbol{\chi}_{1,\boldsymbol{k}}\sigma_{\boldsymbol{k}}=0}}\boldsymbol{k}\mathbb{1}\{\sigma_1=\tau\}\,\hat{z}_{\boldsymbol{\chi}_{1,1},\dots,\boldsymbol{\chi}_{1,\boldsymbol{k}}}(\sigma_1,\dots,\sigma_{\boldsymbol{k}})\right]\qquad\text{für alle }\tau\in\mathbb{F}_q 0.\end{aligned} \tag{5.0.7}$$

Die balancierte Lösung [27, Eq. 2.6]

$$z_i(\sigma)=q^{-1}\qquad\qquad \hat{z}_{\chi_1,\dots,\chi_\ell}(\sigma_1,\dots,\sigma_\ell)=q^{1-\ell}\qquad\qquad \text{für alle } i,\chi_1,\dots,\chi_\ell$$

erhält bei Anwendung in (5.0.7) den Wert $(1-d/k)\log q$. Dieser Wert entspricht dem normalisierten ersten Moment $\frac{1}{n}\log\mathbb{E}_{\mathfrak{A}}[\boldsymbol{Z}]$. Dies impliziert, dass für jedes ℓ die einzigen sinnvollen Werte, die zur Optimierung von (5.0.7) zu berücksichtigen sind, die fast ausgeglichenen Vektoren mit der gleichmäßigen Verteilung auf q sind. Somit bieten die folgenden zwei Beziehungen den Weg für den Beweis: [27, Eq. 2.8], [27, Eq. 2.9],

$$\mathbb{E}_{\mathfrak{A}}[\boldsymbol{Z}\cdot\mathbb{1}\{\mathbb{A}\in\mathfrak{O}\}]\sim\mathbb{E}_{\mathfrak{A}}[\boldsymbol{Z}]\sim q^{n-\boldsymbol{m}} \tag{5.0.8}$$

$$\mathbb{E}_{\mathfrak{A}}\big[\boldsymbol{Z}^2\cdot\mathbb{1}\{\mathbb{A}\in\mathfrak{O}\}\big]\sim\mathbb{E}_{\mathfrak{A}}[\boldsymbol{Z}]^2. \tag{5.0.9}$$

Wenn die Schlüsselbedingung in Theorem 5.0.6 erfüllt ist, können wir zeigen, dass (5.0.8), (5.0.9) mit

hoher Wahrscheinlichkeit wahr sind. Theorem (5.0.6) wird sich als einfache Konsequenz aus (5.0.8)–(5.0.9) und zwei anderen Sätzen herausstellen.

Die Hauptaufgabe besteht also darin, (5.0.8) und (5.0.9) zu beweisen. In Bezug auf (5.0.8) verwenden wir bei der ersten asymptotischen Gleichheit einen quenched Durchschnitt und eine Matrix mit wenigen zusätzlichen Zeilen. Die zweite asymptotische Gleichheit ist so einfach wie bei zufälligem 3-XORSAT. Wie bei (5.0.9) erweitern wir hier das zweite Moment um die uniforme Lösung. Diese Erweiterung beinhaltet die Betrachtung der Gitter, die von bestimmten ganzzahligen Vektoren erzeugt werden, die nahezu gleiche Lösungen codieren. Diese Methode verallgemeinert Huangs Argument für die Adjazenzmatrizen zufälliger d-regulärer Graphen [48] und verwendet einen lokalen Grenzwertsatz, um zu verifizieren, dass die balancierten Lösungen tatsächlich die meisten Lösungen einnehmen, damit die Momente berechnet werden können. Wir verweisen den Leser für Einzelheiten auf [27].

6 Conclusion

In this thesis, we covered various sparse random objects in combinatorics. First by exploring a random constraint satisfiability problem 2-SAT, we saw how the ideas inspired by statistical physics catalyzed concrete results. In particular, Belief Propagation was successfully applied to simplify the analysis of the marginal probabilities. Along with Belief Propagation, another method devised via the cavity ansatz, the Aizenman-Sims-Starr scheme was applied to the free energy density to find its tight lower bound. Furthermore, a discrete message passing algorithm called Warning Propagation was explored and was proven to be an effective tool to analyze various types of random graphs. Next, we studied combinatorial random matrices. The message passing algorithms we previously explored aided our study of a Bernoulli square matrix. To our suprise, this particular model revealed a unique phase transition that boasts replica symmetry but not strong replica symmetry. Furthermore, we took on a general random matrix model and successfully pinned down a sufficient condition for it to be full rank. The proof entailed the quenched computation, some algebraic ideas and a local limit theorem. The aforementioned methods have vast potential to answer many unexplored questions in constraint satisfiability problems and combinatorial random matrices.

A

THE RANDOM 2-SAT PARTITION FUNCTION

DIMITRIS ACHLIOPTAS, AMIN COJA-OGHLAN, MAX HAHN-KLIMROTH, JOON LEE, NOËLA MÜLLER, MANUEL PENSCHUCK, GUANGYAN ZHOU

ABSTRACT. We show that throughout the satisfiable phase the normalised number of satisfying assignments of a random 2-SAT formula converges in probability to an expression predicted by the cavity method from statistical physics. The proof is based on showing that the Belief Propagation algorithm renders the correct marginal probability that a variable is set to 'true' under a uniformly random satisfying assignment. *MSC:* 05C80, 60C05, 68Q87

1. INTRODUCTION

1.1. **Background and motivation.** The random 2-SAT problem was the first random constraint satisfaction problem whose satisfiability threshold could be pinpointed precisely, an accomplishment attained independently by Chvátal and Reed [14] and Goerdt [30] in 1992. The proofs evince the link between the 2-SAT threshold and the percolation phase transition of a random digraph. This connection subsequently enabled Bollobás, Borgs, Chayes, Kim and Wilson [11] to identify the size of the scaling window, which matches that of the giant component phase transition of the Erdős-Rényi random graph [10, 33]. Ramifications and extensions of these results pertain to random 2-SAT formulas with given literal degrees [19], the random MAX 2-SAT problem [20] and the performance of algorithms [45]. But despite the great attention devoted to random 2-SAT over the years, a fundamental question, mentioned prominently in the survey [28], remained conspicuously open: *how many satisfying assignments does a random* 2*-SAT formula typically possess?* While percolation-type arguments have been stretched to derive (rough) bounds [12], the exact answer remained beyond the reach of elementary techniques.

In addition to the mathematical literature, the 2-SAT problem attracted the interest of statistical physicists, who brought to bear a canny but non-rigorous approach called the cavity method [36, 37]. Instead of relying on percolation ideas, the physics *ansatz* seizes upon a heuristic message passing scheme called Belief Propagation. Its purpose is to calculate the marginal probabilities that a random satisfying assignment sets specific variables of the 2-SAT formula to 'true'. According to physics intuition Belief Propagation reveals a far more fine-grained picture than a mere percolation argument possibly could. Indeed, in combination with a functional called the Bethe free entropy, Belief Propagation renders a precise conjecture as to the number of satisfying assignments.

We prove this conjecture. Specifically, we show that for all clause-to-variable densities below the 2-SAT threshold the number of satisfying assignments is determined by the Bethe functional applied to a particular solution of a stochastic fixed point equation that mimics Belief Propagation. The formula that we obtain does not boil down to a simple algebraic expression, which may explain why the problem has confounded classical methods for nearly three decades. Nonetheless, thanks to rapid convergence of the stochastic fixed point iteration, the formula can be evaluated numerically within arbitrary precision. A crucial step towards the main theorem is to verify that Belief Propagation does indeed yield the correct marginals, a fact that may be of independent interest.

By comparison to prior work on Belief Propagation in combinatorics (e.g., [16, 22, 21, 39]), we face the substantial technical challenge of dealing with the 'hard' constraints of the 2-SAT problems, which demands that *all* clauses be satisfied. A second novelty is that in order to prove convergence of Belief Propagation to the correct marginals we need to investigate delicately constructed extremal initial conditions for the message passing process. Since these depend on the random 2-SAT formula itself, we need to develop means to confront the ensuing stochastic dependencies between the construction of the initial condition and the subsequent message passing iterations. We proceed to state the main results precisely. An outline of the proofs and a detailed discussion of related work follow in Sections 2 and 3.

Amin Coja-Oghlan's research received support under DFG CO 646/4. Max Hahn-Klimroth has been supported by Stiftung Polytechnische Gesellschaft. Manuel Penschuck's research received support under DFG ME 2088/3-2 and ME 2088/4-2. Guangyan Zhou is supported by National Natural Science Foundation of China, No. 61702019.

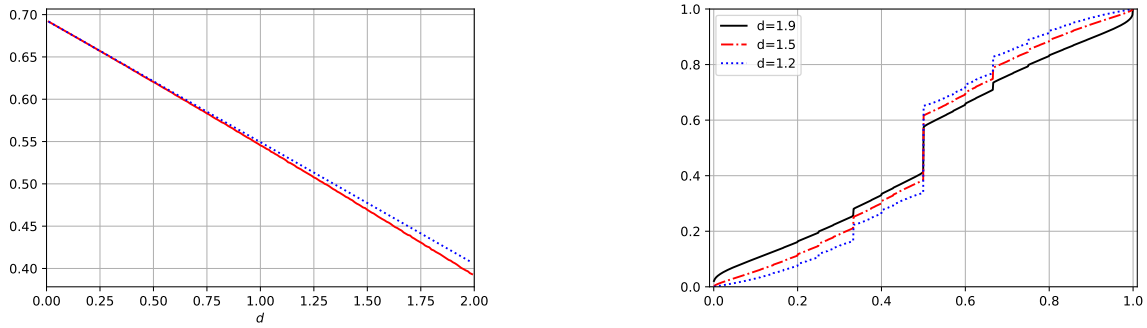

FIGURE 1. *Left:* the red line depicts a numerical approximation to the r.h.s. of (1.2) after 24 iterations of $\mathrm{BP}_d(\cdot)$. The dotted blue line displays the first moment bound. *Right:* the cumulative density functions of numerical approximations to $\mathrm{BP}_d^{24}(\delta_{1/2})$ for various d.

1.2. **The main result.** Let $n > 1$ be an integer, let $d > 0$ be a positive real and let $\boldsymbol{m} \stackrel{\mathrm{d}}{=} \mathrm{Po}(dn/2)$ be a Poisson random variable. Further, let $\boldsymbol{\Phi} = \boldsymbol{\Phi}_n$ be a random 2-SAT formula with Boolean variables $x_1, \ldots, x_n$ and $\boldsymbol{m}$ clauses, drawn uniformly and independently from the set of all $4n(n-1)$ possible clauses with two distinct variables. Thus, each variable appears in d clauses on the average and the satisfiability threshold occurs at $d = 2$. We aim to estimate the number $Z(\boldsymbol{\Phi})$ of satisfying assignments, the *partition function* in physics jargon. More precisely, since $Z(\boldsymbol{\Phi})$ remains exponentially large for all $d < 2$ w.h.p., in order to obtain a well-behaved limit we compute the normalised logarithm $n^{-1}\log Z(\boldsymbol{\Phi})$.

The result comes in terms of the solution to a stochastic fixed point equation on the unit interval. Hence, let $\mathscr{P}(0,1)$ be the set of all Borel probability measures on $(0,1)$, endowed with the weak topology. Further, define an operator $\mathrm{BP}_d : \mathscr{P}(0,1) \to \mathscr{P}(0,1)$, $\pi \mapsto \hat{\pi}$ as follows. With $\boldsymbol{d}^+, \boldsymbol{d}^-$ Poisson variables with mean $d/2$ and $\boldsymbol{\mu}_{\pi,1}, \boldsymbol{\mu}_{\pi,2}, \ldots$ random variables with distribution π, all mutually independent, let $\hat{\pi}$ be the distribution of the random variable

$$\frac{\prod_{i=1}^{\boldsymbol{d}^-}\boldsymbol{\mu}_{\pi,i}}{\prod_{i=1}^{\boldsymbol{d}^-}\boldsymbol{\mu}_{\pi,i} + \prod_{i=1}^{\boldsymbol{d}^+}\boldsymbol{\mu}_{\pi,i+\boldsymbol{d}^-}} \in (0,1). \tag{1.1}$$

Let $\delta_{1/2} \in \mathscr{P}(0,1)$ signify the atom at $1/2$ and write $\mathrm{BP}_d^\ell(\cdot)$ for the ℓ-fold application of the operator BP_d.

Theorem 1.1. *For any $d < 2$ the limit $\pi_d = \lim_{\ell\to\infty}\mathrm{BP}_d^\ell(\delta_{1/2})$ exists and*

$$\lim_{n\to\infty}\frac{1}{n}\log Z(\boldsymbol{\Phi}) = \mathbb{E}\left[\log\left(\prod_{i=1}^{\boldsymbol{d}^-}\boldsymbol{\mu}_{\pi_d,i} + \prod_{i=1}^{\boldsymbol{d}^+}\boldsymbol{\mu}_{\pi_d,i+\boldsymbol{d}^-}\right) - \frac{d}{2}\log\left(1-\boldsymbol{\mu}_{\pi_d,1}\boldsymbol{\mu}_{\pi_d,2}\right)\right] \qquad \textit{in probability.} \tag{1.2}$$

Of course, the fact that the r.h.s. of (1.2) is well-defined is part of the statement of Theorem 1.1.

By construction, the distribution π_d is a solution to the stochastic fixed point equation

$$\pi_d = \mathrm{BP}_d(\pi_d). \tag{1.3}$$

The equation (1.3) is known as the *density evolution* equation in physics lore, while the expression on the r.h.s. of (1.2) is called the *Bethe free entropy* [34]. Hence, Theorem 1.1 matches the conjecture from [36]. By comparison, Markov's inequality yields the elementary first moment bound

$$\frac{1}{n}\log Z(\boldsymbol{\Phi}) \le \frac{1}{n}\log\mathbb{E}[Z(\boldsymbol{\Phi})] + o(1) = (1-d)\log 2 + \frac{d}{2}\log 3 + o(1) \qquad \text{w.h.p.,} \tag{1.4}$$

which, however, fails to be tight for any $0 < d < 2$ [42]. Furthermore, while (1.2) may appear difficult to evaluate, the proof reveals that the fixed point iteration $\mathrm{BP}_d^\ell(\delta_{1/2})$ converges geometrically (in an appropriate metric). In effect, decent numerical approximations can be obtained; see Figure 1.

For $d < 1$ the random digraph on $\{x_1, \neg x_1, \ldots, x_n, \neg x_n\}$ obtained by inserting for each clause $l_1 \vee l_2$ of $\boldsymbol{\Phi}$ the two directed edges $\neg l_1 \to l_2$, $\neg l_2 \to l_1$ is sub-critical and the distribution π_d is supported on a countable set. In effect, for $d < 1$ the formula (1.2) can be obtained via elementary counting arguments. By contrast, the emergence of a weak giant component for $1 < d < 2$ turns the computation of $Z(\boldsymbol{\Phi})$ into a challenge. Finally, for $d > 2$ the digraph

contains a strongly connected giant component w.h.p. Its long directed cycles likely cause contradictions, which is why satisfying assignments cease to exist.

An asymptotically tight upper bound on $n^{-1}\log Z(\mathbf{\Phi})$ could be obtained via the interpolation method from mathematical physics [29, 42]. We will revisit this point in Section 3. Thus, the principal contribution of Theorem 1.1 is the lower bound on $\log Z(\mathbf{\Phi})$. The best prior lower bound was obtained by Boufkhad and Dubois [12] in 1999 via percolation arguments. However, this bound drastically undershoots the actual value from Theorem 1.1. For instance, for $d = 1.2$, [12] gives $n^{-1}\log Z(\mathbf{\Phi}) \geq 0.072\ldots$, while actually $n^{-1}\log Z(\mathbf{\Phi}) = 0.515\ldots$ w.h.p.

1.3. **Belief Propagation.** To elaborate on the combinatorial meaning of the distribution π_d, we need to look into the Belief Propagation heuristic. Instantiated to 2-SAT, Belief Propagation is a message passing algorithm designed to approximate the marginal probability that a specific variable takes the value 'true' under a random satisfying assignment. While finding satisfying assignments of a given 2-SAT formula is an easy computational task, calculating these marginals is not. In fact, the problem is #P-hard [49]. Nonetheless, we are going to prove that Belief Propagation approximates the marginals well on random formulas w.h.p.

To introduce Belief Propagation, we associate a bipartite graph $G(\mathbf{\Phi})$ with the formula $\mathbf{\Phi}$. One vertex class $V_n = \{x_1, \ldots, x_n\}$ represents the propositional variables, the other class $F_{\boldsymbol{m}} = \{a_1, \ldots, a_{\boldsymbol{m}}\}$ represents the clauses. Each clause a_i is adjacent to the two variables that it contains. We write $\partial v = \partial(\mathbf{\Phi}, v)$ for the set of neighbours of a vertex v of $G(\mathbf{\Phi})$. Moreover, for $\ell \geq 1$ let $\partial^\ell v$ signify the set of all vertices at distance precisely ℓ from v.

Associated with the edges of $G(\mathbf{\Phi})$, the Belief Propagation messages are probability distributions on the Boolean values 'true' and 'false'. To be precise, any adjacent clause/variable pair a, x comes with two messages, one directed from a to x and a reverse one from x to a. Encoding 'true' and 'false' by ± 1, we initialise all messages by

$$\nu^{(0)}_{\mathbf{\Phi},a\to x}(\pm 1) = \nu^{(0)}_{\mathbf{\Phi},x\to a}(\pm 1) = 1/2. \tag{1.5}$$

For $\ell \geq 1$ the messages $\nu^{(\ell)}_{\mathbf{\Phi},a\to x}, \nu^{(\ell)}_{\mathbf{\Phi},x\to a}$ are defined inductively. Specifically, suppose that clause a contains the two variables x, y. Let $r, s \in \{\pm 1\}$ indicate whether x, y appear as positive or negative literals in a. Then for $t = \pm 1$ let

$$\nu^{(\ell)}_{\mathbf{\Phi},a\to x}(t) = \frac{1 - \mathbf{1}\{r \neq t\}\,\nu^{(\ell-1)}_{\mathbf{\Phi},y\to a}(-s)}{1 + \nu^{(\ell-1)}_{\mathbf{\Phi},y\to a}(s)}, \qquad \nu^{(\ell)}_{\mathbf{\Phi},x\to a}(t) = \frac{\prod_{b\in\partial x\setminus\{a\}} \nu^{(\ell)}_{\mathbf{\Phi},b\to x}(t)}{\prod_{b\in\partial x\setminus\{a\}} \nu^{(\ell)}_{\mathbf{\Phi},b\to x}(1) + \prod_{b\in\partial x\setminus\{a\}} \nu^{(\ell)}_{\mathbf{\Phi},b\to x}(-1)}. \tag{1.6}$$

The last expression is deemed to equal $1/2$ if the denominator vanishes (which does not happen if $\mathbf{\Phi}$ is satisfiable). Finally, the Belief Propagation estimate of the marginal of a variable x after ℓ iterations reads

$$\nu^{(\ell)}_{\mathbf{\Phi},x}(t) = \frac{\prod_{a\in\partial x} \nu^{(\ell)}_{\mathbf{\Phi},a\to x}(t)}{\prod_{a\in\partial x} \nu^{(\ell)}_{\mathbf{\Phi},a\to x}(1) + \prod_{a\in\partial x} \nu^{(\ell)}_{\mathbf{\Phi},a\to x}(-1)}, \tag{1.7}$$

again interpreted to yield $1/2$ if the denominator vanishes. For an excellent exposition of Belief Propagation, including the derivation of (1.6)–(1.7), we point to [34, Chapter 14].

The next theorem establishes that (1.7) approximates the true marginals well for large ℓ. In fact, we prove a significantly stronger result. To set the stage, let $S(\mathbf{\Phi})$ be the set of all satisfying assignments of $\mathbf{\Phi}$. Assuming $S(\mathbf{\Phi}) \neq \emptyset$, let

$$\mu_{\mathbf{\Phi}}(\sigma) = \mathbf{1}\{\sigma \in S(\mathbf{\Phi})\}/Z(\mathbf{\Phi}) \qquad (\sigma \in \{\pm 1\}^{\{x_1,\ldots,x_n\}}) \tag{1.8}$$

be the uniform distribution on $S(\mathbf{\Phi})$. Further, write $\boldsymbol{\sigma}$ for a sample from $\mu_{\mathbf{\Phi}}$. Then for a satisfying assignment $\tau \in S(\mathbf{\Phi})$ and $\ell \geq 1$ the conditional distribution $\mu_{\mathbf{\Phi}}(\cdot \mid \boldsymbol{\sigma}_{\partial^{2\ell} x_1} = \tau_{\partial^{2\ell} x_1}) = \mu_{\mathbf{\Phi}}(\cdot \mid \forall y \in \partial^{2\ell} x_1 : \boldsymbol{\sigma}_y = \tau_y)$ imposes the 'boundary condition' τ on all variables y at distance 2ℓ from x_1. The following theorem shows that Belief Propagation does not just approximate the plain, unconditional marginals well w.h.p., but even the conditional marginals given any conceivable boundary condition. Recall that $\mathbb{P}[Z(\mathbf{\Phi}) > 0] = 1 - o(1)$ for $d < 2$.

Theorem 1.2. *If $d < 2$, then*

$$\lim_{\ell\to\infty} \limsup_{n\to\infty} \mathbb{E}\left[\max_{\tau\in S(\mathbf{\Phi})} \left|\mu_{\mathbf{\Phi}}(\boldsymbol{\sigma}_{x_1} = 1 \mid \boldsymbol{\sigma}_{\partial^{2\ell} x_1} = \tau_{\partial^{2\ell} x_1}) - \nu^{(\ell)}_{\mathbf{\Phi},x_1}(1)\right| \,\middle|\, Z(\mathbf{\Phi}) > 0\right] = 0. \tag{1.9}$$

Since $\nu^{(\ell)}_{\mathbf{\Phi},x_1}$ does not depend on τ, averaging (1.9) on the boundary condition $\tau \in S(\mathbf{\Phi})$ yields

$$\lim_{\ell\to\infty} \limsup_{n\to\infty} \mathbb{E}\left[\left|\mu_{\mathbf{\Phi}}(\boldsymbol{\sigma}_{x_1} = \pm 1) - \nu^{(\ell)}_{\mathbf{\Phi},x_1}(\pm 1)\right| \mid Z(\mathbf{\Phi}) > 0\right] = 0. \tag{1.10}$$

Thus, Belief Propagation approximates the unconditional marginal of x_1 well in the limit of large n and ℓ. Indeed, because the distribution of $\mathbf{\Phi}$ is invariant under permutations of the variables $x_1,\ldots,x_n$, (1.10) implies that the marginals of all but $o(n)$ variables x_i are within $\pm o(1)$ of the Belief Propagation approximation w.h.p.

But thanks to the presence of the boundary condition τ, Theorem 1.2 leads to further discoveries. For a start, applying the triangle inequality to (1.9) and (1.10), we obtain

$$\lim_{\ell\to\infty}\limsup_{n\to\infty}\mathbb{E}\left[\max_{\tau\in S(\mathbf{\Phi})}\left|\mu_{\mathbf{\Phi}}(\boldsymbol{\sigma}_{x_1}=1\mid\boldsymbol{\sigma}_{\partial^{2\ell}x_1}=\tau_{\partial^{2\ell}x_1})-\mu_{\mathbf{\Phi}}(\boldsymbol{\sigma}_{x_1}=1)\right|\;\middle|\;Z(\mathbf{\Phi})>0\right]=0. \tag{1.11}$$

Thus, no discernible shift of the marginal of x_1 is likely to ensue upon imposition of any possible boundary condition τ. The spatial mixing property (1.11) is colloquially known as *Gibbs uniqueness* [32]. Further, (1.11) rules out extensive long-range correlations. Specifically, for any fixed ℓ the first two variables x_1,x_2 likely have distance greater than 4ℓ in $G(\mathbf{\Phi})$. Therefore, (1.11) implies that for all $d<2$,

$$\lim_{n\to\infty}\sum_{s,t\in\{\pm1\}}\mathbb{E}\left[\left|\mu_{\mathbf{\Phi}}(\boldsymbol{\sigma}_{x_1}=s,\boldsymbol{\sigma}_{x_2}=t)-\mu_{\mathbf{\Phi}}(\boldsymbol{\sigma}_{x_1}=s)\cdot\mu_{\mathbf{\Phi}}(\boldsymbol{\sigma}_{x_2}=t)\right|\;\middle|\;Z(\mathbf{\Phi})>0\right]=0. \tag{1.12}$$

Thus, the truth values $\boldsymbol{\sigma}_{x_1},\boldsymbol{\sigma}_{x_2}$ are asymptotically independent. Of course, once again by permutation invariance, (1.12) implies that asymptotic independence extends to all but $o(n^2)$ pairs of variables x_i,x_j w.h.p. The decorrelation property (1.12) is called *replica symmetry* in the physics literature [32].

Finally, we can clarify the combinatorial meaning of the distribution π_d from Theorem 1.1. Namely, π_d is the limit of the empirical distribution of the marginal probabilities $\mu_{\mathbf{\Phi}}(\boldsymbol{\sigma}_{x_i}=1)$.

Corollary 1.3. *For any $0<d<2$ the random probability measure*

$$\pi_{\mathbf{\Phi}}=\frac{1}{n}\sum_{i=1}^{n}\delta_{\mu_{\mathbf{\Phi}}(\boldsymbol{\sigma}_{x_i}=1)} \tag{1.13}$$

converges to π_d weakly in probability.[1]

Thus, the stochastic fixed point equation (1.3) that characterises π_d simply expresses that the marginal probabilities $\mu_{\mathbf{\Phi}}(\boldsymbol{\sigma}_{x_i}=1)$ result from the Belief Propagation recurrence (1.6).

1.4. **Preliminaries and notation.** Throughout we denote by $V_n=\{x_1,\ldots,x_n\}$ the variable set of $\mathbf{\Phi}_n$. Generally, given a 2-SAT formula Φ we write $V(\Phi)$ for the set of variables and $F(\Phi)$ for the set of clauses. The bipartite clause/variable-graph $G(\Phi)$ is defined as in Section 1.3. For a vertex v of $G(\Phi)$ we let $\partial(\Phi,v)$ be the set of neighbours. Where Φ is apparent we just write ∂v. Moreover, $\partial^\ell(\Phi,v)$ or briefly $\partial^\ell v$ stands for the set of vertices at distance exactly ℓ from v. Additionally, $\nabla^\ell(\Phi,v)$ denotes the sub-formula obtained from Φ by deleting all clauses and variables at distance greater than ℓ from v. This sub-formula may contain clauses of length less than two. Further, for a clause a and a variable x of Φ we let $\mathrm{sign}(x,a)=\mathrm{sign}_\Phi(x,a)\in\{\pm1\}$ be the sign with which x appears in a. In addition, we let $S(\Phi)$ be the set of all satisfying assignments of Φ, $Z(\Phi)=|S(\Phi)|$ and, assuming $Z(\Phi)>0$, we let μ_Φ be the probability distribution on $\{\pm1\}^{V(\Phi)}$ that induces the uniform distribution on $S(\Phi)$ as in (1.8). Moreover, $\boldsymbol{\sigma}_\Phi=(\boldsymbol{\sigma}_{\Phi,x})_{x\in V(\Phi)}$ signifies a uniformly random satisfying assignment; we drop Φ where the reference is apparent.

For any Φ we set up Belief Propagation as in (1.5)–(1.7). It is well known that Belief Propagation yields the correct marginals if $G(\Phi)$ is a tree. To be precise, the *depth* of $x\in V(\Phi)$ is the maximum distance between x and a leaf of $G(\Phi)$.

Proposition 1.4 ([34, Theorem 14.1])**.** *If $G(\Phi)$ is a tree and $x\in V(\Phi)$, then for any ℓ greater than or equal to the depth of x we have $\mu_\Phi(\boldsymbol{\sigma}_x=\pm1)=\nu^{(\ell)}_{\Phi,x}(\pm1)$.*

We will encounter the following functions repeatedly. For $\varepsilon>0$ let $\Lambda_\varepsilon(z)=\log(z\vee\varepsilon)$ be the log function truncated at $\log\varepsilon$. Moreover, we need the continuous and mutually inverse functions

$$\psi:\mathbb{R}\to(0,1),\quad z\mapsto(1+\tanh(z/2))/2,\qquad\qquad \varphi:(0,1)\to\mathbb{R},\quad p\mapsto\log(p/(1-p)). \tag{1.14}$$

Let $\mathscr{P}(\mathbb{R})$ be the set of all Borel probability measures on $\mathbb{R}$ with the weak topology. Moreover, for a real $q\geq1$ let $\mathscr{W}_q(\mathbb{R})$ be the set of all $\rho\in\mathscr{P}(\mathbb{R})$ such that $\int_{\mathbb{R}}|x|^q\mathrm{d}\rho(x)<\infty$. We equip this space with the Wasserstein metric

$$W_q(\rho,\rho')=\inf\left\{\left(\int_{\mathbb{R}^2}|x-y|^q\mathrm{d}\gamma(x,y)\right)^{1/q}:\gamma\text{ is a coupling of }\rho,\rho'\right\}, \tag{1.15}$$

[1] That is, for any continuous function $f:[0,1]\to\mathbb{R}$ we have $\lim_{n\to\infty}\mathbb{E}\left|\int_0^1 f(z)\mathrm{d}\pi_d(z)-\int_0^1 f(z)\mathrm{d}\pi_{\mathbf{\Phi}}(z)\right|=0$.

thereby turning $\mathscr{W}_q(\mathbb{R})$ into a complete separable space [9].

For $\rho \in \mathscr{P}(\mathbb{R})$ we denote by $\boldsymbol{\eta}_\rho, \boldsymbol{\eta}_{\rho,1}, \boldsymbol{\eta}_{\rho,2}, \ldots$ random variables with distribution ρ. Similarly, for $\pi \in \mathscr{P}(0,1)$ we let $\boldsymbol{\mu}_\pi, \boldsymbol{\mu}_{\pi,1}, \boldsymbol{\mu}_{\pi,2}, \ldots$ be a sequence of random variables with distribution π. We also continue to let $\boldsymbol{d}$ be a Poisson variable with mean d and $\boldsymbol{d}^+, \boldsymbol{d}^-$ Poisson variables with mean $d/2$. Moreover, $\boldsymbol{s}_1, \boldsymbol{s}'_1, \boldsymbol{s}_2, \boldsymbol{s}'_2, \ldots \in \{\pm 1\}$ always denote uniformly distributed random variables. All of these random variables are mutually independent as well as independent of any other sources of randomness.

Finally, from here on we tacitly assume that $0 < d < 2$**.**

2. Overview

The proof of Theorem 1.1 proceeds in four steps. First we show that the limit π_d from Theorem 1.1 exists. Subsequently we establish the fact (1.9) that Belief Propagation approximates the conditional marginals well. This will easily imply the convergence of the empirical marginals (1.13) to π_d. Third, building upon these preparations, we will prove that the truncated mean $n^{-1}\mathbb{E}[\log(Z(\boldsymbol{\Phi}) \vee 1)]$ converges to the r.h.s. of (1.2). The truncation is necessary to deal with the (unlikely) event that $Z(\boldsymbol{\Phi}) = 0$. Finally, we will show that $\log(Z(\boldsymbol{\Phi}) \vee 1)$ concentrates about its mean to obtain convergence in probability, thus completing the proof of Theorem 1.1.

2.1. **Step 1: density evolution.** We begin by verifying that the distribution π_d from Theorem 1.1 is well-defined and that π_d satisfies a tail bound.

Proposition 2.1. *The weak limit* $\pi_d = \lim_{\ell\to\infty} \mathrm{BP}_d^\ell(\delta_{1/2})$ *exists and*

$$\mathbb{E}\left[\log^2 \frac{\boldsymbol{\mu}_{\pi_d}}{1-\boldsymbol{\mu}_{\pi_d}}\right] < \infty. \tag{2.1}$$

Moreover, $\boldsymbol{\mu}_{\pi_d}$ *and* $1-\boldsymbol{\mu}_{\pi_d}$ *are identically distributed and*

$$\mathbb{E}\left|\log\left(\prod_{i=1}^{\boldsymbol{d}^-} \boldsymbol{\mu}_{\pi_d,i} + \prod_{i=1}^{\boldsymbol{d}^+} \boldsymbol{\mu}_{\pi_d,i+\boldsymbol{d}^-}\right)\right| < \infty, \qquad \mathbb{E}\left|\log\left(1-\boldsymbol{\mu}_{\pi_d,1}\boldsymbol{\mu}_{\pi_d,2}\right)\right| < \infty. \tag{2.2}$$

The proof of Proposition 2.1, which we carry out in Section 4, is based on a contraction argument. This argument implies that the fixed point iteration converges rapidly to π_d, a fact that can be exploited to obtain numerical estimates. The bounds (2.2) ensure that the expectation on the r.h.s. of (1.2) is well-defined.

2.2. **Step 2: Gibbs uniqueness.** As a next step we verify the Gibbs uniqueness property (1.11). We proceed by way of analysing a multi-type Galton-Watson tree $\boldsymbol{T}$ that mimics the local structure of the graph $G(\boldsymbol{\Phi})$ upon exploration from variable x_1. The Galton-Watson process has five types: variable nodes and four types of clause nodes $(+1,+1), (+1,-1), (-1,+1), (-1,-1)$. The root is a variable node o. Moreover, each variable node spawns independent $\mathrm{Po}(d/4)$ numbers of clauses nodes of each of the four types. Additionally, each clause has a single offspring, which is a variable. The semantics of the clause types is that the first component indicates whether the parent variable appears in the clause positively or negatively. The second component indicates whether the child variable appears as a positive or as a negative literal. Clearly, for $d \le 1$ the tree $\boldsymbol{T}$ is finite with probability one, while infinite trees appear with positive probability for $d > 1$.

Let $\boldsymbol{T}^{(\ell)}$ be the finite tree obtained from $\boldsymbol{T}$ by dropping all nodes at distance greater than ℓ from the root. For even ℓ it will be convenient to view $\boldsymbol{T}^{(\ell)}$ interchangeably as a tree or as a 2-SAT formula. In particular, we write $\partial^{2\ell} o = \partial^{2\ell}(\boldsymbol{T}, o)$ for the set of all variables at distance exactly 2ℓ from o. The following proposition, which is the linchpin of the entire proof strategy, establishes the Gibbs uniqueness property for the tree formula $\boldsymbol{T}^{(2\ell)}$.

Proposition 2.2. *We have*

$$\lim_{\ell\to\infty} \mathbb{E}\left[\max_{\tau \in S(\boldsymbol{T}^{(2\ell)})} \left|\mu_{\boldsymbol{T}^{(2\ell)}}(\boldsymbol{\sigma}_o = 1 \mid \boldsymbol{\sigma}_{\partial^{2\ell} o} = \tau_{\partial^{2\ell} o}) - \mu_{\boldsymbol{T}^{(2\ell)}}(\boldsymbol{\sigma}_o = 1)\right|\right] = 0. \tag{2.3}$$

Thus, w.h.p. no conceivable boundary condition is apt to significantly shift the marginal of the root.

We prove Proposition 2.2 by a subtle contraction argument in combination with a construction of extremal boundary conditions of the tree formula $\boldsymbol{T}^{(2\ell)}$. More specifically, we will construct boundary conditions $\boldsymbol{\sigma}^\pm$ that maximise or minimise the conditional probability

$$\mu_{\boldsymbol{T}^{(2\ell)}}(\boldsymbol{\sigma}_o = 1 \mid \boldsymbol{\sigma}_{\partial^{2\ell} o} = \boldsymbol{\sigma}^\pm_{\partial^{2\ell} o}), \tag{2.4}$$

respectively. Then we will show that the difference of the conditional marginals induced by both these extremal boundary conditions vanishes with probability tending to one as $\ell \to \infty$. The delicate point is that the extremal boundary conditions $\boldsymbol{\sigma}^{\pm}$ depend on the tree $\boldsymbol{T}^{(2\ell)}$. Thus, at first glance it seems that we need to pass the tree twice, once top–down to construct $\boldsymbol{\sigma}^{\pm}$ and then bottom–up to calculate the conditional marginals (2.4). But such an analysis seems untenable because after the top–down pass the tree is exposed and 'no randomness remains' to facilitate the bottom–up phase. Fortunately, we will see that a single stochastic fixed point equation captures both the top–down and the bottom–up phase. This discovery reduces the proof of Proposition 2.2 to showing that the fixed point iteration contracts. The details of this delicate argument can be found in Section 5.

Proposition 2.2 easily implies the Gibbs uniqueness condition (1.11) and thereby Theorem 1.2. A further consequence is the asymptotic independence of the joint truth values of bounded numbers of variables.

Corollary 2.3. *The statement* (1.9) *is true and for any integer $k \geq 2$ we have*

$$\lim_{n\to\infty} \sum_{\sigma\in\{\pm1\}^k} \mathbb{E}\left[\left|\mu_{\boldsymbol{\Phi}}(\boldsymbol{\sigma}_{x_1}=\sigma_1,\ldots,\boldsymbol{\sigma}_{x_k}=\sigma_k) - \prod_{i=1}^{k}\mu_{\boldsymbol{\Phi}}(\boldsymbol{\sigma}_{x_i}=\sigma_i)\right| \mid Z(\boldsymbol{\Phi})>0\right] = 0.$$

2.3. **Step 3: the Aizenman-Sims-Starr scheme.** The aforementioned results pave the way for deriving an expression for the conditional expectation of $\log Z(\boldsymbol{\Phi})$ given that $\boldsymbol{\Phi}$ is satisfiable. Since $\boldsymbol{\Phi}$ is satisfiable w.h.p. for all $d < 2$, an equivalent task is to calculate $\mathbb{E}[\log(Z(\boldsymbol{\Phi})\vee 1)]$. To this end we seize upon a simple but powerful strategy colloquially called the Aizenman-Sims-Starr scheme [5]. Originally proposed in the context of the Sherrington-Kirkpatrick spin glass model, this proof strategy suggests to compute the asymptotic mean of a random variable on a 'system' of size n by carefully estimating the change of that mean upon going to a 'system' of size $n+1$. This difference is calculated by coupling the systems of size n and $n+1$ such that the latter is obtained from the former by a small expected number of local changes.

We apply this idea to the random 2-SAT problem by coupling the random formula $\boldsymbol{\Phi}_n$ with n variables and $\mathrm{Po}(dn/2)$ clauses and the random formula $\boldsymbol{\Phi}_{n+1}$ with $n+1$ variables and $\mathrm{Po}(d(n+1)/2)$ clauses. Roughly speaking, we obtain $\boldsymbol{\Phi}_{n+1}$ from $\boldsymbol{\Phi}_n$ by adding a new variable x_{n+1} along with a few random adjacent clauses that connect x_{n+1} with the variables $x_1,\ldots,x_n$ of $\boldsymbol{\Phi}_n$. Then the information about the joint distribution of the truth values of bounded numbers of variables furnished by Corollaries 1.3 and 2.3 and the tail bound (2.1) will enable us to accurately estimate $\mathbb{E}\left[\log(Z(\boldsymbol{\Phi}_{n+1})\vee 1) - \log(Z(\boldsymbol{\Phi}_n)\vee 1)\right]$.

Needless to say, upon closer inspection matters will emerge to be rather subtle. The main source of complications is that, in contrast to other models in mathematical physics such as the Sherrington-Kirkpatrick model or the Ising model, the 2-SAT problem has hard constraints. Thus, the addition of a single clause could trigger a dramatic drop in the partition function. In fact, in the worst case a single awkward clause could wipe out all satisfying assignments. In Section 6 we will iron out all these difficulties and prove the following.

Proposition 2.4. *We have*

$$\lim_{n\to\infty} \mathbb{E}[\log(Z(\boldsymbol{\Phi}_{n+1})\vee 1)] - \mathbb{E}[\log(Z(\boldsymbol{\Phi}_n)\vee 1)] = \mathbb{E}\left[\log\left(\prod_{i=1}^{\boldsymbol{d}^-}\boldsymbol{\mu}_{\pi_d,i} + \prod_{i=1}^{\boldsymbol{d}^+}\boldsymbol{\mu}_{\pi_d,i+\boldsymbol{d}^-}\right) - \frac{d}{2}\log\left(1-\boldsymbol{\mu}_{\pi_d,1}\boldsymbol{\mu}_{\pi_d,2}\right)\right]. \tag{2.5}$$

We notice that (2.2) guarantees that the r.h.s. of (2.5) is well-defined. As an immediate consequence of Proposition 2.4 we obtain a formula for $\mathbb{E}[\log(Z(\boldsymbol{\Phi})\vee 1)]$.

Corollary 2.5. *For any $d < 2$ we have*

$$\lim_{n\to\infty} \frac{1}{n}\mathbb{E}[\log(Z(\boldsymbol{\Phi})\vee 1)] = \mathbb{E}\left[\log\left(\prod_{i=1}^{\boldsymbol{d}^-}\boldsymbol{\mu}_{\pi_d,i} + \prod_{i=1}^{\boldsymbol{d}^+}\boldsymbol{\mu}_{\pi_d,i+\boldsymbol{d}^-}\right) - \frac{d}{2}\log\left(1-\boldsymbol{\mu}_{\pi_d,1}\boldsymbol{\mu}_{\pi_d,2}\right)\right].$$

Proof. Writing $\mathbb{E}[\log(Z(\boldsymbol{\Phi})\vee 1)]$ as a telescoping sum and applying Proposition 2.4, we obtain

$$\begin{aligned}\lim_{n\to\infty} \frac{1}{n}\mathbb{E}[\log(Z(\boldsymbol{\Phi}_n)\vee 1)] &= \lim_{n\to\infty}\frac{1}{n}\sum_{N=2}^{n-1}\mathbb{E}[\log(Z(\boldsymbol{\Phi}_{N+1})\vee 1)] - \mathbb{E}[\log(Z(\boldsymbol{\Phi}_N)\vee 1)] \\ &= \mathbb{E}\left[\log\left(\prod_{i=1}^{\boldsymbol{d}^-}\boldsymbol{\mu}_{\pi_d,i} + \prod_{i=1}^{\boldsymbol{d}^+}\boldsymbol{\mu}_{\pi_d,i+\boldsymbol{d}^-}\right) - \frac{d}{2}\log\left(1-\boldsymbol{\mu}_{\pi_d,1}\boldsymbol{\mu}_{\pi_d,2}\right)\right],\end{aligned}$$

as desired. □

2.4. **Step 4: concentration.** The final step towards Theorem 1.1 is to show that $\log(Z(\mathbf{\Phi}) \vee 1)$ concentrates about its mean.

Proposition 2.6. *We have* $\lim_{n\to\infty} n^{-1}\mathbb{E}\left|\log(Z(\mathbf{\Phi}) \vee 1) - \mathbb{E}[\log(Z(\mathbf{\Phi}) \vee 1)]\right| = 0$.

Proposition 2.6 does not easily follow from routine arguments such as the Azuma-Hoeffding inequality. Once more the issue is that changing a single clause could alter $\log(Z(\mathbf{\Phi}) \vee 1)$ by as much as $\Theta(n)$. Instead we will resort to another technique from mathematical physics called the interpolation method. The details can be found in Section 7.

Proof of Theorem 1.1. The theorem follows from Proposition 2.1, Corollary 2.5 and Proposition 2.6. □

3. Discussion

The random 2-SAT satisfiability threshold was established mathematically shortly after the experimental work of Cheeseman, Kanefsky and Taylor [13] that triggered the quest for satisfiability thresholds appeared. The second successful example, nearly a decade later, was the random 1-in-k-SAT threshold (to satisfy exactly one literal in each clause), which Achlioptas, Chtcherba, Istrate and Moore pinpointed by analysing the Unit Clause algorithm [2]. In a subsequent landmark contribution Dubois and Mandler determined the 3-XORSAT threshold via the second moment method [27]. Subsequent work extended this result to random k-XORSAT [23, 43]. Finally, the most notable success thus far has been the verification of the '1RSB cavity method' prediction [35] of the random k-SAT threshold for large k due to Ding, Sly and Sun [25], the culmination of a line of work that refined the use of the second moment method [3, 4, 17].

Over the past two decades the general theme of estimating the partition functions of discrete structures has received a great deal of attention; e.g., [8]. With respect to random 2-SAT (and, more generally, k-SAT), Montanari and Shah [39], Panchenko [41] and Talagrand [48] investigated 'soft' versions of the partition function. To be precise, introducing a parameter $\beta > 0$ called the 'inverse temperature', these articles study the random variable

$$Z_\beta(\mathbf{\Phi}) = \sum_{\sigma\in\{\pm1\}^n}\prod_{i=1}^{m}\exp\left(-\beta\mathbf{1}\left\{\sigma \text{ violates clause } a_i\right\}\right). \tag{3.1}$$

Thus, instead of dismissing assignments that fail to satisfy all clauses outright, there is an $\exp(-\beta)$ penalty factor for each violated clause. Talagrand [48] computes $\lim_{n\to\infty} n^{-1}\mathbb{E}[\log Z_\beta(\mathbf{\Phi})]$ for β not exceeding a small but unspecified $\beta_0 > 0$. Panchenko [41] calculates this limit under the assumption $(4\beta \wedge 1)d < 1$. Thus, for $\beta > 1/4$ the result is confined to $d < 1$, in which case the random graph $G(\mathbf{\Phi})$ is sub-critical and both $Z_\beta(\mathbf{\Phi})$ and the actual number $Z(\mathbf{\Phi})$ of satisfying assignments could be calculated via elementary methods. Furthermore, Montanari and Shah [39] obtain $\lim_{n\to\infty} n^{-1}\mathbb{E}[\log Z_\beta(\mathbf{\Phi})]$ for all finite β under the assumption $d < 1.16\ldots$. Although for any fixed formula $\mathbf{\Phi}$ the limit $\lim_{\beta\to\infty} Z_\beta(\mathbf{\Phi})$ is equal to the number of satisfying assignments, it is not possible to interchange the limits $\beta\to\infty$ and $n\to\infty$. Thus, [39, 41] do not yield the the number of actual satisfying assignments even for $d < 1.16\ldots$ or $d < 1$, respectively. Apart from estimating $\mathbb{E}\log Z_\beta(\mathbf{\Phi})$, Montanari and Shah [39] also show that the Belief Propagation message passing scheme approximates the marginals of the Boltzmann distribution that goes with $Z_\beta(\mathbf{\Phi})$ well, i.e., they obtain a 'soft' version of Theorem 1.2 for $d < 1.16\ldots$.

In terms of proof techniques, all three contributions [39, 41, 48] are based on establishing the Gibbs uniqueness property. So is the present paper. But while [39, 41, 48] rely on relatively straightforward contraction arguments, a key distinction is that here we develop a more accurate (and delicate) method for verifying the Gibbs uniqueness property based on the explicit construction of an extremal boundary condition. This is the key to pushing the range of d all the way up to the satisfiability threshold $d = 2$.

Specifically, in order to construct a boundary condition of the random tree $\boldsymbol{T}^{(2\ell)}$ for large ℓ that maximises the conditional probability of observing the truth value $+1$ at the root we will work our way top–down from the root to level 2ℓ. Exposing the degrees and the signs with which the variables appear, the construction assigns a 'desired' truth value to each variable of the tree so as to nudge the parent variable towards its desired value as much as possible. Subsequently, once this process reaches the bottom level of the tree, we go into reverse gear and study the Belief Propagation messages bottom–up to calculate the conditional marginal of the root. Clearly, analysing this upwards process seems like a tall order because the tree was already exposed during the top-down phase, a challenge that is exacerbated by the presence of hard constraints. Fortunately, in Section 5 we will see how this problem can be transformed into the study of another stochastic fixed point equation that captures the effect of the children's 'nudging' their parents. This fixed point problem is amenable to the contraction method. A spatial

mixing analysis from an extremal boundary condition was previously conducted in by Dembo and Montanari [21] for the Ising model on random graphs. But of course a crucial difference is that in the Ising model the extremal boundary conditions are constant (all-$+1$ and all--1, respectively).

A second novelty of the present work is that we directly deal with the 'hard' 2-SAT problem. Montanari and Shah [39] interpolate on the 'inverse temperature' parameter $\beta > 0$, effectively working their way from smaller to larger β. Because the limits $\beta \to \infty$ and $n \to \infty$ do not commute, this approach does not seem applicable to problems with hard constraints. Furthermore, while Panchenko [40, 41] applies the Aizenman-Sims-Starr scheme to the soft constraint version, the hard problem of counting actual satisfying assignments requires a far more careful analysis. Indeed, adding one clause can shift $\log Z_\beta(\mathbf{\Phi})$ merely by $\pm\beta$. By contrast, a single additional clause could very well reduce the logarithm $\log Z(\mathbf{\Phi})$ of the number of satisfying assignments by as much as $\Omega(n)$, or even render the formula unsatisfiable. A few prior applications of the Aizenman-Sims-Starr scheme to problems with hard constraints exist [7, 15, 16], but these hinge on peculiar symmetry properties that enable an indirect approach via a 'planted' version of the problem in question. The required symmetries for this approach are absent in several important problems, with random satisfiability the most prominent example. Thus, a significant technical contribution of the present work is that we show how to apply the Aizenman-Sims-Starr scheme directly to problems with hard constraints. Among other things, this requires a careful quantification of the probabilities of rare, potentially cataclysmic events in comparison to their impact on $\log Z(\mathbf{\Phi})$. That said, we should point out that [39, 41, 48] actually also deal with the (soft) k-SAT partition function for $k > 2$ for certain regimes of clause/variable densities, while the technique that we develop here does not seem to extend beyond binary problems.

A mathematical physics technique called the interpolation method, first proposed by Guerra for the study of the Sherrington-Kirkpatrick model [31], can be applied to the random k-SAT problem [29, 42] to bound the number of satisfying assignments from above. For $k = 2$ the interpolation method yields the upper bound

$$\frac{1}{n}\log Z(\mathbf{\Phi}) \leq \inf_{\pi\in\mathscr{P}(0,1)} \mathbb{E}\left[\log\left(\prod_{i=1}^{\boldsymbol{d}^-}\boldsymbol{\mu}_{\pi,i} + \prod_{i=1}^{\boldsymbol{d}^+}\boldsymbol{\mu}_{\pi,i+\boldsymbol{d}^-}\right) - \frac{d}{2}\log\left(1-\boldsymbol{\mu}_{\pi,1}\boldsymbol{\mu}_{\pi,2}\right)\right] + o(1) \qquad \text{w.h.p.,} \tag{3.2}$$

for all $0 < d < 2$; we will revisit this bound in Section 7. Since the expression on the r.h.s. coincides with (1.2) for $\pi = \pi_d$, the main contribution of Theorem 1.1 is the matching lower bound on $\log Z(\mathbf{\Phi})$. Furthermore, Abbe and Montanari [1] used the interpolation method to establish the *existence* of a function ϕ such that

$$\lim_{n\to\infty} n^{-1}\log(Z(\mathbf{\Phi}) \vee 1) = \phi(d) \qquad \text{in probability} \tag{3.3}$$

for all but a countable number of $d \in (0,2)$. Theorem 1.1 actually determines $\phi(d)$ and shows that convergence holds for *all* $d \in (0,2)$. Clearly, (3.3) implies the concentration bound from Proposition 2.6 for all d outside the countable set. But of course we need concentration for all d, and in Section 7 we will use the upper bound (3.2) to prove this concentration result. As an aside, a conditional concentration inequality for $\log Z(\mathbf{\Phi})$, quoted in [28], was obtained by Sharell [46] (unpublished). But the necessary conditions appear to be difficult to check.

In addition, several prior contributions deal with the combinatorial problem of counting solutions to random CSPs. For problems such as k-NAESAT, k-XORSAT or graph colouring where the first moment provides the correct answer due to inherent symmetry properties, the second moment method and small subgraph conditioning yield very precise information as to the number of solutions [15, 18, 44]. Verifying that the number of solutions is determined by the physicists' 1RSB formula [34], the contribution of Sly, Sun and Zhang [47] on the random regular k-NAESAT problem near its satisfiability threshold [24] deals with an even more intricate scenario.

Finally, returning to random 2-SAT, as an intriguing question for future work determining the precise limiting distribution of $\log Z(\mathbf{\Phi})$ stands out. This random variable has standard deviation $\Omega(\sqrt{n})$ for all $0 < d < 2$ even once we condition on $\boldsymbol{m}$, as is easily seen by re-randomising the signs of the literals in small components. In effect, $\log Z(\mathbf{\Phi})$ is far less concentrated than the partition functions of symmetric random constraint satisfaction problems [15]. May $n^{-1/2}(\log Z(\mathbf{\Phi}) - \mathbb{E}[\log Z(\mathbf{\Phi})])$ be asymptotically normal?

4. Proof of Proposition 2.1

We prove Proposition 2.1 by means of a contraction argument. The starting point is the following observation. For $\ell \geq 0$ let $\pi_d^{(\ell)} = \mathrm{BP}_d^\ell(\delta_{1/2})$ be the probability measure obtained after ℓ iterations of the operator $\mathrm{BP}_d(\cdot)$.

Fact 4.1. *For all $\ell \geq 0$ the random variables $\boldsymbol{\mu}_{\pi_d^{(\ell)}}$ and $1-\boldsymbol{\mu}_{\pi_d^{(\ell)}}$ are identically distributed.*

Proof. This is because $\boldsymbol{d}^-, \boldsymbol{d}^+$ and hence the random variables

$$\left(\prod_{i=1}^{\boldsymbol{d}^-} \boldsymbol{\mu}_{\pi_d^{(\ell-1)},i}, \prod_{i=1}^{\boldsymbol{d}^-} \boldsymbol{\mu}_{\pi_d^{(\ell-1)},i} + \prod_{i=1}^{\boldsymbol{d}^+} \boldsymbol{\mu}_{\pi_d^{(\ell-1)},i+\boldsymbol{d}^-}\right) \quad \text{and} \quad \left(\prod_{i=1}^{\boldsymbol{d}^+} \boldsymbol{\mu}_{\pi_d^{(\ell-1)},i+\boldsymbol{d}^-}, \prod_{i=1}^{\boldsymbol{d}^-} \boldsymbol{\mu}_{\pi_d^{(\ell-1)},i} + \prod_{i=1}^{\boldsymbol{d}^+} \boldsymbol{\mu}_{\pi_d^{(\ell-1)},i+\boldsymbol{d}^-}\right)$$

from (1.1) are identically distributed. □

Due to Fact 4.1 we can rewrite the construction of the sequence $\pi_d^{(\ell)}$ in terms of another operator that is easier to analyse. This operator describes the expression (1.1) in terms of log-likelihood ratios, a simple reformulation that proved useful in the context of Belief Propagation for random satisfiability before [38]. Thus, we define an operator $\mathrm{LL}_d : \mathscr{P}(\mathbb{R}) \to \mathscr{P}(\mathbb{R})$, $\rho \mapsto \hat{\rho}$ by letting $\hat{\rho}$ be the distribution of the random variable

$$\sum_{i=1}^{\boldsymbol{d}} \boldsymbol{s}_i \log \frac{1 + \boldsymbol{s}'_i \tanh(\boldsymbol{\eta}_{\rho,i}/2)}{2}. \tag{4.1}$$

Further, let $\rho_d^{(\ell)} = \mathrm{LL}_d^\ell(\delta_0) \in \mathscr{P}(\mathbb{R})$ be the result of ℓ iterations of LL_d launched from the atom at zero. We recall the functions ψ, φ from (1.14). For a measure $\rho \in \mathscr{P}(\mathbb{R})$ and a measurable $f : \mathbb{R} \to \mathbb{R}$ let $f(\rho)$ denote the pushforward measure of ρ that assigns mass $\rho(f^{-1}(A))$ to Borel sets $A \subseteq \mathbb{R}$.

Lemma 4.2. *For all $\ell \geq 0$ we have $\pi_d^{(\ell)} = \psi(\rho_d^{(\ell)})$.*

Proof. Since $\psi(\delta_0) = \delta_{1/2}$, the assertion is true for $\ell = 0$. Proceeding by induction, we obtain

$$\begin{aligned}\boldsymbol{\mu}_{\pi_d^{(\ell+1)}} &\stackrel{\mathrm{d}}{=} \frac{\prod_{i=1}^{\boldsymbol{d}^+} \boldsymbol{\mu}_{\pi_d^{(\ell)},i}}{\prod_{i=1}^{\boldsymbol{d}^-} \boldsymbol{\mu}_{\pi_d^{(\ell)},i} + \prod_{i=1}^{\boldsymbol{d}^+} \boldsymbol{\mu}_{\pi_d^{(\ell)},i+\boldsymbol{d}^-}} = \psi\left(\log \frac{\prod_{i=1}^{\boldsymbol{d}^-} \boldsymbol{\mu}_{\pi_d^{(\ell)},i}}{\prod_{i=1}^{\boldsymbol{d}^+} \boldsymbol{\mu}_{\pi_d^{(\ell)},i+\boldsymbol{d}^-}}\right) \\ &= \psi\left(\sum_{i=1}^{\boldsymbol{d}^-} \log\left(\boldsymbol{\mu}_{\pi_d^{(\ell)},i}\right) - \sum_{i=1}^{\boldsymbol{d}^+} \log\left(\boldsymbol{\mu}_{\pi_d^{(\ell)},i+\boldsymbol{d}^-}\right)\right) \stackrel{\mathrm{d}}{=} \psi\left(\sum_{i=1}^{\boldsymbol{d}} \boldsymbol{s}_i \log \boldsymbol{\mu}_{\pi_d^{(\ell)},i}\right) \stackrel{\mathrm{d}}{=} \psi\left(\sum_{i=1}^{\boldsymbol{d}} \boldsymbol{s}_i \log\left(\psi(\boldsymbol{\eta}_{\rho_d^{(\ell)},i})\right)\right).\end{aligned} \tag{4.2}$$

Moreover, since $\boldsymbol{s}_i \in \{\pm 1\}$ is random, it is immediate from (4.1) that $\boldsymbol{\eta}_{\rho_d^{(\ell)},i} \stackrel{\mathrm{d}}{=} -\boldsymbol{\eta}_{\rho_d^{(\ell)},i}$. Consequently, (4.2) yields

$$\boldsymbol{\mu}_{\pi_d^{(\ell+1)}} \stackrel{\mathrm{d}}{=} \psi\left(\sum_{i=1}^{\boldsymbol{d}} \boldsymbol{s}_i \log\left(\psi(\boldsymbol{s}'_i \boldsymbol{\eta}_{\rho_d^{(\ell)},i})\right)\right) \stackrel{\mathrm{d}}{=} \psi(\boldsymbol{\eta}_{\rho_d^{(\ell+1)}}),$$

which completes the induction. □

Due to the continuous mapping theorem, to establish convergence of $(\pi_d^{(\ell)})_{\ell \geq 0}$ it suffices to show that $(\rho_d^{(\ell)})_{\ell \geq 0}$ converges weakly. To this end, we will prove that the operator $\mathrm{LL}_d(\cdot)$ is a contraction.

Lemma 4.3. *If $d < 2$, then LL_d is a contraction on the space $\mathscr{W}_2(\mathbb{R})$.*

Proof. The operator LL_d maps the space $\mathscr{W}_2(\mathbb{R})$ into itself because the derivative of $x \mapsto \log((1+\tanh(x/2))/2)$ is bounded by one in absolute value for all $x \in \mathbb{R}$. To show contraction let $\rho, \rho' \in \mathscr{W}_2(\mathbb{R})$ and consider a sequence of independent random pairs $(\boldsymbol{\eta}_i, \boldsymbol{\eta}'_i)_{i \geq 1}$ such that the $\boldsymbol{\eta}_i$ have distribution ρ and the $\boldsymbol{\eta}'_i$ have distribution ρ'. Because the signs $\boldsymbol{s}_i$ are uniform and independent, we obtain

$$\begin{aligned}W_2(\mathrm{LL}(\rho), \mathrm{LL}(\rho'))^2 &\leq \mathbb{E}\left[\left(\sum_{i=1}^{\boldsymbol{d}} \boldsymbol{s}_i \log \frac{1+\boldsymbol{s}'_i \tanh(\boldsymbol{\eta}_i/2)}{1+\boldsymbol{s}'_i \tanh(\boldsymbol{\eta}'_i/2)}\right)^2\right] = \mathbb{E}\left[\sum_{h,i=1}^{\boldsymbol{d}} \boldsymbol{s}_h \boldsymbol{s}_i \log \frac{1+\boldsymbol{s}'_h \tanh(\boldsymbol{\eta}_h/2)}{1+\boldsymbol{s}'_h \tanh(\boldsymbol{\eta}'_h/2)} \log \frac{1+\boldsymbol{s}'_i \tanh(\boldsymbol{\eta}_i/2)}{1+\boldsymbol{s}'_i \tanh(\boldsymbol{\eta}'_i/2)}\right] \\ &= \mathbb{E}\left[\sum_{i=1}^{\boldsymbol{d}} \log^2 \frac{1+\boldsymbol{s}'_i \tanh(\boldsymbol{\eta}_i/2)}{1+\boldsymbol{s}'_i \tanh(\boldsymbol{\eta}'_i/2)}\right] = d\mathbb{E}\left[\log^2 \frac{1+\boldsymbol{s}_1 \tanh(\boldsymbol{\eta}_1/2)}{1+\boldsymbol{s}_1 \tanh(\boldsymbol{\eta}'_1/2)}\right].\end{aligned} \tag{4.3}$$

Further,

$$\log^2 \frac{1+\tanh(\boldsymbol{\eta}_1/2)}{1+\tanh(\boldsymbol{\eta}'_1/2)} = \left[\int_{\boldsymbol{\eta}'_1}^{\boldsymbol{\eta}_1} \frac{\partial \log(1+\tanh(z/2))}{\partial z} \mathrm{d}z\right]^2 = \left[\int_{\boldsymbol{\eta}_1 \wedge \boldsymbol{\eta}'_1}^{\boldsymbol{\eta}_1 \vee \boldsymbol{\eta}'_1} \frac{1-\tanh(z/2)}{2} \mathrm{d}z\right]^2, \tag{4.4}$$

$$\log^2 \frac{1-\tanh(\boldsymbol{\eta}_1/2)}{1-\tanh(\boldsymbol{\eta}'_1/2)} = \left[\int_{\boldsymbol{\eta}'_1}^{\boldsymbol{\eta}_1} \frac{\partial \log(1-\tanh(z/2))}{\partial z} \mathrm{d}z\right]^2 = \left[\int_{\boldsymbol{\eta}_1 \wedge \boldsymbol{\eta}'_1}^{\boldsymbol{\eta}_1 \vee \boldsymbol{\eta}'_1} \frac{1+\tanh(z/2)}{2} \mathrm{d}z\right]^2. \tag{4.5}$$

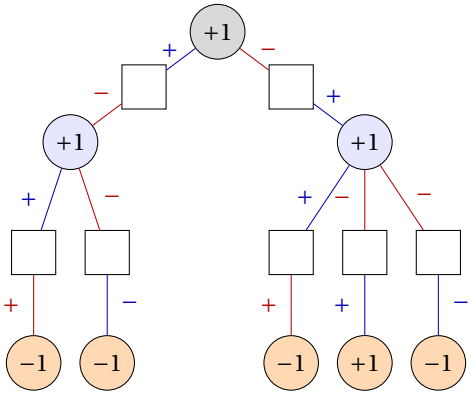

FIGURE 2. The graph $G(\boldsymbol{\Phi})$ together with extremal boundary condition $\boldsymbol{\sigma}^+$. Variables are indicated by circles and clauses by squares. The labels on the edges illustrate the sign with which variables appears in the clauses. To obtain the extremal boundary condition $\boldsymbol{\sigma}^+$ we proceed top-down. The truth values of the children are chosen so as to nudge the parent variables in the direction provided by $\boldsymbol{\sigma}^+$.

Combining (4.4)–(4.5) and applying the Cauchy-Schwarz inequality, we obtain

$$\mathbb{E}\left[\log^2\frac{1+\boldsymbol{s}_1\tanh(\boldsymbol{\eta}_1/2)}{1+\boldsymbol{s}_1\tanh(\boldsymbol{\eta}_1'/2)}\right] = \frac{1}{2}\mathbb{E}\left[\left[\int_{\boldsymbol{\eta}_1\wedge\boldsymbol{\eta}_1'}^{\boldsymbol{\eta}_1\vee\boldsymbol{\eta}_1'}\frac{1-\tanh(z/2)}{2}\mathrm{d}z\right]^2+\left[\int_{\boldsymbol{\eta}_1\wedge\boldsymbol{\eta}_1'}^{\boldsymbol{\eta}_1\vee\boldsymbol{\eta}_1'}\frac{1+\tanh(z/2)}{2}\mathrm{d}z\right]^2\right]$$
$$\leq \frac{1}{2}\mathbb{E}\left[|\boldsymbol{\eta}_1-\boldsymbol{\eta}_1'|\int_{\boldsymbol{\eta}_1\wedge\boldsymbol{\eta}_1'}^{\boldsymbol{\eta}_1\vee\boldsymbol{\eta}_1'}\left(\frac{1-\tanh(z/2)}{2}\right)^2+\left(\frac{1+\tanh(z/2)}{2}\right)^2\mathrm{d}z\right] \leq \frac{1}{2}\mathbb{E}\left[(\boldsymbol{\eta}_1-\boldsymbol{\eta}_1')^2\right]. \quad (4.6)$$

Finally, (4.3) and (4.6) yield $W_2(\mathrm{LL}(\rho),\mathrm{LL}(\rho'))^2 \leq d\mathbb{E}[(\boldsymbol{\eta}_1-\boldsymbol{\eta}_1')^2]/2$, which implies contraction because $d<2$. □

Proof of Proposition 2.1. Together with the Banach fixed point theorem Lemma 4.3 ensures that the W_2-limit $\rho_d = \lim_{\ell\to\infty}\mathrm{LL}_d^\ell(\delta_0)$ exists. Therefore, Lemma 4.2 implies that the sequence $(\pi_d^{(\ell)})_{\ell\geq 0}$ converges weakly. In addition, since $\rho_d \in \mathscr{W}_2(\mathbb{R})$, Lemma 4.2 also implies the bound (2.1). Finally, to prove (2.2) we apply (2.1) to obtain

$$\mathbb{E}\left|\log\left(\prod_{i=1}^{\boldsymbol{d}^-}\boldsymbol{\mu}_{\pi_d,i}+\prod_{i=1}^{\boldsymbol{d}^+}\boldsymbol{\mu}_{\pi_d,i+\boldsymbol{d}^-}\right)\right| \leq \log(2)-\mathbb{E}\log\prod_{i=1}^{\boldsymbol{d}^-}\boldsymbol{\mu}_{\pi_d,i} \leq \log(2)-\frac{d}{2}\mathbb{E}\log\boldsymbol{\mu}_{\pi_d,1} \leq 2\log(2)+d\mathbb{E}\left|\log\frac{\boldsymbol{\mu}_{\pi_d}}{1-\boldsymbol{\mu}_{\pi_d}}\right|<\infty,$$
$$\mathbb{E}\left|\log(1-\boldsymbol{\mu}_{\pi_d,1}\boldsymbol{\mu}_{\pi_d,2})\right| \leq \mathbb{E}\left|\log(1-\boldsymbol{\mu}_{\pi_d})\right| \leq \mathbb{E}\left|\log\frac{\boldsymbol{\mu}_{\pi_d}}{1-\boldsymbol{\mu}_{\pi_d}}\right|+\log 2<\infty,$$

thereby completing the proof. □

5. PROOF OF PROPOSITION 2.2

5.1. **Outline.** The goal is to prove that the marginal of the root variable o of $\boldsymbol{T}^{(2\ell)}$ remains asymptotically invariant even upon imposition of an arbitrary (feasible) boundary condition on the variables at distance 2ℓ from the root o. A priori, a proof of this statement seems challenging because of the very large number of possible boundary conditions. Indeed, we expect about d^ℓ variables at distance 2ℓ. But a crucial feature of the 2-SAT problem is that we can construct a pair of extremal boundary conditions. One of these maximises the probability that the root is set to one. The other one minimises that probability. As a consequence, instead of inspecting all possible boundary conditions, it suffices to show that the marginals on the root o that these two extremal boundary induce asymptotically coincide with the unconditional marginals. Of course, due to symmetry it actually suffices to consider the 'positive' extremal boundary condition that maximally nudges the root towards +1.

To construct this extremal boundary condition we define a satisfying assignment $\boldsymbol{\sigma}^+$ by working our way down the tree $\boldsymbol{T}^{(2\ell)}$. We begin by defining $\boldsymbol{\sigma}_o^+ = 1$. Further, suppose for $\ell \geq 1$ the values of the variables at distance $2(\ell-1)$ from o have been defined already. Consider a variable $v \in \partial^{2\ell} o$, its parent clause a and the parent variable u of a.

Our aim is to choose $\boldsymbol{\sigma}^+_v$ so as to 'nudge' u towards $\boldsymbol{\sigma}^+_u$ as much as possible. To this end we set $\boldsymbol{\sigma}^+_v$ so as to not satisfy a if setting u to $\boldsymbol{\sigma}^+_u$ satisfies a. Otherwise we pick the value that satisfies a; see Figure 2. In formulas,

$$\boldsymbol{\sigma}^+_v = \mathrm{sign}(a,v)\mathbf{1}\{\mathrm{sign}(a,u) \neq \boldsymbol{\sigma}^+_u\} - \mathrm{sign}(a,v)\mathbf{1}\{\mathrm{sign}(a,u) = \boldsymbol{\sigma}^+_u\}.$$

The following lemma verifies that $\boldsymbol{\sigma}^+$ is extremal, i.e., that imposing the values provided by $\boldsymbol{\sigma}^+$ on the boundary variables $\partial^{2\ell} o$ maximises the probability of the truth value 1 at the root o. The proof can be found in Section 5.2.

Lemma 5.1. *For any integer $\ell \geq 0$ we have* $\max_{\tau \in S(\boldsymbol{T}^{(2\ell)})} \mu_{\boldsymbol{T}^{(2\ell)}}(\boldsymbol{\sigma}_o = 1 \mid \boldsymbol{\sigma}_{\partial^{2\ell} o} = \tau_{\partial^{2\ell} o}) = \mu_{\boldsymbol{T}^{(2\ell)}}(\boldsymbol{\sigma}_o = 1 \mid \boldsymbol{\sigma}_{\partial^{2\ell} o} = \boldsymbol{\sigma}^+_{\partial^{2\ell} o})$.

Lemma 5.1 reduces the task of proving Proposition 2.2 to establishing the following statement.

Proposition 5.2. *We have* $\lim_{\ell\to\infty} \mathbb{E}\left|\mu_{\boldsymbol{T}^{(2\ell)}}(\boldsymbol{\sigma}_o = 1) - \mu_{\boldsymbol{T}^{(2\ell)}}(\boldsymbol{\sigma}_o = 1 \mid \boldsymbol{\sigma}_{\partial^{2\ell} o} = \boldsymbol{\sigma}^+_{\partial^{2\ell} o})\right| = 0$.

In words, the root marginal given the extremal boundary condition $\boldsymbol{\sigma}^+$ asymptotically coincides with the unconditional marginal.

The proof of Proposition 5.2 is delicate because the boundary condition $\boldsymbol{\sigma}^+$ depends on the tree $\boldsymbol{T}^{(2\ell)}$. Indeed, it seems hopeless to confront these dependencies head on by first passing down the tree to construct $\boldsymbol{\sigma}^+$ and to subsequently work up the tree to calculate marginals. To sidestep this problem we devise a quantity that recovers the Markov property of the random tree. Specifically, with each variable node $x \in \partial^{2k} o$, $k > 0$, of $\boldsymbol{T}^{(2\ell)}$ we will associate a carefully defined quantity $\boldsymbol{\eta}^{(\ell)}_x \in \mathbb{R} \cup \{\pm\infty\}$ that gauges how strongly x can nudge its (grand-)parent variable y towards the truth value mandated by $\boldsymbol{\sigma}^+_y$. This random variable $\boldsymbol{\eta}^{(\ell)}_x$ will turn out to be essentially independent of the top $2k$ levels of the tree. In effect, we will discover that the distribution of $\boldsymbol{\eta}^{(\ell)}_o$ can be approximated by the k-fold application of a suitable operator that will turn out to be a W_1-contraction. Taking limits $k, \ell \to \infty$ carefully will then complete the proof.

To facilitate this construction we need to count satisfying assignments of sub-formulas of $\boldsymbol{T}^{(2\ell)}$ subject to certain boundary conditions. Specifically, for a variable x we let $\boldsymbol{T}^{(2\ell)}_x$ be the sub-formula of $\boldsymbol{T}^{(2\ell)}$ comprising x and its progeny. Moreover, for a satisfying assignment $\tau \in S(\boldsymbol{T}^{(2\ell)})$ we let

$$S(\boldsymbol{T}^{(2\ell)}_x, \tau) = \left\{\chi \in S(\boldsymbol{T}^{(2\ell)}_x) : \forall y \in V(\boldsymbol{T}^{(2\ell)}_x) \cap \partial^{2\ell}(\boldsymbol{T}, o) : \chi_y = \tau_y\right\}, \qquad Z(\boldsymbol{T}^{(2\ell)}_x, \tau) = \left|S(\boldsymbol{T}^{(2\ell)}_x, \tau)\right|.$$

In words, $S(\boldsymbol{T}^{(2\ell)}_x, \tau)$ contains all satisfying assignments of $\boldsymbol{T}^{(2\ell)}_x$ that comply with the boundary condition induced by τ. As a final twist, for $t = \pm 1$ we also need the number

$$Z(\boldsymbol{T}^{(2\ell)}_x, \tau, t) = \left|\left\{\chi \in S(\boldsymbol{T}^{(2\ell)}_x, \tau) : \chi_x = t\right\}\right|$$

of satisfying assignments of $\boldsymbol{T}^{(2\ell)}_x$ that agree with τ on the boundary and assign value t to x.

The protagonist of the proof of Proposition 5.2 is the log-likelihood ratio

$$\boldsymbol{\eta}^{(\ell)}_x = \log \frac{Z(\boldsymbol{T}^{(2\ell)}_x, \boldsymbol{\sigma}^+, \boldsymbol{\sigma}^+_x)}{Z(\boldsymbol{T}^{(2\ell)}_x, \boldsymbol{\sigma}^+, -\boldsymbol{\sigma}^+_x)} \in \mathbb{R} \cup \{\pm\infty\} \qquad (x \in V(\boldsymbol{T}^{(2\ell)})), \tag{5.1}$$

with the conventions $\log 0 = -\infty$, $\log\infty = \infty$. Thus, $\boldsymbol{\eta}^{(\ell)}_x$ gauges how likely a random satisfying assignment $\boldsymbol{\sigma}$ of $\boldsymbol{T}^{(2\ell)}_x$ subject to the $\boldsymbol{\sigma}^+$-boundary condition is to set x to its designated value $\boldsymbol{\sigma}^+_x$.

To get a handle on the $\boldsymbol{\eta}^{(\ell)}_x$, we show that these quantities can be calculated by propagating the extremal boundary condition $\boldsymbol{\sigma}^+$ bottom–up toward the root of the tree. Specifically, we consider the operator

$$\mathrm{LL}^+_{\boldsymbol{T}^{(2\ell)}} : (-\infty,\infty]^{V(\boldsymbol{T}^{(2\ell)})} \to (-\infty,\infty]^{V(\boldsymbol{T}^{(2\ell)})}, \qquad \eta \mapsto \hat{\eta}$$

defined as follows. For all $x \in \partial^{2\ell} o$ we set $\hat{\eta}_x = \infty$. Moreover, for a variable $x \in \partial^{2k} o$ with $k < \ell$ with children $a_1, \ldots, a_j$ and grandchildren $y_1 \in \partial a_1 \setminus \{x\}, \ldots, y_j \in \partial a_j \setminus \{x\}$ we define

$$\hat{\eta}_x = -\sum_{i=1}^{j} \boldsymbol{\sigma}^+_x \,\mathrm{sign}(x, a_i) \log \frac{1 - \boldsymbol{\sigma}^+_x \,\mathrm{sign}(x, a_i)\tanh(\eta_{y_i}/2)}{2}. \tag{5.2}$$

It may not be apparent that the above sum is well-defined as a $-\infty$ summand might occur. However, the next lemma rules this out and shows that ℓ-fold iteration of $\mathrm{LL}^+_{\boldsymbol{T}^{(2\ell)}}$ from all-$+\infty$ yields $\boldsymbol{\eta}^{(\ell)} = (\boldsymbol{\eta}^{(\ell)}_x)_{x \in V(\boldsymbol{T}^{(2\ell)})}$.

Lemma 5.3. *The operator* $\mathrm{LL}^+_{\boldsymbol{T}^{(2\ell)}}$ *is well-defined and* $\mathrm{LL}^{+(\ell)}_{\boldsymbol{T}^{(2\ell)}}(\infty, \ldots, \infty) = \boldsymbol{\eta}^{(\ell)}$.

We defer the proof of Lemma 5.3 to Section 5.3.

The next aim is to approximate the ℓ-fold iteration of $\mathrm{LL}^+_{\boldsymbol{T}^{(2\ell)}}$, and specifically the distribution of the value $\boldsymbol{\eta}_o^{(\ell)}$ associated with the root, via a non-random operator $\mathscr{P}(\mathbb{R}) \to \mathscr{P}(\mathbb{R})$. To this end we need to cope with the $\pm\infty$-entries of the vector $\boldsymbol{\eta}^{(\ell)}$, a task that we solve by bounding $\boldsymbol{\eta}_x^{(\ell)}$ for variables x near the top of the tree.

Lemma 5.4. *There exist $c = c(d) > 0$ and a sequence $(\varepsilon_k)_{k\geq 1}$ with $\lim_{k\to\infty}\varepsilon_k = 0$ such that for any $k > 0$, $\ell > ck$ we have $\mathbb{P}[\max_{x\in\partial^{2k}o}|\boldsymbol{\eta}_x^{(\ell)}| \leq ck] > 1-\varepsilon_k$.*

The proof of Lemma 5.4, based on a percolation argument, can be found in Section 5.4. We continue to denote by c and $(\varepsilon_k)_k$ the number and the sequence supplied by Lemma 5.4.

Guided by Lemma 5.4 we consider the vector $\bar{\boldsymbol{\eta}}^{(\ell,k)}$ of truncated log-likelihood ratios

$$\bar{\boldsymbol{\eta}}_x^{(\ell,k)} = \begin{cases} -ck & \text{if } x\in\partial^{2k}o \text{ and } \boldsymbol{\eta}_x^{(\ell)} < -ck,\\ ck & \text{if } x\in\partial^{2k}o \text{ and } \boldsymbol{\eta}_x^{(\ell)} > ck,\\ \boldsymbol{\eta}_x^{(\ell)} & \text{otherwise.}\end{cases}$$

Further, let

$$\boldsymbol{\eta}^{(\ell,k)} = \mathrm{LL}^{+(k)}_{\boldsymbol{T}^{(2\ell)}}(\bar{\boldsymbol{\eta}}^{(\ell,k)})$$

be the result of k iterations of $\mathrm{LL}^+_{\boldsymbol{T}^{(2\ell)}}(\cdot)$ starting from $\bar{\boldsymbol{\eta}}^{(\ell,k)}$.

Corollary 5.5. *For any $\ell > ck$ we have $d_{\mathrm{TV}}(\boldsymbol{\eta}_o^{(\ell,k)}, \boldsymbol{\eta}_o^{(\ell)}) < \varepsilon_k$.*

Proof. This follows from Lemma 5.3 and Lemma 5.4, which shows that the truncation is inconsequential with probability at least $1-\varepsilon_k$. □

We are ready to introduce the operator $\mathscr{P}(\mathbb{R}) \to \mathscr{P}(\mathbb{R})$ that mimics $\mathrm{LL}^+_{\boldsymbol{T}^{(2\ell)}}$. Specifically, $\mathrm{LL}^+_d : \mathscr{P}(\mathbb{R}) \to \mathscr{P}(\mathbb{R})$ maps $\rho \in \mathscr{P}(\mathbb{R})$ to the distribution of

$$-\sum_{i=1}^{\boldsymbol{d}} \boldsymbol{s}_i \log\frac{1-\boldsymbol{s}_i\tanh(\boldsymbol{\eta}_{\rho,i}/2)}{2}. \tag{5.3}$$

We emphasise the subtle difference between (5.3) and (4.1), which involves two independent signs $\boldsymbol{s}_i, \boldsymbol{s}_i'$. The next lemma establishes the connection between the random operator $\mathrm{LL}^+_{\boldsymbol{T}^{(2\ell)}}$ and the operator LL^+_d. Namely, let $\rho^{(\ell,k)}$ be the distribution of $\boldsymbol{\eta}_o^{(\ell,k)}$. Moreover, let $\bar{\rho}^{(\ell-k)}$ be the distribution of

$$\boldsymbol{\eta}_o^{(\ell-k)}\mathbf{1}\{-ck < \boldsymbol{\eta}_o^{(\ell-k)} < ck\} + ck\mathbf{1}\{ck < \boldsymbol{\eta}_o^{(\ell-k)}\} - ck\mathbf{1}\{\boldsymbol{\eta}_o^{(\ell-k)} < -ck\},$$

i.e., the truncation of $\boldsymbol{\eta}_o^{(\ell-k)}$.

Lemma 5.6. *For $\ell > ck$ we have $\rho^{(\ell,k)} = \mathrm{LL}^{+(k)}_d(\bar{\rho}^{(\ell-k)})$.*

We prove Lemma 5.6 in Section 5.5. Recalling φ from (1.14), as in the proof of Proposition 2.1 we let $\rho_d = \varphi(\pi_d)$ be the distribution of the log-likelihood ratio $\log(\boldsymbol{\mu}_{\pi_d}/(1-\boldsymbol{\mu}_{\pi_d}))$.

Lemma 5.7. *The operator LL^+_d is a W_1-contraction with unique fixed point ρ_d.*

The proof of Lemma 5.7 can be found in Section 5.6. Let $(\rho^{(\ell)})_\ell$ be the sequence of distributions of $(\boldsymbol{\eta}_o^{(\ell)})_\ell$. As an immediate consequence we obtain the limit of the sequence $(\rho^{(\ell)})_\ell$. We recall ψ from (1.14).

Corollary 5.8. *The sequence $(\psi(\rho^{(\ell)}))_{\ell\geq 0}$ converges weakly to π_d.*

Proof. This follows from Corollary 5.5, Lemma 5.6, Lemma 5.7 and the continuous mapping theorem. □

Proof of Proposition 5.2. Set $\boldsymbol{\vartheta}_o^{(\ell)} = (\mathrm{LL}^{+(\ell)}_{\boldsymbol{T}^{(2\ell)}}(0,\dots,0))_o = \log(\mu_{\boldsymbol{T}^{(2\ell)}}(\boldsymbol{\sigma}_o = 1)/\mu_{\boldsymbol{T}^{(2\ell)}}(\boldsymbol{\sigma}_o = -1))$. Then

$$\mu_{\boldsymbol{T}^{(2\ell)}}(\boldsymbol{\sigma}_o = 1) = \psi(\boldsymbol{\vartheta}_o^{(\ell)}) \qquad \text{and} \qquad \mu_{\boldsymbol{T}^{(2\ell)}}(\boldsymbol{\sigma}_o = 1 \mid \boldsymbol{\sigma}_{\partial^{2\ell}o} = \boldsymbol{\sigma}^+_{\partial^{2\ell}o}) = \psi(\boldsymbol{\eta}_o^{(\ell)}).$$

Moreover, Lemma 5.1 shows that $0 \leq \psi(\boldsymbol{\vartheta}_o^{(\ell)}) \leq \psi(\boldsymbol{\eta}_o^{(\ell)}) \leq 1$. Further, Lemma 5.7 implies that $\psi(\boldsymbol{\vartheta}_o^{(\ell)})$ converges weakly to π_d. Finally, Corollary 5.8 implies that $\psi(\boldsymbol{\eta}_o^{(\ell)})$ also converges weakly to π_d, whence

$$\lim_{\ell\to\infty}\mathbb{E}\Big|\psi(\boldsymbol{\eta}_o^{(\ell)}) - \psi(\boldsymbol{\vartheta}_o^{(\ell)})\Big| = \lim_{\ell\to\infty}\Big|\mathbb{E}[\psi(\boldsymbol{\vartheta}_o^{(\ell)})] - \mathbb{E}[\psi(\boldsymbol{\eta}_o^{(\ell)})]\Big| = 0,$$

which directly implies the assertion. □

Proof of Proposition 2.2. The proposition follows immediately from Lemma 5.1 and Proposition 5.2. □

5.2. **Proof of Lemma 5.1.** The proof is by induction on the height of the tree. The following claim summarises the main step of the induction.

Claim 5.9. *For all $\ell \geq 0$, all variables x of $\boldsymbol{T}^{(2\ell)}$ and all satisfying assignments $\tau \in S(\boldsymbol{T}^{(2\ell)})$ we have*

$$\frac{Z(\boldsymbol{T}_x^{(2\ell)}, \tau, \boldsymbol{\sigma}_x^+)}{Z(\boldsymbol{T}_x^{(2\ell)}, \tau)} \leq \frac{Z(\boldsymbol{T}_x^{(2\ell)}, \boldsymbol{\sigma}^+, \boldsymbol{\sigma}_x^+)}{Z(\boldsymbol{T}_x^{(2\ell)}, \boldsymbol{\sigma}^+)}. \tag{5.4}$$

Proof. For boundary variables $x \in \partial^{2\ell} o$ there is nothing to show because the r.h.s. of (5.4) equals one. Hence, consider a variable $x \in \partial^{2k} o$ for some $k < \ell$. If $Z(\boldsymbol{T}_x^{(2\ell)}, \tau, \boldsymbol{\sigma}_x^+) = 0$, then (5.4) is trivially satisfied. Hence, assume that $Z(\boldsymbol{T}_x^{(2\ell)}, \tau, \boldsymbol{\sigma}_x^+) > 0$. Let $a_1^+, \ldots, a_g^+$ be the children (clauses) of x with $\mathrm{sign}(x, a_i^+) = \boldsymbol{\sigma}_x^+$. Also let $y_1, \ldots, y_g$ be the children (variables) of $a_1^+, \ldots, a_g^+$. Similarly, let $a_1^-, \ldots, a_h^-$ be the children of x with $\mathrm{sign}(x, a_i^-) = -\boldsymbol{\sigma}_x^+$ and let $z_1, \ldots, z_h$ be their children. We claim that for all $\tau \in S(\boldsymbol{T}^{(2\ell)})$,

$$Z(\boldsymbol{T}_x^{(2\ell)}, \tau, \boldsymbol{\sigma}_x^+) = \prod_{i=1}^{g} Z(\boldsymbol{T}_{y_i}^{(2\ell)}, \tau) \prod_{i=1}^{h} Z(\boldsymbol{T}_{z_i}^{(2\ell)}, \tau, \boldsymbol{\sigma}_{z_i}^+), \quad Z(\boldsymbol{T}_x^{(2\ell)}, \tau, -\boldsymbol{\sigma}_x^+) = \prod_{i=1}^{g} Z(\boldsymbol{T}_{y_i}^{(2\ell)}, \tau, -\boldsymbol{\sigma}_{y_i}^+) \prod_{i=1}^{h} Z(\boldsymbol{T}_{z_i}^{(2\ell)}, \tau). \tag{5.5}$$

For setting x to $\boldsymbol{\sigma}_x^+$ satisfies $a_1^+, \ldots, a_g^+$; hence, arbitrary satisfying assignments of the sub-trees $\boldsymbol{T}_{y_i}^{(2\ell)}$ can be combined, which explains the first product. By contrast, upon assigning x the value $\boldsymbol{\sigma}_x^+$ we need to assign the variables z_i the values $\boldsymbol{\sigma}_{z_i}^+$ so that they satisfy the clauses a_i^-. This leaves us with $Z(\boldsymbol{T}_{z_i}^{(2\ell)}, \tau, \boldsymbol{\sigma}_{z_i}^+)$ possible satisfying assignments of the sub-trees $\boldsymbol{T}_{z_i}^{(2\ell)}$; hence the second product, and we obtain the left equation. A similar argument yields the right one. Dividing the two expressions from (5.5) and invoking the induction hypothesis (for $k+1$), we obtain

$$\begin{aligned}\frac{Z(\boldsymbol{T}_x^{(2\ell)}, \tau, -\boldsymbol{\sigma}_x^+)}{Z(\boldsymbol{T}_x^{(2\ell)}, \tau, \boldsymbol{\sigma}_x^+)} &= \prod_{i=1}^{g} \frac{Z(\boldsymbol{T}_{y_i}^{(2\ell)}, \tau, -\boldsymbol{\sigma}_{y_i}^+)}{Z(\boldsymbol{T}_{y_i}^{(2\ell)}, \tau)} \cdot \prod_{i=1}^{h} \frac{Z(\boldsymbol{T}_{z_i}^{(2\ell)}, \tau)}{Z(\boldsymbol{T}_{z_i}^{(2\ell)}, \tau, \boldsymbol{\sigma}_{z_i}^+)} \\ &\geq \prod_{i=1}^{g} \frac{Z(\boldsymbol{T}_{y_i}^{(2\ell)}, \boldsymbol{\sigma}^+, -\boldsymbol{\sigma}_{y_i}^+)}{Z(\boldsymbol{T}_{y_i}^{(2\ell)}, \boldsymbol{\sigma}^+)} \cdot \prod_{i=1}^{h} \frac{Z(\boldsymbol{T}_{z_i}^{(2\ell)}, \boldsymbol{\sigma}^+)}{Z(\boldsymbol{T}_{z_i}^{(2\ell)}, \boldsymbol{\sigma}^+, \boldsymbol{\sigma}_{z_i}^+)} = \frac{Z(\boldsymbol{T}_x^{(2\ell)}, \boldsymbol{\sigma}^+, -\boldsymbol{\sigma}_x^+)}{Z(\boldsymbol{T}_x^{(2\ell)}, \boldsymbol{\sigma}^+, \boldsymbol{\sigma}_x^+)},\end{aligned}$$

completing the induction. □

Proof of Lemma 5.1. The assertion follows by applying Claim 5.9 to $x = o$. □

5.3. **Proof of Lemma 5.3.** To show that $\mathrm{LL}^+_{\boldsymbol{T}^{(2\ell)}}$ is well defined we verify that, in the notation of (5.2), $\hat{\eta}_x \in (-\infty, \infty]$ for all x. Indeed, in the expression on the r.h.s. of (5.2) a $\pm\infty$ summand can arise only from variables y_i with $\eta_{y_i} = \infty$. But the definition of $\boldsymbol{\sigma}^+$ ensures that such y_i either render a zero summand if $\boldsymbol{\sigma}_x^+ \mathrm{sign}(x, a_i) = -1$, or a $+\infty$ summand if $\boldsymbol{\sigma}_x^+ \mathrm{sign}(x, a_i) = 1$. Thus, the sum is well-defined and $\hat{\eta}_x \in (-\infty, \infty]$.

Further, to verify the identity $\boldsymbol{\eta}^{(\ell)} = \mathrm{LL}^{+(\ell)}_{\boldsymbol{T}^{(2\ell)}}(\infty, \ldots, \infty)$, consider a variable x of $\boldsymbol{T}^{(2\ell)}$. Let $a_1^+, \ldots, a_g^+$ be its children with $\mathrm{sign}(a_i^+, x) = \boldsymbol{\sigma}_x^+$, let $y_1, \ldots, y_g$ be their children, let $a_1^-, \ldots, a_h^-$ be the children of x with $\mathrm{sign}(a_i^-, x) = -\boldsymbol{\sigma}_x^+$ and let $z_1, \ldots, z_h$ be their children. Then (1.14) and (5.5) yield

$$\boldsymbol{\eta}_x^{(\ell)} = -\sum_{i=1}^{g} \log \frac{Z(\boldsymbol{T}_{y_i}^{(2\ell)}, \boldsymbol{\sigma}^+, -\boldsymbol{\sigma}_{y_i}^+)}{Z(\boldsymbol{T}_{y_i}^{(2\ell)}, \boldsymbol{\sigma}^+)} + \sum_{i=1}^{h} \log \frac{Z(\boldsymbol{T}_{z_i}^{(2\ell)}, \boldsymbol{\sigma}^+, \boldsymbol{\sigma}_{z_i}^+)}{Z(\boldsymbol{T}_{z_i}^{(2\ell)}, \boldsymbol{\sigma}^+)} = -\sum_{i=1}^{g} \log \frac{1 - \tanh(\boldsymbol{\eta}_{y_i}^{(\ell)}/2)}{2} + \sum_{i=1}^{h} \log \frac{1 + \tanh(\boldsymbol{\eta}_{z_i}^{(\ell)}/2)}{2}.$$

The assertion follows because $\mathrm{sign}(x, a_i^+)\boldsymbol{\sigma}_x^+ = 1$ and $\mathrm{sign}(x, a_i^-)\boldsymbol{\sigma}_x^+ = -1$.

5.4. **Proof of Lemma 5.4.** The goal is to prove that for variables some distance away from level 2ℓ of $\boldsymbol{T}^{(2\ell)}$ the counts $Z(\boldsymbol{T}_x^{(2\ell)}, \boldsymbol{\sigma}^+, \pm 1)$ are roughly of the same order of magnitude. Approaching this task somewhat indirectly, we begin by tracing the logical implications of imposing a specific value $s = \pm 1$ on a variable x of the (possibly infinite) tree $\boldsymbol{T}$. Clearly, upon setting x to the value s a child (clause) a of x will be satisfied iff x appears in a with sign s. In effect, all clauses a with $\mathrm{sign}(a, x) \neq s$ need to be satisfied by their second variable y, a grandchild of x. Thus, we impose the value $\mathrm{sign}(a, y)$ on y and recurse down the tree. Let $\boldsymbol{T}_{x,s}$ denote the sub-tree of $\boldsymbol{T}$ comprising x and all other variables on which this process imposes specific values as well as all clauses that contain two such variables. Clearly, for every leaf y of $\boldsymbol{T}_{x,s}$ the values imposed on y happens to satisfy all child clauses of y in $\boldsymbol{T}$. Let $\boldsymbol{N}_{x,s} \in [1, \infty]$ be the number of variables in $\boldsymbol{T}_{x,s}$. The next lemma shows that the impact of a boundary condition on the marginal of x can be bounded in terms of $\boldsymbol{N}_{x,s}$.

Claim 5.10. *Let $s \in \{\pm 1\}$. If $x \in \partial^{2k} o$ satisfies $\boldsymbol{N}_{x,s} < \ell - k$ then $Z(\boldsymbol{T}_x^{(2\ell)}, \tau) \le 2^{\boldsymbol{N}_{x,s}} Z(\boldsymbol{T}_x^{(2\ell)}, \tau, s)$.*

Proof. The construction of the implication tree $\boldsymbol{T}_{x,s}$ imposes a truth value σ_y on each variable y of the tree that y must inevitably take if x gets assigned s. Thus, $\boldsymbol{T}_{x,s}$ comes with a satisfying assignment $\sigma \in S(\boldsymbol{T}_{x,s})$ with $\sigma_x = s$. For any leaf y of $\boldsymbol{T}_{x,s}$ every child clause a of y in the super-tree $\boldsymbol{T}$ will be automatically satisfied by setting y to σ_y (because otherwise a would have been included in $\boldsymbol{T}_{x,s}$). Hence, all the clauses of $\boldsymbol{T}$ that are children of the leaves of $\boldsymbol{T}_{x,s}$ are satisfied by σ. Moreover, because $\boldsymbol{N}_{x,s} < \ell - k$, any leaf y of $\boldsymbol{T}_{x,s}$ has distance less than 2ℓ from o. Thus, the assignment σ does not clash with the boundary condition τ. As a consequence, for any $\chi \in S(\boldsymbol{T}_x^{(2\ell)}, \tau)$ we obtain another satisfying assignment $\chi' \in S(\boldsymbol{T}_x^{(2\ell)}, \tau)$ by letting

$$\chi'_z = \begin{cases} \sigma_z & \text{if } z \in V(\boldsymbol{T}_{x,s}), \\ \chi_z & \text{otherwise.} \end{cases}$$

Moreover, under the map $\chi \mapsto \chi'$ the number of inverse images of any assignment χ' is bounded by the total number $2^{\boldsymbol{N}_{x,s}}$ of different truth assignments of the variables $V(\boldsymbol{T}_{x,s})$. Therefore, $Z(\boldsymbol{T}_x^{(2\ell)}, \tau) \le 2^{\boldsymbol{N}_{x,s}} Z(\boldsymbol{T}_x^{(2\ell)}, \tau, s)$. □

As a next step we bound the random variable $\boldsymbol{N}_{x,s}$.

Claim 5.11. *There exists a number $\alpha = \alpha(d) > 0$ such that $\mathbb{P}\left[\boldsymbol{N}_{o,s} \ge u\right] \le \exp(-u\alpha)/\alpha$ for all $u \ge 0$, $s \in \{\pm 1\}$.*

Proof. In the construction of $\boldsymbol{T}_{o,s}$ we only propagate along clauses in which the parent variable is forced to take a value that fails to satisfy the clause. Since the signs are uniformly random, the number of such child clauses has distribution $\mathrm{Po}(d/2)$. Therefore, $\boldsymbol{N}_{o,s}$ is bounded by the total progeny of a Galton-Watson process with $\mathrm{Po}(d/2)$ offspring. The assertion therefore follows from the tail bound for such processes (e.g., [6, eq. (11.7)]). □

As a final preparation toward the proof of Lemma 5.4 we need a bound on the size of the $2k$-th level of $\boldsymbol{T}$.

Claim 5.12. *We have $\lim_{k\to\infty} \mathbb{P}\left[|\partial^{2k} o| > 2d^k + k\right] = 0$.*

Proof. Since every clause of $\boldsymbol{T}$ has precisely one child, the size of level $2k$ of $\boldsymbol{T}$ coincides with the size of the k-th level of a $\mathrm{Po}(d)$ Galton-Watson tree. Therefore, the assertion follows from standard tail bounds for Galton-Watson processes (e.g., [6, eq. (11.7)]). □

Proof of Lemma 5.4. Claim 5.11 ensures that for a large enough constant $c = c(d) > 0$ and all large enough k,

$$\mathbb{P}\left[\boldsymbol{N}_{o,\pm 1} \ge ck\right] \le (2d)^{-k}. \tag{5.6}$$

Combining (5.6) with Claim 5.12 and using the union bound, we obtain a sequence $\varepsilon_k \to 0$ such that

$$\mathbb{P}\left[\forall x \in \partial^{2k} o : \boldsymbol{N}_{x,\pm 1} < ck\right] \ge 1 - \varepsilon_k. \tag{5.7}$$

Further, if $x \in \partial^{2k} o$ satisfies $\boldsymbol{N}_{x,\pm 1} < ck$ and $\ell > (1+c)k$, Claim 5.10 ensures that for all $x \in \partial^{2k} o$,

$$\left|\boldsymbol{\eta}_x^{(\ell)}\right| \le \log \frac{Z(\boldsymbol{T}_x^{(2\ell)}, \boldsymbol{\sigma}^+)}{Z(\boldsymbol{T}_x^{(2\ell)}, \boldsymbol{\sigma}^+, 1)} + \log \frac{Z(\boldsymbol{T}_x^{(2\ell)}, \boldsymbol{\sigma}^+)}{Z(\boldsymbol{T}_x^{(2\ell)}, \boldsymbol{\sigma}^+, -1)} \le \boldsymbol{N}_{x,1} + \boldsymbol{N}_{x,-1} < 2ck. \tag{5.8}$$

Combining (5.7) and (5.8) completes the proof. □

5.5. **Proof of Lemma 5.6.** A straightforward induction shows that for any $p \in \mathscr{P}(\mathbb{R})$ the result $p^{(k)} = \mathrm{LL}_d^{+(k)}(p)$ of the k-fold application of LL_d^+ coincides with the distribution of the root value of the random operator $\mathrm{LL}^{+(k)}_{\boldsymbol{T}^{(2k)}}$ applied to a vector $(\boldsymbol{\eta}_x)_{x \in V(\boldsymbol{T}^{(2k)})}$ of independent samples from p. Indeed, for $k = 1$ the claim is immediate from the definitions. Moreover, for the inductive step we notice that the k-fold application of LL_d^+ comes down to applying LL_d^+ once to the outcome of the $(k-1)$-fold application. By the induction hypothesis,

$$p^{(k-1)} = \left(\mathrm{LL}^{+(k-1)}_{\boldsymbol{T}^{(2(k-1))}}(\boldsymbol{\eta}_x)_x\right)_o.$$

Finally, applying LL_d^+ to $p^{(k-1)}$ implies the assertion because the first layer of $\boldsymbol{T}^{(2k)}$ is independent of the subtrees rooted at the grandchildren $\partial^2 o$ of the root, which are distributed as independent random trees $\boldsymbol{T}^{(2(k-1))}$. The lemma follows from applying this identity to $p = \bar{\rho}^{(\ell-k)}$.

5.6. **Proof of Lemma 5.7.** The operator LL_d^+ maps the space $\mathscr{W}_1(\mathbb{R})$ into itself because the derivative of $x \mapsto \log((1-\tanh(x/2))/2)$ is bounded by one in absolute value for all $x \in \mathbb{R}$. We proceed to show that $\mathrm{LL}_d^+ : \mathscr{W}_1(\mathbb{R}) \to \mathscr{W}_1(\mathbb{R})$ is a contraction. Thus, consider a sequence of independent random pairs $(\boldsymbol{\eta}_i, \boldsymbol{\eta}_i')_{i\geq 1}$ with $\boldsymbol{\eta}_i \stackrel{\mathrm{d}}{=} \rho$, $\boldsymbol{\eta}_i' \stackrel{\mathrm{d}}{=} \rho'$. Then

$$W_1(\mathrm{LL}_d^+(\rho), \mathrm{LL}_d^+(\rho')) \leq \mathbb{E}\left|\sum_{i=1}^{\boldsymbol{d}} \boldsymbol{s}_i \log\frac{1-\boldsymbol{s}_i\tanh(\boldsymbol{\eta}_i/2)}{1-\boldsymbol{s}_i\tanh(\boldsymbol{\eta}_i'/2)}\right| \leq d\mathbb{E}\left|\log\frac{1-\boldsymbol{s}_1\tanh(\boldsymbol{\eta}_1/2)}{1-\boldsymbol{s}_1\tanh(\boldsymbol{\eta}_1'/2)}\right|.$$

Since the function $z \mapsto \log(1+\tanh(z/2))$ is monotonically increasing, we obtain

$$\left|\log\frac{1+\tanh(\boldsymbol{\eta}_1/2)}{1+\tanh(\boldsymbol{\eta}_1'/2)}\right| = \left|\int_{\boldsymbol{\eta}_1'}^{\boldsymbol{\eta}_1} \frac{\partial\log(1+\tanh(z/2))}{\partial z}\mathrm{d}z\right| = \int_{\boldsymbol{\eta}_1\wedge\boldsymbol{\eta}_1'}^{\boldsymbol{\eta}_1\vee\boldsymbol{\eta}_1'} \frac{1-\tanh(z/2)}{2}\mathrm{d}z,$$
$$\left|\log\frac{1-\tanh(\boldsymbol{\eta}_1/2)}{1-\tanh(\boldsymbol{\eta}_1'/2)}\right| = \left|\int_{\boldsymbol{\eta}_1'}^{\boldsymbol{\eta}_1} \frac{\partial\log(1-\tanh(z/2))}{\partial z}\mathrm{d}z\right| = \int_{\boldsymbol{\eta}_1\wedge\boldsymbol{\eta}_1'}^{\boldsymbol{\eta}_1\vee\boldsymbol{\eta}_1'} \frac{1+\tanh(z/2)}{2}\mathrm{d}z.$$

Hence, $W_1(\mathrm{LL}_d^+(\rho), \mathrm{LL}_d^+(\rho')) \leq d\mathbb{E}\left|\boldsymbol{\eta}_1 - \boldsymbol{\eta}_1'\right|/2$ and therefore $W_1(\mathrm{LL}_d^+(\rho), \mathrm{LL}_d^+(\rho')) \leq dW_1(\rho,\rho')/2$.

Finally, we observe that ρ_d is a fixed point of LL_d^+. Indeed, Proposition 2.1 implies that $\boldsymbol{\eta}^{\rho_d}$ and $-\boldsymbol{\eta}^{\rho_d}$ are identically distributed. Therefore, if $\boldsymbol{s}_i, \boldsymbol{s}_i' \in \{\pm 1\}$ are uniform and independent, we obtain

$$\boldsymbol{s}_i \log\Big(\Big(1-\boldsymbol{s}_i\tanh(\boldsymbol{\eta}_{\rho_d,i}/2)\Big)/2\Big) \stackrel{\mathrm{d}}{=} \boldsymbol{s}_i \log\Big(\Big(1+\boldsymbol{s}_i'\tanh(\boldsymbol{\eta}_{\rho_d,i}/2)\Big)/2\Big).$$

Hence, recalling the definitions (4.1) and (5.3) of the operators, we see that $\mathrm{LL}_d^+(\rho_d) = \mathrm{LL}_d(\rho_d) = \rho_d$.

5.7. **Proof of Theorem 1.2.** Consider the sub-formula $\nabla^{2\ell}(\boldsymbol{\Phi}, x_1)$ of $\boldsymbol{\Phi}$ obtained by deleting all clauses and variables at distance greater than 2ℓ from x_1. By design, we can couple $\nabla^{2\ell}(\boldsymbol{\Phi}, x_1)$ and $\boldsymbol{T}^{(2\ell)}$ such that both coincide w.h.p. Therefore, since any satisfying assignment of $\boldsymbol{\Phi}$ induces a satisfying assignment of $\boldsymbol{T}^{(2\ell)}$, Proposition 2.2 implies the Gibbs uniqueness property (1.11). Furthermore, because Proposition 1.4 shows that Belief Propagation correctly computes the root marginal $\mu_{\boldsymbol{T}^{(2\ell)}}(\boldsymbol{\sigma}_o = 1)$, (1.9) follows from (1.11).

5.8. **Proof of Corollary 1.3.** Let $\pi_d^{(\ell)} = \mathrm{BP}^{(\ell)}(\delta_{1/2})$. Thanks to Proposition 2.1 it suffices to prove that

$$\lim_{\ell\to\infty}\limsup_{n\to\infty}\mathbb{E}[W_1(\pi_{\boldsymbol{\Phi}}, \pi_d^{(\ell)})] = 0. \tag{5.9}$$

Hence, fix $\varepsilon > 0$, pick a large $\ell = \ell(\varepsilon) > 0$ and a larger $L = L(\ell) > 0$. A routine second moment calculation shows that for any possible outcome T of $\boldsymbol{T}^{(2\ell)}$ the number X_T of variables x_i of $\boldsymbol{\Phi}$ such that $\nabla^{2\ell}(\boldsymbol{\Phi}, x_i) = T$ satisfies $X_T = n\mathbb{P}\left[\boldsymbol{T}^{(2\ell)} = T\right] + o(n)$ w.h.p. Hence, w.h.p. $\boldsymbol{\Phi}$ admits a coupling $\gamma_{\boldsymbol{\Phi}}$ of $\boldsymbol{T}^{(2\ell)}$ and a uniform variable $\boldsymbol{i}$ on $[n]$ such that $\gamma(\{\nabla^{2\ell}(\boldsymbol{\Phi}, x_{\boldsymbol{i}}) = \boldsymbol{T}^{(2\ell)}\}) = 1 - o(1)$. Further, Theorem 1.2 implies that given $\nabla^{2\ell}(\boldsymbol{\Phi}, x_{\boldsymbol{i}}) = \boldsymbol{T}^{(2\ell)}$ we have

$$\mathbb{P}\left[\left|\mu_{\boldsymbol{\Phi}}(\boldsymbol{\sigma}_{x_i} = 1) - \mu_{\boldsymbol{T}^{(2\ell)}}(\boldsymbol{\tau}_o = 1)\right| > \varepsilon\right] < \varepsilon, \tag{5.10}$$

provided ℓ is large enough. Finally, Lemma 1.4 implies together with a straightforward induction on ℓ that $\pi_d^{(\ell)}$ is the distribution of $\mu_{\boldsymbol{T}^{(2\ell)}}(\boldsymbol{\tau}_o = 1)$. Therefore, (5.9) follows from (5.10).

5.9. **Proof of Corollary 2.3.** Fix $\varepsilon > 0$ and pick a small $\xi = \xi(\varepsilon) > 0$ and large $\ell = \ell(\xi) > 0$. Since k is fixed independently of n, Theorem 1.2 shows that w.h.p.

$$\sum_{i=1}^{k}\max_{\tau\in S(\boldsymbol{\Phi})}\left|\mu_{\boldsymbol{\Phi}}(\boldsymbol{\sigma}_{x_i} = 1 \mid \boldsymbol{\sigma}_{\partial^{2\ell}x_i} = \tau_{\partial^{2\ell}x_i}) - \mu_{\boldsymbol{\Phi},x_i}^{(\ell)}(1)\right| < \xi. \tag{5.11}$$

Further, the smallest pairwise distance between $x_1,\ldots,x_n$ exceeds 4ℓ w.h.p. Therefore, we can draw a sample $\boldsymbol{\sigma}$ from $\mu_{\boldsymbol{\Phi}}$ in two steps. First, draw $\boldsymbol{\sigma}'$ from $\mu_{\boldsymbol{\Phi}}$. Then, independently re-sample assignments of all the variables in $\nabla^{2\ell-2}(\boldsymbol{\Phi}, x_i)$ from $\mu_{\boldsymbol{\Phi}}(\cdot\,|\boldsymbol{\sigma}'_{\partial^{2\ell}x_i})$ for $i = 1,\ldots,k$. The resulting assignment $\boldsymbol{\sigma}''$ has distribution $\mu_{\boldsymbol{\Phi}}$ and the values $\boldsymbol{\sigma}''_{x_i}$, $i \in [k]$, are mutually independent given $\boldsymbol{\sigma}'$. Finally, since (5.11) shows that conditioning on the boundary conditions $\boldsymbol{\sigma}'_{\partial^{2\ell}x_i}$ is inconsequential w.h.p., we obtain the assertion by taking $\varepsilon \to 0$ sufficiently slowly.

6. Proof of Proposition 2.4

6.1. **Outline.** The proof is based on a natural coupling of the random formulas $\mathbf{\Phi}_n$ and $\mathbf{\Phi}_{n+1}$ with n and $n+1$ variables, respectively. Specifically, let

$$\boldsymbol{m}' \stackrel{\mathrm{d}}{=} \mathrm{Po}(dn/2 - d/2), \qquad \mathbf{\Delta}'' \stackrel{\mathrm{d}}{=} \mathrm{Po}(d/2), \qquad \mathbf{\Delta}''' \stackrel{\mathrm{d}}{=} \mathrm{Po}(d) \tag{6.1}$$

be independent random variables. Moreover, let $\mathbf{\Phi}'$ be a random formula with n variables and $\boldsymbol{m}'$ clauses, chosen independently and uniformly from the set of all $4n(n-1)$ possible clauses. Then obtain $\mathbf{\Phi}''$ from $\mathbf{\Phi}'$ by adding another $\mathbf{\Delta}''$ uniformly random and independent clauses. Moreover, obtain $\mathbf{\Phi}'''$ from $\mathbf{\Phi}'$ by adding one variable x_{n+1} along with $\mathbf{\Delta}'''$ clauses, chosen uniformly and independently from the set of all $8n$ possible clauses that contain x_{n+1} and another variable from the set $\{x_1, \ldots, x_n\}$.

Fact 6.1. *We have $\mathbf{\Phi}'' \stackrel{d}{=} \mathbf{\Phi}_n$ and $\mathbf{\Phi}''' \stackrel{d}{=} \mathbf{\Phi}_{n+1}$; therefore,*

$$\mathbb{E}[\log(Z(\mathbf{\Phi}_{n+1}) \vee 1)] - \mathbb{E}[\log(Z(\mathbf{\Phi}_n) \vee 1)] = \mathbb{E}\left[\log \frac{Z(\mathbf{\Phi}''') \vee 1}{Z(\mathbf{\Phi}') \vee 1}\right] - \mathbb{E}\left[\log \frac{Z(\mathbf{\Phi}'') \vee 1}{Z(\mathbf{\Phi}') \vee 1}\right]. \tag{6.2}$$

Hence, the proof of Proposition 2.4 boils down to establishing the following two statements.

Proposition 6.2. *We have* $\lim_{n\to\infty} \mathbb{E}\log \frac{Z(\mathbf{\Phi}'') \vee 1}{Z(\mathbf{\Phi}') \vee 1} = \frac{d}{2}\mathbb{E}\left[\log\left(1 - \boldsymbol{\mu}_{\pi_d,1}\boldsymbol{\mu}_{\pi_d,2}\right)\right]$.

Proposition 6.3. *We have* $\lim_{n\to\infty} \mathbb{E}\log \frac{Z(\mathbf{\Phi}''') \vee 1}{Z(\mathbf{\Phi}') \vee 1} = \mathbb{E}\left[\log\left(\sum_{\sigma\in\{\pm1\}} \prod_{i=1}^{\boldsymbol{d}} \left(1 - \mathbf{1}\{\sigma \neq \boldsymbol{s}_i\}\boldsymbol{\mu}_{\pi_d,i}\right)\right)\right]$.

Further, to prove Propositions 6.2 and 6.3 we 'just' need to understand the impact of a bounded expected number of 'local' changes (such as adding a random clause) on the partition function.

The proof strategy sketched in the previous paragraph is known as the Aizenman-Sims-Starr scheme. The technique was originally deployed to study the Sherrington-Kirkpatrick spin glass model [5], but has since found various applications to models on sparse random graphs (e.g., [16, 40]). By comparison to prior applications, the difficulty here is that we apply this technique to a model with hard constraints. In effect, while typically the addition of a single clause will only reduce the number of satisfying assignments by a bounded factor, occasionally a much larger change might ensue. For instance, for any $0 < d < 2$ there is a small but non-zero probability that a single additional clause might close a 'bicycle', i.e., a sequence of clauses that induce an implication chain $x_i \to \cdots \to \neg x_i \to \cdots \to x_i$. Thus, a single unlucky clause might wipe out all satisfying assignments.

Suppose we wish to roughly estimate the change in the number of satisfying assignments upon going from $\mathbf{\Phi}'$ to $\mathbf{\Phi}'''$. Clearly $Z(\mathbf{\Phi}''') \leq 2Z(\mathbf{\Phi}')$ because we only add one new variable. But of course $Z(\mathbf{\Phi}''')$ might be much smaller than $Z(\mathbf{\Phi}')$. To obtain a bound, consider the new clauses $b_1, \ldots, b_{\mathbf{\Delta}'''}$ that were added along with x_{n+1} and let $y_1, \ldots, y_{\mathbf{\Delta}'''}$ be the variables of $\mathbf{\Phi}'$ where the new clauses attach. Define an assignment $\chi : Y = \{y_1, \ldots, y_{\mathbf{\Delta}'''}\} \to \{\pm1\}$ by letting $\chi_{y_i} = \mathrm{sign}(y_i, b_i)$; thus, χ satisfies the b_i. Further, let

$$S(\mathbf{\Phi}', \chi) = \left\{\sigma \in S(\mathbf{\Phi}') : \forall y \in Y : \sigma_y = \chi_y\right\}, \qquad Z(\mathbf{\Phi}', \chi) = |S(\mathbf{\Phi}', \chi)|$$

be the set and the number of satisfying assignments of $\mathbf{\Phi}'$ that coincide with χ on Y. Because each $\sigma \in S(\mathbf{\Phi}', \chi)$ already satisfies all the new clauses regardless of the value assigned to x_{n+1}, we obtain $Z(\mathbf{\Phi}''') \geq 2Z(\mathbf{\Phi}', \chi)$. Hence, it seems that we just need to lower bound $Z(\mathbf{\Phi}', \chi)$.

To this end we could employ a process similar to the one that we applied in Section 5.4 to the tree $\boldsymbol{T}$. Generally, let $Y \subseteq \{x_1, \ldots, x_n\}$ be a set of variables and let $\chi \in \{\pm1\}^Y$ be an assignment. The following process, known as the Unit Clause Propagation algorithm [26], chases the implications of imposing the assignment χ on Y:

> while $\mathbf{\Phi}'$ possesses a clause a that has exactly one neighbouring variable $z \in \partial a$ on which the value $-\mathrm{sign}(z, a)$ has been imposed, impose the value $\mathrm{sign}(a, z')$ on the second variable $z' \in \partial a \setminus \{z\}$ of a.

Let $\mathscr{I}_\chi$ be the set of variables on which the process has imposed a value upon termination (including the initial set Y). Unfortunately, it is possible that $\mathbf{\Phi}'$ contains a clause a on whose both variables z, z' the 'wrong' values $-\mathrm{sign}(a, z), -\mathrm{sign}(a, z')$ got imposed. In other words, Unit Clause might be left with contradictions. If such a clause exists we let $\boldsymbol{I}_\chi = n$. Otherwise we set $\boldsymbol{I}_\chi = |\mathscr{I}_\chi|$. We obtain the following lower bound on $Z(\mathbf{\Phi}', \chi)$.

Fact 6.4. *We have $Z(\mathbf{\Phi}') \leq 2^{\boldsymbol{I}_\chi}(Z(\mathbf{\Phi}', \chi) \vee 1)$.*

Proof. The inequality is trivially satisfied if $Z(\mathbf{\Phi}')=0$ or $\boldsymbol{I}_\chi = n$. Hence, we may assume that $Z(\mathbf{\Phi}')>0$ and that Unit Clause did not run into a contradiction. Consequently, Unit Clause produced an assignment χ^* of the variables $\mathscr{I}_\chi$ that satisfies all clauses a of $\mathbf{\Phi}'$ with $\partial a \cap \mathscr{I}_\chi \neq \emptyset$. Hence, for any satisfying assignment $\sigma \in S(\mathbf{\Phi}')$ we obtain another satisfying assignment $\hat\sigma \in S(\mathbf{\Phi}',\chi)$ by letting $\hat\sigma = \chi^*_x \mathbf{1}\{x \in \mathscr{I}_\chi\} + \sigma_x \mathbf{1}\{x \notin \mathscr{I}_\chi\}$, i.e., we overwrite the variables in $\mathscr{I}_\chi$ according to χ^*. Clearly, under the map $\sigma \mapsto \hat\sigma$ an assignment $\hat\sigma \in S(\mathbf{\Phi}',\chi)$ has at most $2^{\boldsymbol{I}_\chi}$ inverse images. □

Hence, we need an upper bound on $\boldsymbol{I}_\chi$, which will be proven at the end of Section 6.2.

Lemma 6.5. *There exists $C = C(d) > 0$ such that for every set $Y \subseteq \{x_1,\ldots,x_n\}$ of size $|Y| \le \log^2 n$ and any $\chi \in \{\pm1\}^Y$ we have $\mathbb{E}[\boldsymbol{I}_\chi] \le C|Y|^2$.*

Unfortunately, this first moment bound does not quite suffice for our purposes. Indeed, Lemma 6.5 allows for the possibility that $\boldsymbol{I}_\chi = n$ with probability $\Omega(1/n)$. In combination with Fact 6.4 this rough bound would lead to error terms that eclipse the 'main' terms displayed in Propositions 6.2 and 6.3. But we cannot hope for a much better bound on $\boldsymbol{I}_\chi$. Indeed, $\mathbb{P}\left[\boldsymbol{I}_\chi = n\right] = \Omega(1/n)$ because the graph $G(\mathbf{\Phi}')$ likely contains a few short cycles and if Y contains a variable on a short cycle, then there is a $\Omega(1)$ probability that Unit Clause will cause a contradiction.

Hence, we need to be more circumspect. Previously we aimed for an assignment χ that satisfied *all* the new clauses $b_1,\ldots,b_{\Delta'''}$ added upon going to $\mathbf{\Phi}'''$. But we still have the new variable x_{n+1} at our disposal to at least satisfy a single clause b_i. Hence, we can afford to start Unit Clause from an assignment χ' that differs from χ on a single variable. Thus, for a set Y of variables and $\chi \in \{\pm1\}^Y$ we define

$$\boldsymbol{A}_\chi = \min\left\{\boldsymbol{I}_{\chi'} : \chi' \in \{\pm1\}^Y,\ \sum_{y\in Y}\mathbf{1}\{\chi_y \neq \chi'_y\} \le 1\right\}. \tag{6.3}$$

Lemma 6.6. *There exists $C' = C'(d) > 0$ such that for every set $Y \subseteq \{x_1,\ldots,x_n\}$ of size $|Y| \le \log^2 n$ and any $\chi \in \{\pm1\}^Y$ we have $\mathbb{E}[\boldsymbol{A}_\chi^2] \le C'|Y|^4$.*

This second moment bound significantly improves over Lemma 6.5. For instance, Lemma 6.6 implies that the probability of an enormous drop $Z(\mathbf{\Phi}''') \le \exp(-\Omega(n))Z(\mathbf{\Phi}')$ is bounded by $O(n^{-2})$. Once more this estimate is about tight because there is an $\Omega(n^{-2})$ probability that a single new clause closes a bicycle. As we shall see, with a bit of care the bound from Lemma 6.6 suffices to prove Propositions 6.2 and 6.3. Yet Lemma 6.5 has its uses, too, as it implies the following vital tail bound.

Corollary 6.7. *We have* $\limsup_{n\to\infty}\mathbb{E}\left[n \wedge \left|\log\frac{\mu_{\mathbf{\Phi}'}(\boldsymbol{\sigma}_{x_1}=1)}{\mu_{\mathbf{\Phi}'}(\boldsymbol{\sigma}_{x_1}=-1)}\right| \mid Z(\mathbf{\Phi}')>0\right] < \infty$.

We proceed to study Unit Clause Propagation in order to prove Lemmas 6.5, 6.6 and Corollary 6.7. Then we will prove Propositions 6.2 and 6.3, which imply Proposition 2.4.

6.2. **Unit Clause Propagation.** To avoid dependencies we consider a binomial model $\mathbf{\Phi}^\dagger$ of a random 2-SAT formula with variables $x_1,\ldots,x_n$, where each of the $4\binom{n}{2}$ possible (unordered) 2-clauses is present with probability

$$p = d/(4n) + n^{-4/3} \tag{6.4}$$

independently. We define a random variable $\boldsymbol{A}^\dagger_\chi$ on $\mathbf{\Phi}^\dagger$ in perfect analogy to $\boldsymbol{A}_\chi$. Since the choice (6.4) of p ensures that $\mathbf{\Phi}^\dagger$ and $\mathbf{\Phi}'$ can be coupled so that the former has more clauses than the latter with probability $1-o(n^{-2})$, it suffices to analyse $\boldsymbol{A}^\dagger_\chi$. Moreover, thanks to symmetry it suffices to prove Lemmas 6.5 and 6.6 under the assumption that the initial set of variables is $Y = \{x_1,\ldots,x_\ell\}$, $\ell \le \log^2 n$.

At first glance investigating $\boldsymbol{A}^\dagger_\chi$ appears to be complicated by the fact that (6.3) takes the minimum over all possible χ'. To sidestep this issue we will investigate a 'comprehensive' propagation process whose progeny encompasses all the unit clauses that may result from any χ'. In its first round this process pursues for each variable x_i, $i \le \ell$, the Unit Clauses created by imposing either of the two possible truth values on x_i. The effect will be the imposition of truth values on all variables at distance two from Y. Subsequently we trace Unit Clause Propagation from the values imposed on the variables in $\partial^2 Y$. Hence, the difficulty of considering all χ' as in (6.3) disappears because the first step disregards χ.

To deal with possible contradictions the process will actually operate on literals rather than variables. Throughout each literal will belong to one of three possible categories: unexplored, explored, or finished. Initially the 2ℓ literals $x_1,\neg x_1,\ldots,x_\ell,\neg x_\ell$ qualify as explored and all others as unexplored. Formally, we let $\mathscr{E}_0 = \{x_1,\neg x_1,\ldots,x_\ell,\neg x_\ell\}$,

$\mathscr{U}_0 = \{x_{\ell+1}, \neg x_{\ell+1}, \ldots, x_n, \neg x_n\}$ and $\mathscr{F}_0 = \emptyset$. Further, for $t \geq 0$ we construct $\mathscr{E}_{t+1}, \mathscr{U}_{t+1}, \mathscr{F}_{t+1}$ as follows. If $\mathscr{E}_t = \emptyset$, the process has terminated and we set $\mathscr{E}_{t+1} = \mathscr{E}_t, \mathscr{U}_{t+1} = \mathscr{U}_t, \mathscr{F}_{t+1} = \mathscr{F}_t$. Otherwise, pick a literal $l_{t+1} \in \mathscr{E}_t$ and let $\mathscr{E}'_{t+1}$ be the set of all literals $l' \in \mathscr{U}_t$ such that $\mathbf{\Phi}^\dagger$ features the clause $\neg l_{t+1} \vee l'$. Further, let

$$\mathscr{U}_{t+1} = \mathscr{U}_t \setminus \mathscr{E}'_{t+1}, \qquad \mathscr{E}_{t+1} = (\mathscr{E}_t \cup \mathscr{E}'_{t+1}) \setminus \{l_{t+1}\}, \qquad \mathscr{F}_{t+1} = \mathscr{F}_t \cup \{l_{t+1}\}.$$

Finally, the set $\mathscr{F}_\infty = \bigcup_{t \geq 1} \mathscr{F}_t$ contains all literals upon which Unit Clause could impose the value 'true' from any initial assignment χ. A contradiction might result only if $x_i, \neg x_i \in \mathscr{F}_\infty$ for some $i > \ell$.

Claim 6.8. *For all $T > 8\ell/(2-d)$ we have $\mathbb{P}[|\mathscr{F}_\infty| > T] \leq \exp(-dT/36)$.*

Proof. Let $t \geq 0$. Given $|\mathscr{U}_t|$ and $|\mathscr{E}_t|$ we have

$$\boldsymbol{X}_{t+1} = |\mathscr{E}_{t+1}| - |\mathscr{E}_t| + \mathbf{1}\{\mathscr{E}_t \neq \emptyset\} \stackrel{d}{=} \mathrm{Bin}\left(|\mathscr{U}_t| \mathbf{1}\{|\mathscr{E}_t| \geq 0\}, p\right).$$

Moreover, given $|\mathscr{U}_t|$ and $|\mathscr{E}_t|$ let $\boldsymbol{Y}_{t+1} \stackrel{d}{=} \mathrm{Bin}\left(2n - |\mathscr{U}_t| \mathbf{1}\{|\mathscr{E}_t| \geq 0\}, p\right)$ be independent of $\boldsymbol{X}_{t+1}$ and everything else, and set $\boldsymbol{X}^{\geq}_{t+1} = \boldsymbol{X}_{t+1} + \boldsymbol{Y}_{t+1}$. Then $(\boldsymbol{X}^{\geq}_t)_{t \geq 1}$ is an i.i.d. sequence of $\mathrm{Bin}(2n, p)$ random variables such that $\boldsymbol{X}^{\geq}_t \geq \boldsymbol{X}_t$ for all t. Hence, for any $T \geq 1$,

$$\mathbb{P}[|\mathscr{F}_\infty| > T] = \mathbb{P}[|\mathscr{E}_T| > 0] \leq \mathbb{P}\left[\sum_{t=1}^{T} \boldsymbol{X}_t > T - 2\ell\right] \leq \mathbb{P}\left[\sum_{t=1}^{T} \boldsymbol{X}^{\geq}_t > T - 2\ell\right] = \mathbb{P}\left[\mathrm{Bin}(2nT, p) > T - 2\ell\right]. \tag{6.5}$$

Further, the Chernoff bound shows that for $T > 8\ell/(2-d)$ (and n large enough),

$$\mathbb{P}\left[\mathrm{Bin}(2Tdn, p) > T - 2\ell\right] \leq \exp\left(-\min\left\{(d - n^{-4/3}), (d - n^{-4/3})^2\right\} \frac{2nTp}{3}\right) \leq \exp\left(-\frac{dT}{36}\right), \tag{6.6}$$

Combining (6.5) and (6.6) completes the proof. □

Let $\mathbf{\Phi}^*$ be the sub-formula of $\mathbf{\Phi}^\dagger$ comprising all variables x such that $x \in \mathscr{F}_\infty$ or $\neg x \in \mathscr{F}_\infty$ along with all clauses a that contain two such variables. Let $\boldsymbol{n}^*$ be the number of variables of $\mathbf{\Phi}^*$ and let $\boldsymbol{m}^*$ be the number of clauses.

Claim 6.9. *We have $\mathbb{P}[\boldsymbol{m}^* \geq \boldsymbol{n}^* - \ell + 1] \leq O(\ell^2/n)$ and $\mathbb{P}[\boldsymbol{m}^* > \boldsymbol{n}^* - \ell + 1] \leq O(\ell^4/n^2)$.*

Proof. We set up a graph representing the literals involved in the exploration process and the clauses that contain such literals. Specifically, let $\neg\mathscr{F}_\infty = \{\neg l : l \in \mathscr{F}_\infty\}$ contain all negations of literals in $\mathscr{F}_\infty$. Moreover, let $\mathscr{G}$ be the graph whose vertices are the literals $\mathscr{F}_\infty \cup \neg\mathscr{F}_\infty$ as well as all clauses a of $\mathbf{\Phi}^\dagger$ that consist of two literals from $\mathscr{F}_\infty \cup \neg\mathscr{F}_\infty$. Let $\mathscr{C}_\infty$ be the set of such clauses a. For each clause $a \in \mathscr{C}_\infty$ the graph $\mathscr{G}$ contains two edges joining a and its two constituent literals. The graph $G(\mathbf{\Phi}^*)$ that we are ultimately interested in results from $\mathscr{G}$ by contracting pairs of inverse literals $l, \neg l \in \mathscr{F}_\infty \cup \neg\mathscr{F}_\infty$.

A large excess $\boldsymbol{m}^* - \boldsymbol{n}^*$ can either caused by the presence of atypically many clauses in $\mathscr{G}$ or by excess pairs of inverse litetals that get contracted. We first address the gain in clauses due to inclusion of $\neg\mathscr{F}_\infty$ and all induced clauses. The exploration process discovers each literal $\lambda \in \mathscr{F}_\infty \setminus \{x_1, \neg x_1, \ldots, x_\ell, \neg x_\ell\}$ via a clause $\neg l_t \vee \lambda$, where $\neg l_t \in \mathscr{E}_{t-1}$. Thus, $|\mathscr{C}_\infty| \geq |\mathscr{F}_\infty| - 2\ell$. Hence, the random variable $\boldsymbol{X} = |\mathscr{C}_\infty| - |\mathscr{F}_\infty| + 2\ell$ accounts for the number of excess clauses that are present among the literals $\mathscr{F}_\infty \cup \neg\mathscr{F}_\infty$ but that were not probed by the process. We highlight that $\boldsymbol{X}$ also counts clauses that contain two literals from the seed set $\{x_1, \neg x_1, \ldots, x_\ell, \neg x_\ell\}$. Because clauses appear in $\mathbf{\Phi}^\dagger$ independently with probability $p = O(d/n)$, we obtain the bounds

$$\mathbb{P}[\boldsymbol{X} \geq 1 \mid |\mathscr{F}_\infty|] \leq O(|\mathscr{F}_\infty|^2/n), \qquad \mathbb{P}[\boldsymbol{X} \geq 2 \mid |\mathscr{F}_\infty|] \leq O(|\mathscr{F}_\infty|^4/n^2). \tag{6.7}$$

Secondly, we investigate the loss in nodes due to contraction. Hence, $\boldsymbol{n}^* = |\mathscr{F}_\infty \cup \neg\mathscr{F}_\infty|/2$. By construction, the seeds $x_1, \neg x_1, \ldots, x_\ell, \neg x_\ell$ come in pairs. Let $\boldsymbol{X}' = \frac{1}{2}|\mathscr{F}_\infty \cap \neg\mathscr{F}_\infty| - \ell$ count the number of excess inverse literal pairs that we need to contract. Since the process is oblivious to the identities of the variables underlying the literals, given its size the set $\mathscr{F}_\infty \setminus \{x_1, \neg x_1, \ldots, x_\ell, \neg x_\ell\}$ is a uniformly random subset of the set $\{x_i, \neg x_i : \ell < i \leq n\}$ of non-seed literals. Therefore, a routine balls-into-bins argument shows that

$$\mathbb{P}[\boldsymbol{X}' \geq 1 \mid |\mathscr{F}_\infty|] \leq O(|\mathscr{F}_\infty|^2/n), \qquad \mathbb{P}[\boldsymbol{X}' \geq 2 \mid |\mathscr{F}_\infty|] \leq O(|\mathscr{F}_\infty|^4/n^2). \tag{6.8}$$

Finally, in order to estimate $\boldsymbol{m}^* - \boldsymbol{n}^*$ we consider four separate cases.

Case 1: $\boldsymbol{X} = \boldsymbol{X}' = 0$: Since $\boldsymbol{X} = 0$ the graph $\mathscr{G}$ is a forest with 2ℓ components rooted at $x_1, \neg x_1, \ldots, x_\ell, \neg x_\ell$. Moreover, since $\boldsymbol{X}' = 0$ we have $\mathscr{F}_\infty \cap \neg\mathscr{F}_\infty = \{x_1, \neg x_1, \ldots, x_\ell, \neg x_\ell\}$. Therefore, $G(\boldsymbol{\Phi}^*)$ is obtained from $\mathscr{G}$ by identifying the pairs $x_i, \neg x_i$ for $i = 1, \ldots, \ell$. Hence, $G(\boldsymbol{\Phi}^*)$ is a forest with ℓ components, and thus

$$\boldsymbol{m}^* = \boldsymbol{n}^* - \ell. \tag{6.9}$$

Case 2: $\boldsymbol{X} = 1$, $\boldsymbol{X}' = 0$: Obtain $\hat{\mathscr{G}}$ from $\mathscr{G}$ by adding one new vertex r whose neighbours are $x_1, \neg x_1, \ldots, x_\ell, \neg x_\ell$. Then $\hat{\mathscr{G}}$ is unicyclic because $\boldsymbol{X} = 1$. Let $\tilde{\mathscr{G}}$ be the graph obtained from $\hat{\mathscr{G}}$ by deleting the vertex r along with one (arbitrary) clause a from the cycle of $\hat{\mathscr{G}}$. Then $\tilde{\mathscr{G}}$ is a forest with 2ℓ components. Therefore, by the same token as in Case 1, $G(\boldsymbol{\Phi}^* - a)$ is a forest with ℓ components. Hence, $G(\boldsymbol{\Phi}^*)$, obtained by inserting clause a into $G(\boldsymbol{\Phi}^* - a)$, either contains a single cycle or consists of exactly $\ell - 1$ components. Thus, by (6.7)

$$\boldsymbol{m}^* \leq \boldsymbol{n}^* - \ell + 1, \qquad \mathbb{P}\left[\boldsymbol{X} = 1, \boldsymbol{X}' = 0 \,|\, |\mathscr{F}_\infty|\right] = O(|\mathscr{F}_\infty|^2/n). \tag{6.10}$$

Case 3: $\boldsymbol{X} = 0$, $\boldsymbol{X}' = 1$: The graph $\hat{\mathscr{G}}$, defined as in Case 2, is a tree because $\boldsymbol{X} = 0$. Suppose $(\mathscr{F}_\infty \cap \neg\mathscr{F}_\infty) \setminus \{x_1, \neg x_1, \ldots, x_\ell, \neg x_\ell\} = \{y, \neg y\}$. Let a be a clause on the unique path from y to $\neg y$ in $\hat{\mathscr{G}}$. Then the same argument as in Case 1 shows that $G(\boldsymbol{\Phi}^* - a)$ is a forest with ℓ components. Therefore, $G(\boldsymbol{\Phi}^*)$ either contains a unique cycle or has precisely $\ell - 1$ components. Consequently, (6.8) yields

$$\boldsymbol{m}^* \leq \boldsymbol{n}^* - \ell + 1, \qquad \mathbb{P}\left[\boldsymbol{X} = 0, \boldsymbol{X}' = 1 \,|\, |\mathscr{F}_\infty|\right] = O(|\mathscr{F}_\infty|^2/n). \tag{6.11}$$

Case 4: $\boldsymbol{X} + \boldsymbol{X}' \geq 2$: In this case we do not have a bound on $\boldsymbol{m}^* - \boldsymbol{n}^*$, but we claim that

$$\mathbb{P}\left[\boldsymbol{X} + \boldsymbol{X}' \geq 2 \,|\, |\mathscr{F}_\infty|\right] = O(|\mathscr{F}_\infty|^4/n^2). \tag{6.12}$$

Indeed, (6.7) and (6.8) readily imply that $\mathbb{P}\left[\boldsymbol{X} \vee \boldsymbol{X}' \geq 2 \,|\, |\mathscr{F}_\infty|\right] = O(|\mathscr{F}_\infty|^4/n^2)$. Further, since $\boldsymbol{X}$ is independent of $\boldsymbol{X}'$ given $\mathscr{F}_\infty$, (6.7) and (6.8) also yield the bound $\mathbb{P}\left[\boldsymbol{X} = \boldsymbol{X}' = 1 \,|\, |\mathscr{F}_\infty|\right] = O(|\mathscr{F}_\infty|^4/n^2)$.

The assertion follows by combining (6.9)–(6.12) with Claim 6.8. □

Claim 6.10. *For all $\chi \in \{\pm 1\}^{\{x_1,\ldots,x_\ell\}}$ we have $\boldsymbol{A}_\chi^\dagger \leq |\mathscr{F}_\infty| \mathbf{1}\{\boldsymbol{m}^* \leq \boldsymbol{n}^* - \ell + 1\} + n\mathbf{1}\{\boldsymbol{m}^* > \boldsymbol{n}^* - \ell + 1\}$.*

Proof. The graph $G(\boldsymbol{\Phi}^*)$ consists of at most ℓ components (one for each of the initial variables $x_1, \ldots, x_\ell$). Hence, $\boldsymbol{m}^* \geq \boldsymbol{n}^* - \ell$ and $G(\boldsymbol{\Phi}^*)$ is acyclic if $\boldsymbol{m}^* = \boldsymbol{n}^* - \ell$. Moreover, if $G(\boldsymbol{\Phi}^*)$ is acyclic then $\boldsymbol{A}_\chi^\dagger \leq |\mathscr{F}_\infty|$ by construction.

Thus, we are left to consider the case $\boldsymbol{m}^* = \boldsymbol{n}^* - \ell + 1$. Then $\boldsymbol{\Phi}^*$ contains a clause a such that $G(\boldsymbol{\Phi}^* - a)$ is a forest with ℓ components rooted at $x_1, \ldots, x_\ell$. Assume without loss that $a = x_{n-1} \vee x_n$. Then by construction we have $\{x_{n-1}, \neg x_{n-1}\} \cap \mathscr{F}_\infty \neq \emptyset$ and $\{x_n, \neg x_n\} \cap \mathscr{F}_\infty \neq \emptyset$. Further, unless $\neg x_{n-1}, \neg x_n \in \mathscr{F}_\infty$ we have $\boldsymbol{A}_\chi \leq \boldsymbol{I}_\chi \leq |\mathscr{F}_\infty|$ as in the first case. Hence, assume that $\neg x_{n-1}, \neg x_n \in \mathscr{F}_\infty$. Let $i \in [\ell]$ be such that x_n belongs to the connected component of x_i in $G(\boldsymbol{\Phi}^* - a)$ and obtain χ' from χ by flipping the value assigned to x_i. Because $G(\boldsymbol{\Phi}^* - a)$ is a forest, we conclude that $\boldsymbol{A}_\chi^\dagger \leq \boldsymbol{I}_\chi \wedge \boldsymbol{I}_{\chi'} \leq |\mathscr{F}_\infty|$. □

Proof of Lemma 6.6. The choice of the clause probability p ensures that $\boldsymbol{A}_\chi^\dagger$ stochastically dominates $\boldsymbol{A}_\chi$. Therefore, the assertion follows from Claims 6.8–6.10. □

Proof of Lemma 6.5. The choice of the clause probability p and the construction of the set $\mathscr{F}_\infty$ guarantee that $\boldsymbol{I}_\chi$ is stochastically dominated by the random variable $|\mathscr{F}_\infty| \mathbf{1}\{\boldsymbol{m}^* \leq \boldsymbol{n}^* - \ell\} + n\mathbf{1}\{\boldsymbol{m}^* > \boldsymbol{n}^* - \ell\}$. Hence, Claims 6.8–6.10 imply the desired bound. □

Proof of Corollary 6.7. Let $Y = \{x_1\}$ and $\chi_{x_1}^+ = 1$, $\chi_{x_1}^- = -1$. Assume that $\boldsymbol{\Phi}'$ is satisfiable. Then Fact 6.4 implies that

$$n \wedge \left|\log \frac{\mu_{\boldsymbol{\Phi}'}(\boldsymbol{\sigma}_{x_1} = 1)}{\mu_{\boldsymbol{\Phi}'}(\boldsymbol{\sigma}_{x_1} = -1)}\right| \leq \boldsymbol{I}_{\chi^-} + \boldsymbol{I}_{\chi^+}.$$

Therefore, the assertion follows from Lemma 6.5. □

6.3. **Proof of Proposition 6.2.** Let $c_1, \ldots, c_{\boldsymbol{\Delta}''}$ be the new clauses added to $\boldsymbol{\Phi}''$ and let $\boldsymbol{Y} = \{\boldsymbol{y}_1, \boldsymbol{z}_1, \ldots, \boldsymbol{y}_{\boldsymbol{\Delta}''}, \boldsymbol{z}_{\boldsymbol{\Delta}''}\}$ be the set of variables that occur in these clauses. We begin by deriving the following rough bound.

Lemma 6.11. *We have* $\mathbb{E}\left[\log^2 \frac{Z(\boldsymbol{\Phi}'') \vee 1}{Z(\boldsymbol{\Phi}') \vee 1}\right] = O(1)$.

Proof. If Φ' is unsatisfiable then so is Φ'' and thus $(Z(\Phi'')\vee 1)/(Z(\Phi')\vee 1)=1$. Hence, we may assume that $Z(\Phi')\geq 1$. If $|\boldsymbol{Y}|=2\boldsymbol{\Delta}''$, the new clauses attach to disjoint sets of variables. Consider the truth value assignment $\boldsymbol{\chi}\in\{\pm 1\}^{\boldsymbol{Y}}$ that satisfies both literals in each of the clauses $c_1,\ldots,c_{\boldsymbol{\Delta}''}$. Fact 6.4 shows that

$$Z(\Phi'')\vee 1\geq Z(\Phi',\boldsymbol{\chi})\vee 1\geq 2^{-\boldsymbol{A}_{\boldsymbol{\chi}}}Z(\Phi'). \tag{6.13}$$

Combining (6.13) with Lemma 6.6 and recalling that $\boldsymbol{\Delta}''\stackrel{\mathrm{d}}{=}\mathrm{Po}(d/2)$, we obtain

$$\mathbb{E}\left[\mathbf{1}\left\{Z(\Phi')\geq 1,\ |\boldsymbol{Y}|=2\boldsymbol{\Delta}''\right\}\log^2\frac{Z(\Phi'')\vee 1}{Z(\Phi')\vee 1}\right]\leq\mathbb{E}\left[\mathbf{1}\left\{Z(\Phi')\geq 1,\ |\boldsymbol{Y}|=2\boldsymbol{\Delta}''\right\}\boldsymbol{A}_{\boldsymbol{\chi}}^2\right]=O(1). \tag{6.14}$$

Next, consider the event $|\boldsymbol{Y}|=2\boldsymbol{\Delta}''-1$. Because $c_1,\ldots,c_{\boldsymbol{\Delta}''}$ are drawn independently, we have

$$\mathbb{P}\left[|\boldsymbol{Y}|=2\boldsymbol{\Delta}''-1\mid\boldsymbol{\Delta}''\right]\leq O((\boldsymbol{\Delta}'')^2/n). \tag{6.15}$$

Moreover, because the signs of the clauses $c_1,\ldots,c_{\boldsymbol{\Delta}''}$ are independent of Φ', given $|\boldsymbol{Y}|=2\boldsymbol{\Delta}-1$ there exists an assignment $\boldsymbol{\chi}\in\{\pm 1\}^{\boldsymbol{Y}}$, stochastically independent of Φ', that satisfies $c_1,\ldots,c_{\boldsymbol{\Delta}''}$. Fact 6.4 yields $Z(\Phi'')\vee 1\geq Z(\Phi',\boldsymbol{\chi})\geq 2^{-\boldsymbol{I}_{\boldsymbol{\chi}}}Z(\Phi')$. Therefore, since $\log((Z(\Phi'')\vee 1)/(Z(\Phi')\vee 1))\leq n$, Lemma 6.5 and (6.15) imply

$$\mathbb{E}\left[\mathbf{1}\left\{Z(\Phi')\geq 1,\ |\boldsymbol{Y}|=2\boldsymbol{\Delta}''-1\right\}\log^2\frac{Z(\Phi'')\vee 1}{Z(\Phi')\vee 1}\right]\leq n\mathbb{E}\left[\mathbf{1}\left\{|\boldsymbol{Y}|=2\boldsymbol{\Delta}''-1\right\}\boldsymbol{I}_{\boldsymbol{\chi}}\right]=O(1). \tag{6.16}$$

Finally, consider the event $|\boldsymbol{Y}|<2\boldsymbol{\Delta}''-1$. Due to the independence of $c_1,\ldots,c_{\boldsymbol{\Delta}''}$, this event occurs with probability $O(n^{-2})$. Hence, the deterministic bound $(Z(\Phi'')\vee 1)/(Z(\Phi')\vee 1)\geq 2^{-n}$ implies

$$\mathbb{E}\left[\mathbf{1}\left\{Z(\Phi')\geq 1,\ |\boldsymbol{Y}|<2\boldsymbol{\Delta}''-1\right\}\log^2\frac{Z(\Phi'')\vee 1}{Z(\Phi')\vee 1}\right]=O(1). \tag{6.17}$$

The assertion follows from (6.14), (6.16) and (6.17). □

Lemma 6.12. *There exists a number $K>0$ such that for every $\varepsilon>0$ we have*

$$\limsup_{n\to\infty}\mathbb{E}\left[\left(\sum_{i=1}^{\boldsymbol{\Delta}''}\Lambda_\varepsilon(1-\mu_{\Phi'}(\boldsymbol{\sigma}_{\boldsymbol{y}_i}=-\mathrm{sign}(c_i,\boldsymbol{y}_i))\mu_{\Phi'}(\boldsymbol{\sigma}_{\boldsymbol{z}_i}=-\mathrm{sign}(c_i,\boldsymbol{z}_i))\right)^2\mid Z(\Phi')>0\right]\leq K.$$

Proof. Since $\boldsymbol{\Delta}''\stackrel{\mathrm{d}}{=}\mathrm{Po}(d/2)$ and the pair $(\boldsymbol{y}_1,\boldsymbol{z}_1)$ is uniformly random, due to Cauchy-Schwarz it suffices to prove $\limsup_{n\to\infty}\mathbb{E}\left[\Lambda_\varepsilon(1-\mu_{\Phi'}(\boldsymbol{\sigma}_{x_1}=1)\mu_{\Phi'}(\boldsymbol{\sigma}_{x_2}=1))^2\mid Z(\Phi')>0\right]\leq K$ for every $\varepsilon>0$. We observe that

$$\begin{aligned}\limsup_{n\to\infty}\mathbb{E}\left[\Lambda_\varepsilon(1-\mu_{\Phi'}(\boldsymbol{\sigma}_{x_1}=1)\mu_{\Phi'}(\boldsymbol{\sigma}_{x_2}=1))^2\mid Z(\Phi')>0\right]&\leq\limsup_{n\to\infty}\mathbb{E}\left[\Lambda_\varepsilon(1-\mu_{\Phi'}(\boldsymbol{\sigma}_{x_1}=1))^2\mid Z(\Phi')>0\right]\\&=\limsup_{n\to\infty}\mathbb{E}\left[\frac{1}{n}\sum_{i=1}^n\Lambda_\varepsilon(1-\mu_{\Phi'}(\boldsymbol{\sigma}_{x_i}=1))^2\mid Z(\Phi')>0\right].\end{aligned} \tag{6.18}$$

Moreover, Φ' has $\boldsymbol{m}'\stackrel{\mathrm{d}}{=}\mathrm{Po}(dn/2-d/2)$ clauses, while $\Phi=\Phi_n$ has $\boldsymbol{m}\stackrel{\mathrm{d}}{=}\mathrm{Po}(dn/2)$ clauses. Since $d_{\mathrm{TV}}(\boldsymbol{m}',\boldsymbol{m})=o(1)$, the formulas Φ', Φ can be coupled such that both coincide w.h.p. Hence, for any fixed $\varepsilon>0$ we have

$$\mathbb{E}\left[\frac{1}{n}\sum_{i=1}^n\Lambda_\varepsilon(1-\mu_{\Phi'}(\boldsymbol{\sigma}_{x_i}=1))^2\mid Z(\Phi')\right]=\mathbb{E}\left[\frac{1}{n}\sum_{i=1}^n\Lambda_\varepsilon(1-\mu_{\Phi}(\boldsymbol{\sigma}_{x_i}=1))^2\mid Z(\Phi')\right]+o(1). \tag{6.19}$$

Further, since for every $\varepsilon>0$ the function $u\in[0,1]\mapsto\Lambda_\varepsilon(1-u)^2$ is continuous, Corollary 1.3 implies that

$$\frac{1}{n}\sum_{i=1}^n\Lambda_\varepsilon(1-\mu_{\Phi}(\boldsymbol{\sigma}_{x_i}=1))^2\quad\stackrel{n\to\infty}{\longrightarrow}\quad\mathbb{E}\left[\Lambda_\varepsilon(1-\boldsymbol{\mu}_{\pi_d})^2\right]\qquad\text{in probability.} \tag{6.20}$$

Since (2.1) shows that $\mathbb{E}\left[\Lambda_\varepsilon(1-\boldsymbol{\mu}_{\pi_d})^2\right]\leq\mathbb{E}\left[\log^2(1-\boldsymbol{\mu}_{\pi_d})\right]<\infty$, the assertion follows from (6.18)–(6.20). □

Lemma 6.13. *For any $\delta>0$ there exists $\varepsilon>0$ such that*

$$\limsup_{n\to\infty}\left|\mathbb{E}\left[\log\frac{Z(\Phi'')\vee 1}{Z(\Phi')\vee 1}\right]-\frac{d}{2}\mathbb{E}\left[\Lambda_\varepsilon\left(1-\mu_{\Phi',x_1}(\boldsymbol{s}_1)\mu_{\Phi',x_2}(\boldsymbol{s}_2)\right)\mid Z(\Phi')\right]\right|<\delta.$$

Proof. Choose small enough $\xi=\xi(\delta)>\eta=\eta(\xi)>\varepsilon=\varepsilon(\eta)>0$, assume that $n>n_0(\varepsilon)$ is sufficiently large and let $(\gamma_n)_n$ be a sequence of positive reals, depending on ξ and η, that tends to zero sufficiently slowly. Let $\mathscr{E}=\mathscr{E}_n$ be the event that the following five statements hold.

E1: $Z(\Phi')>0$.

E2: $|\boldsymbol{Y}| = 2\boldsymbol{\Delta}''$.
E3: $\boldsymbol{\Delta}'' < \xi^{-1/4}$.
E4: for all $y \in \boldsymbol{Y}$ and all $s \in \{\pm 1\}$ we have $\mu_{\boldsymbol{\Phi}'}(\boldsymbol{\sigma}_y = s) < 1 - 2\eta$.
E5: $\sum_{\sigma \in \{\pm 1\}^{\boldsymbol{Y}}} \left|\mu_{\boldsymbol{\Phi}}(\forall y \in \boldsymbol{Y} : \boldsymbol{\sigma}_y = \sigma_y) - \prod_{y \in \boldsymbol{Y}} \mu_{\boldsymbol{\Phi}}(\boldsymbol{\sigma}_y = \sigma_y)\right| < \gamma_n$.

The first two events **E1**, **E2** occur with probability $1 - o(1)$ as $n \to \infty$. Moreover, $\mathbb{P}[\mathbf{E3}] > 1 - \xi$ if ξ is small enough. Further, since Corollary 1.3 shows that $\pi_{\boldsymbol{\Phi}}$ converges to π_d weakly in probability, the tail bound (2.1) implies that $\mathbb{P}\left[\mathbf{E4} \mid \boldsymbol{\Delta}'' < \xi^{-1/4}\right] > 1 - \xi$, provided that η is small enough. Additionally, Corollary 2.3 implies $\mathbb{P}\left[\mathbf{E5} \mid \mathbf{E1}\text{–}\mathbf{E4}\right] = 1 - o(1)$ if $\gamma_n \to 0$ slowly enough. Consequently,

$$\mathbb{P}[\mathscr{E}] > 1 - 4\xi. \tag{6.21}$$

Combining Lemma 6.11, (6.21) and the Cauchy-Schwarz inequality, we obtain

$$\left|\mathbb{E}\left[(1 - \mathbf{1}\mathscr{E}) \log \frac{Z(\boldsymbol{\Phi}'')}{Z(\boldsymbol{\Phi}')}\right]\right| \leq \delta/3 + o(1). \tag{6.22}$$

Similarly, by Lemma 6.12, (6.21) and Cauchy-Schwarz,

$$\left|\mathbb{E}\left[(1 - \mathbf{1}\mathscr{E}) \sum_{i=1}^{\boldsymbol{\Delta}''} \Lambda_\varepsilon\left(1 - \mu_{\boldsymbol{\Phi}'}(\boldsymbol{\sigma}_{\boldsymbol{y}_i} = -\operatorname{sign}(\boldsymbol{y}_i, c_i))\mu_{\boldsymbol{\Phi}'}(\boldsymbol{\sigma}_{\boldsymbol{z}_i} = -\operatorname{sign}(\boldsymbol{z}_i, c_i))\right)\right]\right| \leq \delta/3 + o(1). \tag{6.23}$$

Further, because the distribution of $\boldsymbol{\Phi}'$ is invariant under permutations of the variables $x_1, \ldots, x_n$ and $\mathbb{E}[\boldsymbol{\Delta}''] = d/2$,

$$\begin{aligned}
&\mathbb{E}\left[\sum_{i=1}^{\boldsymbol{\Delta}''} \Lambda_\varepsilon\left(1 - \mu_{\boldsymbol{\Phi}'}(\boldsymbol{\sigma}_{\boldsymbol{y}_i} = -\operatorname{sign}(\boldsymbol{y}_i, c_i))\mu_{\boldsymbol{\Phi}'}(\boldsymbol{\sigma}_{\boldsymbol{z}_i} = -\operatorname{sign}(\boldsymbol{z}_i, c_i))\right) \mid Z(\boldsymbol{\Phi}') > 0\right] \\
&\quad = \frac{d}{2}\mathbb{E}\left[\Lambda_\varepsilon\left(1 - \mu_{\boldsymbol{\Phi}'}(\boldsymbol{\sigma}_{x_1} = \boldsymbol{s}_1)\mu_{\boldsymbol{\Phi}'}(\boldsymbol{\sigma}_{x_2} = \boldsymbol{s}_2)\right) \mid Z(\boldsymbol{\Phi}') > 0\right].
\end{aligned} \tag{6.24}$$

Moreover, on the event $\mathscr{E}$ we have

$$\begin{aligned}
\frac{Z(\boldsymbol{\Phi}'')}{Z(\boldsymbol{\Phi}')} &= \sum_{\sigma \in \{\pm 1\}^{\boldsymbol{Y}}} \mathbf{1}\left\{\sigma \text{ satisfies } c_1, \ldots, c_{\boldsymbol{\Delta}''}\right\} \mu_{\boldsymbol{\Phi}'}\left(\forall y \in \boldsymbol{Y} : \boldsymbol{\sigma}_y = \sigma_y\right) \\
&= \sum_{\sigma \in \{\pm 1\}^{\boldsymbol{Y}}} \mathbf{1}\left\{\sigma \text{ satisfies } c_1, \ldots, c_{\boldsymbol{\Delta}''}\right\} \prod_{y \in \boldsymbol{Y}} \mu_{\boldsymbol{\Phi}'}\left(\boldsymbol{\sigma}_y = \sigma_y\right) + o(1) \qquad \text{[due to } \mathbf{E3}\text{,}\mathbf{E5}\text{]} \\
&= \prod_{i=1}^{\boldsymbol{\Delta}''} \left(1 - \mu_{\boldsymbol{\Phi}'}\left(\boldsymbol{\sigma}_{\boldsymbol{y}_i} = -\operatorname{sign}(\boldsymbol{y}_i, c_i)\right)\mu_{\boldsymbol{\Phi}'}\left(\boldsymbol{\sigma}_{\boldsymbol{z}_i} = -\operatorname{sign}(\boldsymbol{z}_i, c_i)\right)\right) + o(1).
\end{aligned}$$

Therefore, by **E4**

$$\begin{aligned}
\mathbb{E}\left[\mathbf{1}\mathscr{E} \log \frac{Z(\boldsymbol{\Phi}'')}{Z(\boldsymbol{\Phi}')}\right] &= \mathbb{E}\left[\mathbf{1}\mathscr{E} \sum_{i=1}^{\boldsymbol{\Delta}''} \log\left(1 - \mu_{\boldsymbol{\Phi}'}\left(\boldsymbol{\sigma}_{\boldsymbol{y}_i} = -\operatorname{sign}(\boldsymbol{y}_i, c_i)\right)\mu_{\boldsymbol{\Phi}'}\left(\boldsymbol{\sigma}_{\boldsymbol{z}_i} = -\operatorname{sign}(\boldsymbol{z}_i, c_i)\right)\right)\right] + o(1) \\
&= \mathbb{E}\left[\mathbf{1}\mathscr{E} \sum_{i=1}^{\boldsymbol{\Delta}''} \Lambda_\varepsilon\left(1 - \mu_{\boldsymbol{\Phi}'}\left(\boldsymbol{\sigma}_{\boldsymbol{y}_i} = -\operatorname{sign}(\boldsymbol{y}_i, c_i)\right)\mu_{\boldsymbol{\Phi}'}\left(\boldsymbol{\sigma}_{\boldsymbol{z}_i} = -\operatorname{sign}(\boldsymbol{z}_i, c_i)\right)\right)\right] + o(1).
\end{aligned} \tag{6.25}$$

Finally, the assertion follows from (6.22)–(6.25). □

Proof of Proposition 6.2. Proposition 2.1 shows that $\boldsymbol{\mu}_{\pi_d,1}$ and $1 - \boldsymbol{\mu}_{\pi_d,1}$ are identically distributed. Since Λ_ε is continuous and bounded, Corollary 1.3 therefore implies that

$$\begin{aligned}
\lim_{n\to\infty} \mathbb{E}\left[\Lambda_\varepsilon\left(1 - \mu_{\boldsymbol{\Phi}',x_1}(\boldsymbol{s}_1)\mu_{\boldsymbol{\Phi}',x_2}(\boldsymbol{s}_2)\right)\right] &= \mathbb{E}\left[\Lambda_\varepsilon\left(1 - \left(\frac{1 - \boldsymbol{s}_1}{2} + \boldsymbol{s}_1\boldsymbol{\mu}_{\pi_d,1}\right)\left(\frac{1 - \boldsymbol{s}_2}{2} + \boldsymbol{s}_2\boldsymbol{\mu}_{\pi_d,2}\right)\right)\right] \\
&= \mathbb{E}\left[\Lambda_\varepsilon\left(1 - \boldsymbol{\mu}_{\pi_d,1}\boldsymbol{\mu}_{\pi_d,2}\right)\right].
\end{aligned} \tag{6.26}$$

for every $\varepsilon > 0$. Further, since $\Lambda_\varepsilon(1 - \boldsymbol{\mu}_{\pi_d,1}\boldsymbol{\mu}_{\pi_d,2})$ decreases monotonically to $\log(1 - \boldsymbol{\mu}_{\pi_d,1}\boldsymbol{\mu}_{\pi_d,2})$ as $\varepsilon \to 0$, the monotone convergence theorem and (2.2) yield

$$\lim_{\varepsilon\to 0} \mathbb{E}\left[\Lambda_\varepsilon\left(1 - \boldsymbol{\mu}_{\pi_d,1}\boldsymbol{\mu}_{\pi_d,2}\right)\right] = \mathbb{E}\log\left(1 - \boldsymbol{\mu}_{\pi_d,1}\boldsymbol{\mu}_{\pi_d,2}\right). \tag{6.27}$$

Combining (6.26) and (6.27) and Lemma 6.13 completes the proof. □

6.4. **Proof of Proposition 6.3.** The steps that we follow are analogous to the ones from the proof of Proposition 6.2. Recall that $\mathbf{\Phi}'''$ is obtained from $\mathbf{\Phi}'$ by adding one variable x_{n+1} along with random adjacent clauses $b_1,\ldots,b_{\mathbf{\Delta}'''}$, where $\mathbf{\Delta}'''$ is a Poisson variable with mean d. Let $\boldsymbol{y}_1,\ldots,\boldsymbol{y}_{\mathbf{\Delta}'''} \in \{x_1,\ldots,x_n\}$ be the variables of $\mathbf{\Phi}'$ where the new clauses attach and let $\boldsymbol{Y} = \{\boldsymbol{y}_1,\ldots,\boldsymbol{y}_{\mathbf{\Delta}'''}\}$. We begin with the following L_2-bound.

Lemma 6.14. *We have* $\limsup_{n\to\infty} \mathbb{E}\left[\log^2 \frac{Z(\mathbf{\Phi}''')\vee 1}{Z(\mathbf{\Phi}')\vee 1}\right] < \infty$.

Proof. If $\mathbf{\Phi}'$ is unsatisfiable, then so is $\mathbf{\Phi}'''$ and thus $(Z(\mathbf{\Phi}''')\vee 1)/(Z(\mathbf{\Phi}')\vee 1) = 1$. Hence, we may assume that $Z(\mathbf{\Phi}') \geq 1$. We now consider three scenarios. First, suppose that $|\boldsymbol{Y}| = \mathbf{\Delta}'''$, i.e., the new clauses attach to distinct variables of $\mathbf{\Phi}'$. Then define an assignment $\boldsymbol{\chi} \in \{\pm 1\}^{\boldsymbol{Y}}$ by setting each $y \in \boldsymbol{Y}$ to the value that satisfies the unique clause among $b_1,\ldots,b_{\mathbf{\Delta}'''}$ in which y occurs. We claim that

$$Z(\mathbf{\Phi}''')\vee 1 \geq 2^{-\boldsymbol{A}_{\boldsymbol{\chi}}} Z(\mathbf{\Phi}'). \tag{6.28}$$

Indeed, if $\boldsymbol{\chi}' \in \{\pm 1\}^{\boldsymbol{Y}}$ differs from $\boldsymbol{\chi}$ on only one variable, then we can always satisfy all clauses $b_1,\ldots,b_{\mathbf{\Delta}'''}$ by setting x_{n+1} appropriately. Therefore, (6.28) follows from Fact 6.4 and the definition (6.3) of $\boldsymbol{A}_{\boldsymbol{\chi}}$. Combining (6.28) with Lemma 6.6, we obtain

$$\mathbb{E}\left[\mathbf{1}\left\{Z(\mathbf{\Phi}')\geq 1,\ |\boldsymbol{Y}| = \mathbf{\Delta}'''\right\}\log^2\frac{Z(\mathbf{\Phi}''')\vee 1}{Z(\mathbf{\Phi}')\vee 1}\right] \leq \mathbb{E}\left[\mathbf{1}\left\{|\boldsymbol{Y}| = \mathbf{\Delta}'''\right\}\boldsymbol{A}_{\boldsymbol{\chi}}^2\right] = O(1). \tag{6.29}$$

Second, consider the case $|\boldsymbol{Y}| = \mathbf{\Delta}''' - 1$. Because $b_1,\ldots,b_{\mathbf{\Delta}'''}$ are drawn independently, we have

$$\mathbb{P}\left[|\boldsymbol{Y}| = \mathbf{\Delta}''' - 1 \mid \mathbf{\Delta}'''\right] = O((\mathbf{\Delta}''')^2/n). \tag{6.30}$$

Further, there exists an assignment $\boldsymbol{\chi} \in \{\pm 1\}^{\boldsymbol{Y}}$ under which all but one of the clauses $b_1,\ldots,b_{\mathbf{\Delta}'''}$ are satisfied. This assignment is independent of $\mathbf{\Phi}'$ because the signs of $b_1,\ldots,b_{\mathbf{\Delta}'''}$ are. Since we can use the new variable x_{n+1} to satisfy the last clause as well, Fact 6.4 implies the bound $(Z(\mathbf{\Phi}''')\vee 1)/Z(\mathbf{\Phi}') \geq 2^{-\boldsymbol{I}_{\boldsymbol{\chi}}}$. Therefore, Lemma 6.5 and (6.30) yield

$$\begin{aligned}\mathbb{E}\left[\mathbf{1}\left\{Z(\mathbf{\Phi}')\geq 1,\ |\boldsymbol{Y}| = \mathbf{\Delta}'''-1\right\}\log^2\frac{Z(\mathbf{\Phi}'')\vee 1}{Z(\mathbf{\Phi}')\vee 1}\right] &\leq \mathbb{E}\left[\mathbf{1}\left\{Z(\mathbf{\Phi}')\geq 1,\ |\boldsymbol{Y}| = \mathbf{\Delta}'''-1\right\}\boldsymbol{I}_{\boldsymbol{\chi}}^2\right]\\ &\leq n\mathbb{E}\left[\mathbf{1}\left\{|\boldsymbol{Y}| = \mathbf{\Delta}'''-1\right\}\boldsymbol{I}_{\boldsymbol{\chi}}\right] = O(1).\end{aligned} \tag{6.31}$$

Finally, because $b_1,\ldots,b_{\mathbf{\Delta}'''}$ are drawn independently, the event $\{|\boldsymbol{Y}| < \mathbf{\Delta}''' - 1\}$ has probability $O(n^{-2})$. Therefore, the deterministic bound $(Z(\mathbf{\Phi}''')\vee 1)/(Z(\mathbf{\Phi}')\vee 1) \geq 2^{-n}$ ensures that

$$\mathbb{E}\left[\mathbf{1}\left\{Z(\mathbf{\Phi}')\geq 1,\ |\boldsymbol{Y}| < \mathbf{\Delta}'''-1\right\}\log^2\frac{Z(\mathbf{\Phi}''')\vee 1}{Z(\mathbf{\Phi}')\vee 1}\right] = O(1). \tag{6.32}$$

The assertion follows from (6.29), (6.31) and (6.32). □

Lemma 6.15. *There exists* $K > 0$ *such that for every* $\varepsilon > 0$ *we have*

$$\limsup_{n\to\infty}\mathbb{E}\left[\Lambda_\varepsilon\left(\sum_{s\in\{\pm 1\}}\prod_{i=1}^{\mathbf{\Delta}'''}\left(1-\mathbf{1}\left\{s\neq\operatorname{sign}(x_{n+1},b_i)\right\}\mu_{\mathbf{\Phi}'}(\boldsymbol{\sigma}_{\boldsymbol{y}_i} = -\operatorname{sign}(\boldsymbol{y}_i,b_i))\right)\right)^2 \mid Z(\mathbf{\Phi}')>0\right] \leq K.$$

Proof. Since $\mathbf{\Delta}''' \stackrel{\mathrm{d}}{=} \mathrm{Po}(d/2)$, $\boldsymbol{y}_1,\ldots,\boldsymbol{y}_{\mathbf{\Delta}'''}$ and the signs $\operatorname{sign}(b_i,\boldsymbol{y}_i)$ are uniformly random, we obtain

$$\begin{aligned}&\mathbb{E}\left[\Lambda_\varepsilon\left(\sum_{s\in\{\pm 1\}}\prod_{i=1}^{\mathbf{\Delta}'''}\left(1-\mathbf{1}\left\{s\neq\operatorname{sign}(x_{n+1},b_i)\right\}\mu_{\mathbf{\Phi}'}(\boldsymbol{\sigma}_{\boldsymbol{y}_i} = -\operatorname{sign}(\boldsymbol{y}_i,b_i))\right)\right)^2 \mid Z(\mathbf{\Phi}')>0\right]\\ &\leq 1+\mathbb{E}\left[\Lambda_\varepsilon\left(\prod_{i=1}^{\mathbf{\Delta}'''}\mu_{\mathbf{\Phi}'}(\boldsymbol{\sigma}_{\boldsymbol{y}_i}=1)\right)^2 \mid Z(\mathbf{\Phi}')>0\right] \leq 1+d\mathbb{E}\left[\Lambda_\varepsilon\left(\mu_{\mathbf{\Phi}'}(\boldsymbol{\sigma}_{\boldsymbol{y}_1}=1)\right)^2 \mid Z(\mathbf{\Phi}')>0\right].\end{aligned} \tag{6.33}$$

Further, the formulas $\mathbf{\Phi}'$, $\mathbf{\Phi}$ can be coupled such that both coincide w.h.p. (cf. the proof of Lemma 6.12). Therefore, Corollary 1.3 implies that for every $\varepsilon > 0$,

$$\mathbb{E}\left[\Lambda_\varepsilon\left(\mu_{\mathbf{\Phi}'}(\boldsymbol{\sigma}_{\boldsymbol{y}_1}=1)\right)^2 \mid Z(\mathbf{\Phi}')>0\right] = \mathbb{E}\left[\Lambda_\varepsilon\left(\boldsymbol{\mu}_{\pi_{\mathbf{\Phi}}}\right)^2 \mid Z(\mathbf{\Phi})>0\right] + o(1) = \mathbb{E}\left[\Lambda_\varepsilon\left(\boldsymbol{\mu}_{\pi_d}^2\right)\right] + o(1) \leq \mathbb{E}\left[\log^2\boldsymbol{\mu}_{\pi_d}\right] + o(1). \tag{6.34}$$

Since (2.1) implies that $\mathbb{E}\left[\log^2\boldsymbol{\mu}_{\pi_d}\right] < \infty$, the assertion follows from (6.33)–(6.34). □

Lemma 6.16. *For any $\delta > 0$ there exists $\varepsilon_0 > 0$ such that for every $0 < \varepsilon < \varepsilon_0$,*

$$\left|\mathbb{E}\left[\log\frac{Z(\boldsymbol{\Phi}''')\vee 1}{Z(\boldsymbol{\Phi}')\vee 1}\right] - \mathbb{E}\left[\Lambda_\varepsilon\left(\sum_{s\in\{\pm1\}}\prod_{i=1}^{\boldsymbol{d}}\left(1-\mathbf{1}\{s\neq \boldsymbol{s}_i\}\,\mu_{\boldsymbol{\Phi}'}(\boldsymbol{\sigma}_{x_i}=\boldsymbol{s}_i')\right)\right)\mid Z(\boldsymbol{\Phi}')>0\right]\right| < \delta + o(1).$$

Proof. Choose small enough $\xi = \xi(\delta) > \eta = \eta(\xi) > \varepsilon = \varepsilon(\eta) > 0$, assume that $n > n_0(\varepsilon)$ is sufficiently large and let $(\gamma_n)_n$ be a sequence of numbers $\gamma_n > 0$ that tends to zero slowly. Let $\mathscr{E} = \mathscr{E}_n$ be the event that the following five statements are satisfied.

E1: $Z(\boldsymbol{\Phi}') > 0$.
E2: $|\boldsymbol{Y}| = \boldsymbol{\Delta}'''$.
E3: $\boldsymbol{\Delta}''' < \xi^{-1/4}$.
E4: for all $y \in \boldsymbol{Y}$ we have $\mu_{\boldsymbol{\Phi}'}(\boldsymbol{\sigma}_y = 1) \vee \mu_{\boldsymbol{\Phi}'}(\boldsymbol{\sigma}_y = -1) < 1 - 2\eta$.
E5: $\sum_{\sigma\in\{\pm1\}^{\boldsymbol{Y}}}\left|\mu_{\boldsymbol{\Phi}}(\forall y\in\boldsymbol{Y}:\boldsymbol{\sigma}_y=\sigma_y) - \prod_{y\in\boldsymbol{Y}}\mu_{\boldsymbol{\Phi}}(\boldsymbol{\sigma}_y=\sigma_y)\right| < \gamma_n$.

As in the proof of Lemma 6.13 we obtain $\mathbb{P}[\mathscr{E}] > 1 - 4\xi$. Hence, Lemmas 6.14 and 6.15 and the Cauchy-Schwarz inequality yield

$$\left|\mathbb{E}\left[(1-\mathbf{1}\mathscr{E})\log\frac{Z(\boldsymbol{\Phi}''')}{Z(\boldsymbol{\Phi}')}\right]\right| \le \delta/3 + o(1), \tag{6.35}$$

$$\left|\mathbb{E}\left[(1-\mathbf{1}\mathscr{E})\Lambda_\varepsilon\left(\sum_{s\in\{\pm1\}}\prod_{i=1}^{\boldsymbol{\Delta}'''}\left(1-\mathbf{1}\left\{s\neq\operatorname{sign}(x_{n+1},b_i)\right\}\mu_{\boldsymbol{\Phi}'}(\boldsymbol{\sigma}_{\boldsymbol{y}_i}=-\operatorname{sign}(\boldsymbol{y}_i,b_i))\right)\right)\mid Z(\boldsymbol{\Phi}')>0\right]\right| \le \delta/3 + o(1). \tag{6.36}$$

Moreover, because the distribution of $\boldsymbol{\Phi}'$ is invariant under variable permutations,

$$\begin{aligned}&\mathbb{E}\left[\Lambda_\varepsilon\left(\sum_{s\in\{\pm1\}}\prod_{i=1}^{\boldsymbol{\Delta}'''}\left(1-\mathbf{1}\left\{s\neq\operatorname{sign}(x_{n+1},b_i)\right\}\mu_{\boldsymbol{\Phi}'}(\boldsymbol{\sigma}_{\boldsymbol{y}_i}=-\operatorname{sign}(\boldsymbol{y}_i,b_i))\right)\right)\mid Z(\boldsymbol{\Phi}')>0\right]\\ &\quad=\mathbb{E}\left[\Lambda_\varepsilon\left(\sum_{s\in\{\pm1\}}\prod_{i=1}^{\boldsymbol{d}}\left(1-\mathbf{1}\{s\neq\boldsymbol{s}_i\}\,\mu_{\boldsymbol{\Phi}'}(\boldsymbol{\sigma}_{x_i}=\boldsymbol{s}_i')\right)\right)\mid Z(\boldsymbol{\Phi}')>0\right]+o(1).\end{aligned} \tag{6.37}$$

Further, on $\mathscr{E}$ we obtain

$$\begin{aligned}\frac{Z(\boldsymbol{\Phi}''')}{Z(\boldsymbol{\Phi}')} &= \sum_{\sigma\in\{\pm1\}^{\boldsymbol{Y}\cup\{x_{n+1}\}}}\mathbf{1}\left\{\sigma\text{ satisfies }b_1,\ldots,b_{\boldsymbol{\Delta}'''}\right\}\mu_{\boldsymbol{\Phi}'}\left(\forall y\in\boldsymbol{Y}:\boldsymbol{\sigma}_y=\sigma_y\right)\\ &= \sum_{\sigma\in\{\pm1\}^{\boldsymbol{Y}\cup\{x_{n+1}\}}}\mathbf{1}\left\{\sigma\text{ satisfies }b_1,\ldots,b_{\boldsymbol{\Delta}'''}\right\}\prod_{y\in\boldsymbol{Y}}\mu_{\boldsymbol{\Phi}'}\left(\boldsymbol{\sigma}_y=\sigma_y\right)+o(1) \qquad \text{[due to \textbf{E3},\textbf{E5}]}\\ &= \sum_{s\in\{\pm1\}}\prod_{\substack{i\in[\boldsymbol{\Delta}'''],\\ \operatorname{sign}(x_{n+1},b_i)=-s}}\mu_{\boldsymbol{\Phi}'}(\boldsymbol{\sigma}_{\boldsymbol{y}_i}=\operatorname{sign}(\boldsymbol{y}_i,b_i))\ ;\end{aligned} \tag{6.38}$$

to elaborate, in the last step s represents the value assigned to x_{n+1} and the product ensures that the clauses b_i in which x_{n+1} occurs with sign $-s$ are satisfied by assigning their second variable $\boldsymbol{y}_i$ the value $\operatorname{sign}(\boldsymbol{y}_i, b_i)$. Further, (6.38), **E3** and **E4** yield

$$\begin{aligned}\mathbb{E}\left[\mathbf{1}\mathscr{E}\log\frac{Z(\boldsymbol{\Phi}''')}{Z(\boldsymbol{\Phi}')}\right] &= \mathbb{E}\left[\mathbf{1}\mathscr{E}\log\left(\sum_{s\in\{\pm1\}}\prod_{i=1}^{\boldsymbol{\Delta}'''}\left(1-\mathbf{1}\left\{\operatorname{sign}(x_{n+1},b_i)=-s\right\}\mu_{\boldsymbol{\Phi}'}(\boldsymbol{\sigma}_{\boldsymbol{y}_i}=-\operatorname{sign}(\boldsymbol{y}_i,b_i))\right)\right)\right]+o(1)\\ &= \mathbb{E}\left[\mathbf{1}\mathscr{E}\Lambda_\varepsilon\left(\sum_{s\in\{\pm1\}}\prod_{i=1}^{\boldsymbol{\Delta}'''}\left(1-\mathbf{1}\left\{\operatorname{sign}(x_{n+1},b_i)=-s\right\}\mu_{\boldsymbol{\Phi}'}(\boldsymbol{\sigma}_{\boldsymbol{y}_i}=-\operatorname{sign}(\boldsymbol{y}_i,b_i))\right)\right)\right]+o(1)\end{aligned} \tag{6.39}$$

Finally, the assertion follows from (6.35), (6.36), (6.37) and (6.39). □

Proof of Proposition 6.2. Because $\boldsymbol{\mu}_{\pi_d,1} \overset{\mathrm{d}}{=} 1 - \boldsymbol{\mu}_{\pi_d,1}$ by Proposition 2.1, Corollary 1.3 shows that for every $\varepsilon > 0$,

$$\lim_{n\to\infty}\mathbb{E}\left[\Lambda_\varepsilon\left(\sum_{s\in\{\pm1\}}\prod_{i=1}^{\boldsymbol{d}}\left(1-\mathbf{1}\{s\neq\boldsymbol{s}_i\}\,\mu_{\boldsymbol{\Phi}'}(\boldsymbol{\sigma}_{x_i}=\boldsymbol{s}_i')\right)\mid Z(\boldsymbol{\Phi}')>0\right)\right] = \mathbb{E}\left[\Lambda_\varepsilon\left(\sum_{s\in\{\pm1\}}\prod_{i=1}^{\boldsymbol{d}}\left(1-\mathbf{1}\{s\neq\boldsymbol{s}_i\}\,\boldsymbol{\mu}_{\pi_d,i}\right)\right)\right]. \tag{6.40}$$

Further, the dominated convergence theorem and (2.2) yield

$$\lim_{\varepsilon\to0}\mathbb{E}\left[\Lambda_\varepsilon\left(\sum_{s\in\{\pm1\}}\prod_{i=1}^{\boldsymbol{d}}\left(1-\mathbf{1}\{s\neq\boldsymbol{s}_i\}\,\boldsymbol{\mu}_{\pi_d,i}\right)\right)\right] = \mathbb{E}\log\left(\sum_{s\in\{\pm1\}}\prod_{i=1}^{\boldsymbol{d}}\left(1-\mathbf{1}\{s\neq\boldsymbol{s}_i\}\,\boldsymbol{\mu}_{\pi_d,i}\right)\right). \tag{6.41}$$

To complete the proof we combine (6.40), (6.41) and Lemma 6.13. □

7. Proof of Proposition 2.6

Tools such as Azuma's inequality do not apply to the number $Z(\mathbf{\Phi})$ of satisfying assignments because adding or removing even a single clause could change $Z(\mathbf{\Phi})$ by an exponential factor. Therefore, we prove Proposition 2.6 by way of a 'soft' version of the random 2-SAT problem. Specifically, for a real $\beta > 0$ we define $Z_\beta(\mathbf{\Phi})$ via (3.1). Thus, instead of dismissing assignments $\sigma \notin S(\mathbf{\Phi})$ outright, we charge an $\exp(-\beta)$ penalty factor for each violated clause. Because the constraints are soft, showing that $\log Z_\beta(\mathbf{\Phi})$ concentrates is a cinch.

Lemma 7.1. *For all $t, \beta > 0$ we have* $\mathbb{P}\left[\left|\log Z_\beta(\mathbf{\Phi}) - \mathbb{E}[\log Z_\beta(\mathbf{\Phi})]\right| > t \mid \boldsymbol{m}\right] \le 2\exp\left(-\frac{t^2}{2\boldsymbol{m}\beta^2}\right)$.

Proof. Since adding or removing a single clause can alter $Z_\beta(\mathbf{\Phi})$ by at most a factor $\exp(\pm\beta)$, the assertion follows from Azuma's inequality. □

The following statement, whose proof relies on the interpolation method from mathematical physics, will enable us to link the random variables $\log Z_\beta(\mathbf{\Phi})$ and $\log Z(\mathbf{\Phi})$. For a probability measure $p \in \mathscr{P}(0,1)$ and $\beta > 0$ let

$$\begin{aligned}\mathfrak{B}_\beta(p) = \mathbb{E}\left[\log \sum_{s=\pm1}\prod_{i=1}^{\boldsymbol{d}}\left(1 - \mathbf{1}\{\boldsymbol{s}_i \neq s\}\frac{1-\exp(-\beta)}{2}\left(1 - \boldsymbol{s}_i' + 2\boldsymbol{s}_i'\boldsymbol{\mu}_{p,i}\right)\right)\right] \\ - \frac{d}{2}\mathbb{E}\left[\log\left(1 - \frac{1-\exp(-\beta)}{4}\left(1-\boldsymbol{s}_1+2\boldsymbol{s}_1\boldsymbol{\mu}_{p,1}\right)\left(1-\boldsymbol{s}_2+2\boldsymbol{s}_2\boldsymbol{\mu}_{p,2}\right)\right)\right].\end{aligned} \tag{7.1}$$

These two expectations exist and are finite because $0 \le \beta < \infty$. (More precisely, their absolute values are bounded by $\log 2 + \beta d$ and β, respectively.)

Lemma 7.2 ([42, Theorem 1])**.** *For any $p \in \mathscr{P}(0,1)$ and any $0 \le \beta < \infty$ we have* $\lim_{n\to\infty}\frac{1}{n}\mathbb{E}\log Z_\beta(\mathbf{\Phi}) \le \mathfrak{B}_\beta(p)$.

Combining Lemmas 7.1 and 7.2, we obtain the following bound for 'hard' 2-SAT.

Corollary 7.3. *For any $\beta > 0$ we have* $\lim_{n\to\infty}\mathbb{P}\left[\log Z(\mathbf{\Phi}) > n\mathfrak{B}_\beta(\pi_d) + n^{2/3}\right] = 0$.

Proof. We have $Z_\beta(\mathbf{\Phi}) \ge Z(\mathbf{\Phi})$ and Lemmas 7.1 and 7.2 imply $\lim_{n\to\infty}\mathbb{P}\left[\log Z_\beta(\mathbf{\Phi}) > n\mathfrak{B}_\beta(\pi_d) + n^{2/3}\right] = 0$. □

Proof of Proposition 2.6. We begin by observing that the limit $\lim_{\beta\to\infty}\mathfrak{B}_\beta(\pi_d)$ exists and is finite. First, there is the pointwise and monotone convergence of the integrands:

$$\log\sum_{s=\pm1}\prod_{i=1}^{\boldsymbol{d}}\left(1 - \mathbf{1}\{\boldsymbol{s}_i \neq s\}\frac{1-\exp(-\beta)}{2}\left(1-\boldsymbol{s}_i'+2\boldsymbol{s}_i'\boldsymbol{\mu}_{\pi_d,i}\right)\right) \overset{\beta\to\infty}{\longrightarrow} \log\sum_{s=\pm1}\prod_{i=1}^{\boldsymbol{d}}\left(1 - \frac{\mathbf{1}\{\boldsymbol{s}_i \neq s\}}{2}\left(1-\boldsymbol{s}_i'+2\boldsymbol{s}_i'\boldsymbol{\mu}_{\pi_d,i}\right)\right), \tag{7.2}$$

$$\log\left(1 - \frac{1-\exp(-\beta)}{4}\left(1-\boldsymbol{s}_1+2\boldsymbol{s}_1\boldsymbol{\mu}_{\pi_d,1}\right)\left(1-\boldsymbol{s}_2+2\boldsymbol{s}_2\boldsymbol{\mu}_{\pi_d,2}\right)\right) \overset{\beta\to\infty}{\longrightarrow} \log\left(1 - \frac{1}{4}\left(1-\boldsymbol{s}_1+2\boldsymbol{s}_1\boldsymbol{\mu}_{\pi_d,1}\right)\left(1-\boldsymbol{s}_2+2\boldsymbol{s}_2\boldsymbol{\mu}_{\pi_d,2}\right)\right). \tag{7.3}$$

Further, since $\boldsymbol{\mu}_{\pi_d} \overset{\mathrm{d}}{=} 1-\boldsymbol{\mu}_{\pi_d}$ by Proposition 2.1 and because $1-\boldsymbol{s}+2\boldsymbol{s}\boldsymbol{\mu}_{\pi_d}$ equals either $2\boldsymbol{\mu}_{\pi_d}$ or $2(1-\boldsymbol{\mu}_{\pi_d})$, we obtain

$$\log\sum_{s=\pm1}\prod_{i=1}^{\boldsymbol{d}}\left(1 - \frac{\mathbf{1}\{\boldsymbol{s}_i \neq s\}}{2}\left(1-\boldsymbol{s}_i'+2\boldsymbol{s}_i'\boldsymbol{\mu}_{\pi_d,i}\right)\right) \overset{d}{=} \log\left(\prod_{i=1}^{\boldsymbol{d}^-}\boldsymbol{\mu}_{\pi_d,i} + \prod_{i=1}^{\boldsymbol{d}^+}\boldsymbol{\mu}_{\pi_d,i+\boldsymbol{d}^-}\right), \tag{7.4}$$

$$\frac{d}{2}\log\left(1 - \frac{1}{4}\left(1-\boldsymbol{s}_1+2\boldsymbol{s}_1\boldsymbol{\mu}_{\pi_d,1}\right)\left(1-\boldsymbol{s}_2+2\boldsymbol{s}_2\boldsymbol{\mu}_{\pi_d,2}\right)\right) \overset{d}{=} \frac{d}{2}\log\left(1-\boldsymbol{\mu}_{\pi_d,1}\boldsymbol{\mu}_{\pi_d,2}\right). \tag{7.5}$$

Moreover, Proposition 2.1 shows that the monotone limits are integrable and therefore an application of the monotone convergence theorem to (7.2) and (7.3), followed by the simplifications (7.4), (7.4), yields the identity

$$\lim_{\beta\to\infty}\mathfrak{B}_\beta(\pi_d) = \mathbb{E}\left[\log\left(\prod_{i=1}^{\boldsymbol{d}^-}\boldsymbol{\mu}_{\pi_d,i} + \prod_{i=1}^{\boldsymbol{d}^+}\boldsymbol{\mu}_{\pi_d,i+\boldsymbol{d}^-}\right) - \frac{d}{2}\log\left(1-\boldsymbol{\mu}_{\pi_d,1}\boldsymbol{\mu}_{\pi_d,2}\right)\right] = \mathfrak{B}_\infty(\pi_d) < \infty.$$

Further, Corollary 2.5 shows that $\mathfrak{B}_\infty(\pi_d) = \lim_{n\to\infty} n^{-1}\mathbb{E}[\log(Z(\mathbf{\Phi}) \vee 1)]$. Therefore, Corollary 7.3 implies that

$$\mathbb{P}\left[n^{-1}\log(Z(\mathbf{\Phi}) \vee 1) > \mathfrak{B}_\infty(\pi_d) + \varepsilon\right] = o(1) \qquad \text{for any } \varepsilon > 0. \tag{7.6}$$

To complete the proof, we upper bound

$$n^{-1}\mathbb{E}\left|\log(Z(\mathbf{\Phi})\vee 1)-\mathbb{E}[\log(Z(\mathbf{\Phi})\vee 1)]\right|\leq \mathbb{E}\left|n^{-1}\log(Z(\mathbf{\Phi})\vee 1)-\mathfrak{B}_\infty(\pi_d)\right|+\left|\mathfrak{B}_\infty(\pi_d)-\mathbb{E}[\log(Z(\mathbf{\Phi})\vee 1)]\right|. \quad (7.7)$$

Due to Corollary 2.5, the second term on the r.h.s. of (7.7) tends to zero. On the other hand, (7.6) and Corollary 2.5 yield that for any $\varepsilon>0$,

$$\mathbb{E}\left|n^{-1}\log(Z(\mathbf{\Phi})\vee 1)-\mathfrak{B}_\infty(\pi_d)\right|\leq \mathbb{E}\left[\mathfrak{B}_\infty(\pi_d)-n^{-1}\log(Z(\mathbf{\Phi})\vee 1)\right]+2\varepsilon+o(1)=2\varepsilon+o(1),$$

as desired. □

Acknowledgment. We thank Andreas Galanis and Leslie Goldberg for helpful discussions.

References

[1] E. Abbe, A. Montanari: On the concentration of the number of solutions of random satisfiability formulas. Random Structures and Algorithms **45** (2014) 362–382.

[2] D. Achlioptas, A. Chtcherba, G. Istrate, C. Moore: The phase transition in 1-in-k SAT and NAE 3-SAT. Proc. 12th SODA (2001) 721–722.

[3] D. Achlioptas, C. Moore: Random k-SAT: two moments suffice to cross a sharp threshold. SIAM Journal on Computing **36** (2006) 740–762.

[4] D. Achlioptas, Y. Peres: The threshold for random k-SAT is $2^k\ln 2-O(k)$. Journal of the AMS **17** (2004) 947–973.

[5] M. Aizenman, R. Sims, S. Starr: An extended variational principle for the SK spin-glass model. Phys. Rev. B **68** (2003) 214403.

[6] N. Alon, J. Spencer: The probabilistic method. Wiley (2016).

[7] P. Ayre, A. Coja-Oghlan, P. Gao, N. Müller: The satisfiability threshold for random linear equations. Combinatorica, in press.

[8] A. Barvinok: Combinatorics and complexity of partition functions. Springer (2016).

[9] V. Bogachev, A. Kolesnikov: The Monge-Kantorovich problem: achievements, connections, and perspectives. Russian Mathematical Surveys **67** (2012) 785–890.

[10] B. Bollobás: The evolution of random graphs. Transactions of the AMS **286** (1984) 257–274.

[11] B. Bollobás, C. Borgs J. Chayes, J. Kim, D. Wilson: The scaling window of the 2-SAT transition. Random Structures and Algorithms **18** (2001) 201–256.

[12] Y. Boufkhad, O. Dubois: Length of prime implicants and number of solutions of random CNF formulae. Theoretical Computer Science **215** (1999) 1–30.

[13] P. Cheeseman, B. Kanefsky, W. Taylor: Where the *really* hard problems are. Proc. IJCAI (1991) 331–337.

[14] V. Chvátal, B. Reed: Mick gets some (the odds are on his side). Proc. 33th FOCS (1992) 620–627.

[15] A. Coja-Oghlan, T. Kapetanopoulos, N. Müller: The replica symmetric phase of random constraint satisfaction problems. Combinatorics, Probability and Computing, in press.

[16] A. Coja-Oghlan, F. Krzakala, W. Perkins, L. Zdeborová: Information-theoretic thresholds from the cavity method. Advances in Mathematics **333** (2018) 694–795.

[17] A. Coja-Oghlan, K. Panagiotou: The asymptotic k-SAT threshold. Advances in Mathematics **288** (2016) 985–1068.

[18] A. Coja-Oghlan, N. Wormald: The number of satisfying assignments of random regular k-SAT formulas. Combinatorics, Probability and Computing **27** (2018) 496–530.

[19] C. Cooper, A. Frieze, G. Sorkin: Random 2-SAT with prescribed literal degrees. Algorithmica **48** (2007) 249–265.

[20] D. Coppersmith, D. Gamarnik, M. Hajiaghayi, G. Sorkin: Random MAX SAT, random MAX CUT, and their phase transitions. Random Structures and Algorithms **24** (2004) 502–545.

[21] A. Dembo, A. Montanari: Ising models on locally tree-like graphs. Annals of Applied Probability **20** (2010) 565–592.

[22] A. Dembo, A. Montanari, N. Sun: Factor models on locally tree-like graphs. Annals of Probability **41** (2013) 4162–4213.

[23] M. Dietzfelbinger, A. Goerdt, M. Mitzenmacher, A. Montanari, R. Pagh, M. Rink: Tight thresholds for cuckoo hashing via XORSAT. arXiv:0912.0287 (2009).

[24] J. Ding, A. Sly, N. Sun: Satisfiability threshold for random regular NAE-SAT. Communications in Mathematical Physics **341** (2016) 435–489.

[25] J. Ding, A. Sly, N. Sun: Proof of the satisfiability conjecture for large k. Proc. 47th STOC (2015) 59–68.

[26] W. Dowling, J. Gallier: Linear-time algorithms for testing the satisfiability of propositional Horn formulae. Journal of Logic Programming **1** (1984) 267–284.

[27] O. Dubois, J. Mandler: The 3-XORSAT threshold. Proc. 43rd FOCS (2002) 769–778.

[28] W. Fernandez de la Vega: Random 2-SAT: results and problems. Theoretical Computer Science **265** (2001) 131–146.

[29] S. Franz, M. Leone: Replica bounds for optimization problems and diluted spin systems. J. Stat. Phys. **111** (2003) 535–564.

[30] A. Goerdt: A threshold for unsatisfiability. J. Comput. Syst. Sci. **53** (1996) 469–486

[31] F. Guerra: Broken replica symmetry bounds in the mean field spin glass model. Comm. Math. Phys. **233** (2003) 1–12.

[32] F. Krzakala, A. Montanari, F. Ricci-Tersenghi, G. Semerjian, L. Zdeborová: Gibbs states and the set of solutions of random constraint satisfaction problems. Proc. National Academy of Sciences **104** (2007) 10318–10323.

[33] T. Łuczak: Component behavior near the critical point of the random graph process. Random Structures and Algorithms **1** (1990) 287–310.

[34] M. Mézard, A. Montanari: Information, physics and computation. Oxford University Press (2009).

[35] M. Mézard, G. Parisi, R. Zecchina: Analytic and algorithmic solution of random satisfiability problems. Science **297** (2002) 812–815.

[36] R. Monasson, R. Zecchina: The entropy of the k-satisfiability problem. Phys. Rev. Lett. **76** (1996) 3881.

[37] R. Monasson, R. Zecchina: Statistical mechanics of the random K-SAT model. Phys. Rev. E **56** (1997) 1357–1370.

[38] A. Montanari, F. Ricci-Tersenghi, G. Semerjian: Solving constraint satisfaction problems through Belief Propagation-guided decimation. Proc. 45th Allerton (2007).

[39] A. Montanari, D. Shah: Counting good truth assignments of random k-SAT formulae. Proc. 18th SODA (2007) 1255–1264.
[40] D. Panchenko: Spin glass models from the point of view of spin distributions. Annals of Probability **41** (2013) 1315–1361.
[41] D. Panchenko: On the replica symmetric solution of the K-sat model. Electron. J. Probab. **19** (2014) #67.
[42] D. Panchenko, M. Talagrand: Bounds for diluted mean-fields spin glass models. Probab. Theory Relat. Fields **130** (2004) 319–336.
[43] B. Pittel, G. Sorkin: The satisfiability threshold for k-XORSAT. Combinatorics, Probability and Computing **25** (2016) 236–268.
[44] F. Rassmann: On the number of solutions in random graph k-colouring. Combinatorics, Probability and Computing **28** (2019) 130–158.
[45] A. Scott, G. Sorkin: Solving sparse random instances of Max Cut and Max 2-CSP in linear expected time. Combinatorics, Probability and Computing **15** (2006) 281–315.
[46] A. Sharell: Concentration of the number of solutions to a random 2-CNF formula. Manuscript (2000).
[47] A. Sly, N. Sun, Y. Zhang: The number of solutions for random regular NAE-SAT. Proc. 57th FOCS (2016) 724–731.
[48] M. Talagrand: The high temperature case for the random K-sat problem. Probab. Theory Related Fields **119** (2001) 187–212.
[49] L. Valiant: The complexity of enumeration and reliability problems. SIAM Journal on Computing **8** (1979) 410–421.

DIMITRIS ACHLIOPTAS, optas@di.uoa.gr, UNIVERSITY OF ATHENS, DEPARTMENT OF COMPUTER SCIENCE & TELECOMMUNICATIONS, PANEPISTIMIOPOLIS, ILISSIA, ATHENS 15784, GREECE.

AMIN COJA-OGHLAN, acoghlan@math.uni-frankfurt.de, GOETHE UNIVERSITY, MATHEMATICS INSTITUTE, 10 ROBERT MAYER ST, FRANKFURT 60325, GERMANY.

MAX HAHN-KLIMROTH, hahnklim@math.uni-frankfurt.de, GOETHE UNIVERSITY, MATHEMATICS INSTITUTE, 10 ROBERT MAYER ST, FRANKFURT 60325, GERMANY.

JOON LEE, lee@math.uni-frankfurt.de, GOETHE UNIVERSITY, MATHEMATICS INSTITUTE, 10 ROBERT MAYER ST, FRANKFURT 60325, GERMANY.

NOËLA MÜLLER, nmueller@math.uni-frankfurt.de, GOETHE UNIVERSITY, MATHEMATICS INSTITUTE, 10 ROBERT MAYER ST, FRANKFURT 60325, GERMANY.

MANUEL PENSCHUCK, manuel@ae.cs.uni-frankfurt.de, GOETHE UNIVERSITY, COMPUTER SCIENCE INSTITUTE, 11–15 ROBERT MAYER ST, FRANKFURT 60325, GERMANY.

GUANGYAN ZHOU, gyzhou76@gmail.com, SCHOOL OF MATHEMATICS AND STATISTICS, BEIJING TECHNOLOGY AND BUSINESS UNIVERSITY, BEIJING 100048, CHINA.

B

WARNING PROPAGATION: STABILITY AND SUBCRITICALITY

OLIVER COOLEY, JOON LEE, JEAN B. RAVELOMANANA

ABSTRACT. Warning Propagation is a combinatorial message passing algorithm that unifies and generalises a wide variety of recursive combinatorial procedures. Special cases include the Unit Clause Propagation and Pure Literal algorithms for satisfiability as well as the peeling process for identifying the k-core of a random graph. Here we analyse Warning Propagation in full generality on a very general class of multi-type random graphs. We prove that under mild assumptions on the random graph model and the stability of the the message limit, Warning Propagation converges rapidly. In effect, the analysis of the fixed point of the message passing process on a random graph reduces to analysing the process on a multi-type Galton-Watson tree. This result corroborates and generalises a heuristic first put forward by Pittel, Spencer and Wormald in their seminal k-core paper (JCTB 1996). [MSc: 05C80]

1. INTRODUCTION

1.1. **Motivation and contributions.** The study of combinatorial structures in random graphs is a huge field encompassing a wide variety of different topics, and the techniques used to study them are as plentiful and as varied as the topics themselves, but there are common themes to be found in approaches in seemingly unrelated areas. One such theme is the implementation of a discrete-time algorithm to pinpoint the desired substructure. A classic example is Unit Clause Propagation, an algorithm which traces implications in a Boolean satisfiability problem [1, 13]. If the formula contains unit clauses, i.e. clauses containing only one literal, the algorithm sets the corresponding variable to the appropriate truth value. This clearly has further knock-on effects: other clauses in which the variable appears with the same sign are now automatically satisfied and can be deleted; but clauses in which the variable appears with the opposite sign are effectively shortened, potentially giving rise to further unit clauses, and the process continues. Ultimately, we may reach a contradiction or a satisfying assignment, or neither if the process stops with all clauses containing at least two literals. In this case we can "have a guess", assigning a random truth value to a random variable and continue the process.

Another quintessential example is the peeling process for the k-core, in which recursively vertices of degree at most $k-1$ are deleted from the graph until what remains is the (possibly empty) k-core (see e.g. [24, 21]). Further examples include the study of sparse random matrices, the freezing phase transition in random constraint satisfaction problems, bootstrap percolation or decoding low-density parity check codes [2, 6, 10, 14, 22, 25].

Warning Propagation is a a message passing scheme that provides a unified framework for such recursive processes [20]. Roughly speaking, the scheme sends messages along edges of a graph which are then recursively updated: the messages that a vertex sends depends on the messages that it receives from its neighbours according to some update rule. The semantics of the messages and the choice of update rule is fundamentally dependent on the particular problem to which the scheme is applied: the messages may indicate truth values of variables in a satisfiability formula, for example, or membership of the k-core. To understand the combinatorial substructures under consideration, we need to understand the fixed points of the corresponding recursive algorithms, or equivalently the fixed points of the appropriate instances of Warning Propagation.

There have been many different approaches to analysing such recursive processes using a variety of different techniques. One classical tool is the differential equations method [28], which was used in the seminal k-core paper of Pittel, Spencer and Wormald [24] as well as in the analysis of Unit Clause Propagation [1]. Other approaches include branching processes [26], enumerative methods [5], or birth-death processes [17, 18].

However, despite their very different appearances, these approaches all share a common feature: in one way or another, they show that the recursive process converges quickly to its fixed point. In other words, the final outcome of the process can be approximated arbitrarily well by running only a bounded number of rounds of the recursive process. Equivalently, in each of these particular instances, the Warning Propagation scheme converges quickly.

Jean B. Ravelomanana is supported by DFG CO 646/4.
Oliver Cooley is supported by Austrian Science Fund (FWF): I3747.

In this paper we analyse Warning Propagation in full generality on a very general multi-type model of random graphs. Special cases of this model include not just the Erdős-Rényi binomial random graph model $G(n,p)$ and its k-partite analogues, but also the stochastic block model, random regular graphs or indeed random graphs with a prescribed degree sequence, and factor graphs of random hypergraphs. We prove that under mild, easy-to-check assumptions Warning Propagation converges rapidly. Not only does this result confirm the heuristic that running Warning Propagation for a bounded number of rounds suffices to approximate its ultimate fixed point arbitrarily well, our result also identifies the essential reason for this behaviour. More precisely, after a large but bounded number of steps, the subsequent knock-on effect of a single change can be modelled by a branching process; we demonstrate that a mild stability assumption guarantees that this branching process is subcritical. The upshot is that late changes in the process will ultimately fizzle out rather than triggering a cascade of further effects.

Apart from re-proving known results in a new, unified way, the main results of this paper facilitate new applications of Warning Propagation. Indeed, to analyse any specific recursive process that can be translated into the formalism of Theorem 1.3 below one just needs to investigate the recursion on a multi-type Galton-Watson tree that mimics the local structure of the respective random graph model. Typically this task boils down to a mundane fixed point problem in Euclidean space. Theorem 1.3 thus enables an easy and accurate analysis of generic recursive processes on random structures. A concrete example that actually inspired this work was our need to study a recursive process that arises in the context of random matrix theory [4].

1.2. **Random graph model.** Our goal is to study warning propagation on a random graph $\mathbb{G}$, which may be chosen from a wide variety of different models, and which we first describe briefly and informally—the formal requirements on $\mathbb{G}$ are introduced in Section 2.2, specifically in Assumption 2.10.

We will assume that the vertices of $\mathbb{G}$ are of *types* $1,\dots,k$ for some fixed integer k; we denote by V_i the set of vertices of type i for $i \in [k]$ and set $n_i := |V_i|$. The n_i need not be deterministically fixed, but may themselves be random variables depending on an implicit parameter $n \in \mathbb{N}$ which tends to infinity, and in particular all asymptotics are with respect to n unless otherwise specified. Vertices of different types may exhibit very different behaviour, but vertices of the same type should behave according to the same random distribution. More specifically, for a vertex $v \in V_i$ the (asymptotic) distribution of the numbers of neighbours of each type $j \in [k]$ will be described by $\mathcal{Z}_i$, which is a probability distribution on $\mathbb{N}_0^k$, the set of sequences of natural numbers of length k; the j-th entry of $\mathcal{Z}_i$ describes the numbers of neighbours of type j. This will be introduced more formally in Section 2.1

To give a concrete example, if we were to study simply $G(n,d/n)$ for some fixed constant d, we would set $k=1$ and $n_1 = n$, and each vertex would have $\mathrm{Po}(d)$ neighbours of type 1. For random d-regular graphs, we would also have $k=1$ and $n_1 = n$, but now the number of neighbours would be deterministically d (i.e. the random distribution would be entirely concentrated on d).

A slightly more complex example is random d-SAT with n variables and m clauses of size d. The standard way of representing an instance of the problem is to have vertex classes V_1, V_2 representing the variables and the clauses respectively, with an edge between a variable v and a clause A if v appears in A. Furthermore, the edge is coloured depending on whether v is negated in A or not. However, since we do not allow for edges of different types, we must represent this differently. This can be done by adding two further classes V_3, V_4 and subdividing an edge vA with a vertex of type 3 if v is unnegated in A and of type 4 otherwise. Then a vertex of V_1, representing a variable, would have $\mathrm{Po}\left(\frac{dm}{2n}\right)$ neighbours of type 3 and similarly and independently of type 4; a vertex of V_2, representing a clause, would have $X \sim \mathrm{Bin}(d,1/2)$ neighbours of type 3 and $d-X$ neighbours of type 4; while vertices of V_3, V_4 would each have precisely one neighbour each of types 1 and 2.

We will have various relatively loose restrictions on the graph model $\mathbb{G}$ which are required during the proof, see Section 2.2 for the full list. Informally, we require $\mathbb{G}$ to satisfy four conditions with high probability, namely:

- The vertex classes have the same order of magnitude and not too large variance.
- The graph $\mathbb{G}$ is uniformly random given its type-degree sequence.
- There are few vertices of high degree.
- The local structure is described by the $\mathcal{T}_i(\mathcal{Z}_1,\dots,\mathcal{Z}_k)$.

Here we note in particular that we require each V_i to have bounded average degree.

1.3. **Warning propagation.** In this section we formally introduce the Warning Propagation (WP) message passing scheme and its application to random graphs. Applied to a graph G, Warning Propagation will associate two directed messages $\mu_{v\to w}, \mu_{w\to v}$ with each edge vw of G. These messages take values in a finite alphabet Σ. Hence, let

$\mathscr{M}(G)$ be the set of all vectors $\left(\mu_{v\to w}\right)_{(v,w)\in V(G)^2:vw\in E(G)} \in \Sigma^{2|E(G)|}$. The messages get updated in parallel according to some fixed rule. To formalise this, for $d\in\mathbb{N}$ let $\left(\!\!\binom{\Sigma}{d}\!\!\right)$ be the set of all d-ary multisets with elements from Σ and let

$$\varphi : \bigcup_{d\geq 0} \left(\!\!\binom{\Sigma}{d}\!\!\right) \to \Sigma \tag{1.1}$$

be an *update rule* that, given any multiset of input messages, computes an output message. Then we define the Warning Propagation operator on G by

$$\mathrm{WP}_G : \mathscr{M}(G) \to \mathscr{M}(G), \qquad \mu = \left(\mu_{v\to w}\right)_{vw} \mapsto \left(\varphi\left(\{\!\{\mu_{u\to v} : uv\in E(G), u\neq w\}\!\}\right)\right)_{vw},$$

where $\{\!\{a_1,\dots,a_k\}\!\}$ denotes the multiset whose elements (with multiplicity) are $a_1,\dots,a_k$.

In words, to update the message from v to w we apply the update rule φ to the messages that v receives from all its *other* neighbours $u\neq w$.

To give some examples of concrete instances, when studying the k-core the messages would typically be 0 or 1, and the update rule would be defined by $\varphi(A) = \mathbf{1}\left\{\sum_{a\in A} a \geq k-1\right\}$, i.e. a vertex sends a message of 1 to a neighbour iff it receives at least $k-1$ messages of 1 from its other neighbours. At the end of the process, the k-core consists of precisely those vertices which receive at least k messages of 1 from their neighbours. Alternatively, in a constraint satisfaction problem, the message from a variable to a constraint may indicate that the variable is frozen to a specific value due to its other constraints, while the message from a constraint to a variable indicates whether that constraint requires the variable to take a specific value.

Let us note that in many applications, the obvious approach would be to define the WP scheme with different update rules $\varphi_1,\dots,\varphi_k$ for each type of vertex, or indeed where the update rule takes account of which type of vertex each message was received from. While this would be entirely natural, it would lead to some significant notational complexities later on. We therefore adopt an alternative approach: the messages of the alphabet Σ will, in particular, encode the types of the source and target vertices, and we can therefore make do with a single update function which receives this information and takes account of it. Of course, this means that along a particular directed edge, many messages from Σ are automatically disqualified from appearing because they encode the wrong source and target types. Indeed, at a particular vertex all incoming messages must encode the same appropriate target type, and therefore many multisets of messages can never arise as inputs of the update function. On the other hand, the major benefit of this approach is that much of the notational complexity of the problem is subsumed into the alphabet Σ and the update function φ. This will be discussed more formally in Sections 2, and 3.

In most applications of Warning Propagation the update rule (1.1) enjoys a monotonicity property which ensures that for any graph G and for any initialisation $\mu^{(0)}\in\mathscr{M}(G)$ the pointwise limit $\mathrm{WP}^*_G\left(\mu^{(0)}\right) := \lim_{t\to\infty}\mathrm{WP}^t_G\left(\mu^{(0)}\right)$ exists, although in general monotonicity is not a necessary prerequisite for such a limit to exist. If it does, then clearly this limit is a fixed point of the Warning Propagation operator.

Our goal is to study the fixed points of WP and, particularly, the rate of convergence on the random graph $\mathbb{G}$. We will assume that locally $\mathbb{G}$ has the structure of a multi-type Galton-Watson tree. We will prove that under mild assumptions on the update rule, the WP fixed point can be characterised in terms of this local structure only. To this end we need to define a suitable notion of a WP fixed point on a random tree. At this point we could consider the space of (possibly infinite) trees with WP messages, define a measure on this space and consider the action that the WP operator induces. Fortunately, the recursive nature of the Galton-Watson tree allows us to bypass this complexity. Specifically, our fixed point will just be a collection of probability distributions on Σ, one for each possible type of directed edge, such that if the children of a vertex v in the tree send messages independently according to these distributions, then the message from v to its own parent will also have the appropriate distribution from the collection. The collection of distributions can be conveniently expressed in matrix form. For a matrix M, we denote by $M[i,j]$ the entry at position (i,j) in the matrix and by $M[i]$ the i-th row $\left(M[i,j]\right)_{j\in[k]}$. [1]

Definition 1.1. *Given a set S, a* probability distribution matrix *on S is a $k\times k$ matrix Q in which each entry $Q[i,j]$ of Q is a probability distribution on S.*

The intuition is that the entry $Q[i,j]$ should model the probability distribution of the message along an edge from a vertex of type i to a vertex of type j. Heuristically, the incoming messages at a vertex will be more or less

[1] We avoid the usual M_{ij} index notation since this will clash with other subscripts later on.

independent of each other; short-range correlations can only arise because of short cycles, of which there are very few in the sparse regime, while long-range correlations should be weak if they exist at all. We will certainly *initialise* the messages independently.

Definition 1.2. *For a graph G and a probability distribution matrix Q on Σ, we refer to* initialising messages in G according to Q *to mean that we initialise the message $\mu_{u\to v}(0)$ for each directed edge (u,v) independently at random according to $Q[i,j]$, where i and j are the types of u and v respectively.*

In many applications, the initialisation of the messages is actually deterministic, i.e., each entry of Q is concentrated on a single element of Σ, but there are certainly situations in which it is important to initialise randomly.

Given the local structure of the random graph model $\mathbb{G}$ as described by a multi-type Galton-Watson tree, we can compute the asymptotic effect of the warning propagation update rules on the probability distribution matrix: for a directed edge vw of type (i,j), we consider the other neighbours of v with their types according to the local structure, generate messages independently according to the current probability distribution matrix and compute the updated message along vw. Since the generation of neighbours and of messages was random, the updated vw message is also random and its distribution gives the corresponding entry of the updated matrix. Repeating this for all $i,j\in[k]$ gives the updated matrix. This process is described more formally in Section 2.1.

With this notion of updating probability distribution matrices, we can consider the *limit* of an initially chosen matrix Q_0. More specifically, we will need the existence of a *stable WP limit*, meaning that the update function is a contraction in the neighbourhood of the limit with respect to an appropriate metric. Again, formal details are given in Section 2.1.

1.4. **Main result.** Given a probability distribution matrix Q_0 on Σ, we ask how quickly Warning Propagation will converge on $\mathbb{G}$ from a random initialisation according to Q_0.

We will use $\mathrm{WP}^t_{v\to w}(\mu^{(0)})$ to denote the message from v to w in $\mathbb{G}$ after t iterations of $\mathrm{WP}_{\mathbb{G}}$ with initialisation $\mu^{(0)}$. Note that the graph $\mathbb{G}$ is implicit in this notation.

Theorem 1.3. *Let $\mathbb{G}$ be a random graph model satisfying Assumption 2.10 and let P, Q_0 be probability distributions on Σ such that P is the stable WP limit of Q_0. Then for any $\delta>0$ there exists $t_0=t_0(\delta,\mathscr{Z},\varphi,Q_0)$ such that the following is true.*

Suppose that $\mu^{(0)}\in\mathscr{M}(\mathbb{G})$ is an initialisation according to Q_0. Then w.h.p. for all $t\geq t_0$ we have

$$\sum_{v,w:vw\in E(\mathbb{G})}\mathbf{1}\left\{\mathrm{WP}^t_{v\to w}(\mu^{(0)})\neq\mathrm{WP}^{t_0}_{v\to w}(\mu^{(0)})\right\}<\delta n.$$

In other words, the WP messages at any time $t\geq t_0$ are identical to those at time t_0 except on a set of at most δn directed edges. Thus Theorem 1.3 shows that under a mild stability condition Warning Propagation converges rapidly. Crucially, the number t_0 of steps before Warning Propagation stabilises does not depend on the underlying parameter n, or even on the exact nature of the graph model $\mathbb{G}$, but only on the desired accuracy δ, the degree distribution $\mathscr{Z}$, the Warning Propagation update rule φ and the initial distribution Q_0.

1.5. **Discussion and related work.** Theorem 1.3 implies a number of results that were previously derived by separate arguments. For instance, the theorem directly implies the main result from [24] on the k-core in random graphs. Specifically, the theorem yields the threshold for the emergence of the k-core threshold as well as the typical number of vertices and edges in the core (in a law of large numbers sense). Of course, several alternative proofs of (and extensions of) this result, some attributed as simple, exist [8, 9, 11, 12, 17, 19, 21, 26], but here we obtain this result as an application of a more general theorem.

Since our model also covers multi-type graphs, it enables a systematic approach to the freezing phenomenon in random constraint satisfaction problems [20, 22, 23], as well as to hypergraph analogues of the core problem [7, 17, 19, 21, 24, 26, 27] by considering the factor graph.

The specific application that led us to investigate Warning Propagation in general deals with random matrix theory [4]. In that context Warning Propagation or equivalent constructions have been applied extensively [3, 10, 16, 20]. Technically the approach that is most similar to the present proof strategy is that of Ibrahimi, Kanoria, Kraning and Montanari [16], who use an argument based on local weak convergence.

1.6. **Proof outline.** A fundamental aspect of the proof is that we do not analyse WP directly on $\mathbb{G}$ and consider its effect after t_0 iterations, but instead define an alternative random model $\hat{\mathbb{G}}_{t_0}$ (see Definition 3.4): Rather than generating the edges of the graph and then computing messages, this random model first generates half-edges with messages, and then matches up the half-edges in a consistent way. Thus in particular the messages are known a priori. The key point is that the two models are very similar (Lemma 3.7).

Among other things, it follows from this approximation that very few changes will be made when moving from $\mathrm{WP}_{\mathbb{G}}^{t_0-1}\left(\mu^{(0)}\right)$ to $\mathrm{WP}_{\mathbb{G}}^{t_0}\left(\mu^{(0)}\right)$, but in principle these few changes could cause cascade effects later on. To rule this out we define a branching process $\mathfrak{T}$ which approximates the subsequent effects of a single change at time t_0. The crucial observation is that the stability of the distributional fixed point P implies that this branching process is subcritical (Proposition 6.3), and is therefore likely to die out quickly. Together with the fact that very few changes are made at step t_0, this ultimately implies that there will be few subsequent changes.

1.7. **Paper overview.** The remainder of the paper is arranged as follows. In Section 2 we formally introduce the notation, terminology and assumptions on the model $\mathbb{G}$ which appear in the statement of Theorem 1.3 and throughout the paper. In Section 3 we define the $\hat{\mathbb{G}}_{t_0}$ model and introduce Lemma 3.7, which states that this model is a good approximation for Warning Propagation on $\mathbb{G}$. In Section 4 we present various preliminary results that will be used in later proofs. In Section 5 we go on to prove Lemma 3.7.

In Section 6 we introduce the branching process $\mathfrak{T}$ and prove that it is subcritical. In Section 7 we then draw together the results of previous sections to prove that after t_0 iterations of WP, very few further changes will be made, and thus prove Theorem 1.3.

2. Prerequisites

In this section we formally define some of the notions required for the statement of Theorem 1.3, as well as introducing the assumptions that we require the model $\mathbb{G}$ to satisfy. For a set S, we will denote by $\mathscr{P}(S)$ the space of probability distributions on S. We will occasionally abuse notation by conflating a random variable with its probability distribution, and using the same notation to refer to both.

2.1. Distributional fixed points.

Definition 2.1. *For each $i \in [k]$, let $\mathscr{Z}_i \in \mathscr{P}\left(\mathbb{N}_0^k\right)$. For $j \in [k]$, denote by $\mathscr{Z}_{ij}$ the marginal distributions of $\mathscr{Z}_i$ on the j-th entry. We say that $(i,j) \in [k]^2$ is an* admissible *pair if $\mathbb{P}\left(\mathscr{Z}_{ij} \geq 1\right) \neq 0$, and denote by $\mathscr{K} = \mathscr{K}(\mathscr{Z}_1, \dots, \mathscr{Z}_k)$ the set of admissible pairs.*

Intuitively, the $\mathscr{Z}_i$ will describe the local structure of the random input graph $\mathbb{G}$, in the sense that the distribution of the neighbours with types of a vertex $v \in V_i$ will be approximately $\mathscr{Z}_i$ (see Definition 2.8 later). Therefore the admissible pairs describe precisely those pairs of classes V_i and V_j between which we expect some edges to exist. In particular, if the $\mathscr{Z}_i$ accurately describe the local structure, then (i,j) is admissible if and only if (j,i) is also admissible.

Note, however, that if we aim to analyse the message along a directed edge from $v \in V_i$ to $w \in V_j$, we need to know about the distribution of the *other* neighbours of v, and cannot simply draw from $\mathscr{Z}_i$ because we already have one guaranteed neighbour of type j, which may affect the distribution. This motivates the following definition.

Definition 2.2. *Let $\mathscr{Z}_1, \dots, \mathscr{Z}_k \in \mathscr{P}\left(\mathbb{N}_0^k\right)$. For each $(i,j) \in \mathscr{K}$, define $\mathscr{Y}_{j,i} = \mathscr{Y}_{j,i}(\mathscr{Z}_i) \in \mathscr{P}\left(\mathbb{N}_0^k\right)$ to be the probability distribution such that for $(a_1, \dots, a_k) \in \mathbb{N}_0^k$ we have*

$$\mathbb{P}\left(\mathscr{Y}_{j,i} = (a_1, \dots, a_k)\right) := \frac{\mathbb{P}\left(\mathscr{Z}_i = \left(a_1, \dots, a_{j-1}, a_j + 1, a_{j+1}, \dots, a_k\right)\right)}{\mathbb{P}\left(\mathscr{Z}_{ij} \geq 1\right)}.$$

Equivalently, $\mathscr{Y}_{j,i}$ and $\mathscr{Z}_i$ satisfy the following relation. Let $\mathscr{E}_{ij}$ be the event $\mathscr{Z}_{ij} \geq 1$. Then for any $(a_1, \dots, a_k) \in \mathbb{N}_0^k$ such that $a_j \geq 1$ we have

$$\mathbb{P}\left(\mathscr{Y}_{j,i} = \left(a_1, \dots, a_{j-1}, a_j - 1, a_{j+1}, \dots, a_k\right)\right) = \mathbb{P}\left(\mathscr{Z}_i = (a_1, \dots, a_k) \,\middle|\, \mathscr{E}_{ij}\right).$$

We will talk about *generating vertices with types* according to a distribution $\mathscr{D}$ on $\mathbb{N}_0^k$, by which we mean that we generate a vector $(z_1, \dots, z_k)$ according to $\mathscr{D}$, and for each $i \in [k]$ we generate z_i vertices of type i. Usually, $\mathscr{D}$ will be $\mathscr{Z}_i$ or $\mathscr{Y}_{j,i}$ for some $i, j \in [k]$. Depending on the context, we may also talk about generating *neighbours, children, half-edges* etc. with types, in which case the definition is analogous.

Definition 2.3. *Given $\mathscr{D} \in \mathscr{P}\left(\mathbb{N}_0^k\right)$ and a vector $\boldsymbol{q} = \left(q_1, \ldots, q_k\right) \in \left(\mathscr{P}(\Sigma)\right)^k$ of probability distributions on Σ, let us define a multiset $\mathscr{M}\left(\mathscr{D}, \boldsymbol{q}\right)$ of elements of Σ as follows.*

- *Generate a vector $(a_1, \ldots, a_k)$ according to $\mathscr{D}$.*
- *For each $j \in [k]$ independently, select a_j elements of Σ independently according to q_j. Call the resulting multiset $\mathscr{M}_j$.*
- *Define $\mathscr{M}\left(\mathscr{D}, \boldsymbol{q}\right) := \biguplus_{j=1}^{k} \mathscr{M}_j$.*[2]

The motivation behind this definition is that $\mathscr{D}$ will represent a distribution of neighbours with types, typically $\mathscr{Z}_i$ or $\mathscr{Y}_{j,i}$ for some $i, j \in [k]$. Meanwhile $\boldsymbol{q}$ will represent the distributions of messages from the vertices of various types, typically chosen according to the appropriate entry of a probability distribution matrix, which are heuristically almost independent. Thus $\mathscr{M}\left(\mathscr{D}, \boldsymbol{q}\right)$ describes a random multiset of incoming messages at a vertex with the appropriate distribution.

We can now formally describe how the WP update function affects the distribution of messages, as described by a probability distribution matrix on Σ.

Definition 2.4. *Given a probability distribution matrix Q on Σ with rows $Q[1], \ldots, Q[k]$, let $\phi_\varphi(Q)$ denote the probability distribution matrix R on Σ where each entry $R[i,j]$ is the probability distribution on Σ given by*

$$R[i,j] := \varphi\left(\mathscr{M}\left(\mathscr{Y}_{j,i}, Q[i]\right)\right).$$

Further, let $\phi_\varphi^t(Q) = \phi_\varphi\left(\phi_\varphi^{t-1}(Q)\right)$ denote the t^{th} iterated function of ϕ_φ evaluated at Q. In order to ease notation, we sometimes denote $\phi_\varphi^t(Q)$ by $Q^{(t)}$ when ϕ_φ is clear from the context.

In an idealised scenario, this update function precisely describes how the probability distribution matrix should change over time: along a directed edge of type (i,j), the messages in the next step will be determined by *other* incoming messages at the source vertex; the neighbours and their types may be generated according to $\mathscr{Y}_{j,i}$; the corresponding messages are generated according to $Q[i]$.

We will ultimately show that this idealised scenario is indeed a reasonable approximation. But we are also interested in what occurs when we iterate this process from an appropriate starting matrix. Does it converge to some limit? In order to quantify this, we need the following metric on the space of probability distribution matrices, which is a simple extension of the standard total variation distance for probability distributions, denoted $d_{\mathrm{TV}}(\cdot,\cdot)$.

Definition 2.5. *The total variation distance of two $k \times k$ probability distribution matrices Q and R on the same set S is defined as $d_{\mathrm{TV}}(Q,R) := \sum_{i,j \in [k]} d_{\mathrm{TV}}\left(Q[i,j], R[i,j]\right)$.*

It is elementary to check that d_{TV} is indeed a metric on the space of $k \times k$ probability distribution matrices on Σ, and whenever we talk of limits in this space, those limits are with respect to this metric. We can now define the key notion of a *stable WP limit*, which is fundamental to Theorem 1.3.

Definition 2.6. *Let P be a probability distribution matrix on Σ and $\varphi : \bigcup_{d \geq 0} \left(\!\!\binom{\Sigma}{d}\!\!\right) \to \Sigma$ be a WP update rule.*

(1) We say that P is a fixed point *if $\phi_\varphi(P) = P$.*
(2) A fixed point P is stable *if ϕ_φ is a contraction on a neighbourhood of P with respect to the total variation distance d_{TV} as defined in Definition 2.5.*
(3) We say that P is the stable WP limit *of a probability distribution matrix Q_0 on Σ if P is a stable fixed point, and furthermore the limit $\phi_\varphi^*(Q_0) := \lim_{t \to \infty} \phi_\varphi^t(Q_0)$ exists and equals P.*

2.2. **Assumptions on the $\mathbb{G}$ model.** In order to apply the results of this paper, we will need the random graph $\mathbb{G}$ to be reasonably well-behaved; formally, we require a number of relatively mild properties to be satisfied. In order to introduce the assumptions, we need to introduce some terminology and notation.

Recall that depending on the application, the numbers of vertices $n_1, \ldots, n_k$ in each of the k classes may be random, or some may be random and others deterministic. For example, if we consider the standard bipartite factor graph of a binomial random r-uniform hypergraph $H^r(n,p)$, then one class representing the vertices of $H^r(n,p)$ would have $n_1 = n$ vertices deterministically, while the other class representing the edges of $H^r(n,p)$ would have $n_2 \sim \mathrm{Bin}\left(\binom{n}{r}, p\right)$ vertices.

[2] The symbol $\biguplus$ denotes the multiset union of two multisets A, B, e.g. if $A = \{\{a,a,b\}\}$ and $B = \{\{a,b,c,c\}\}$ then $A \biguplus B = \{\{a,a,a,b,b,c,c\}\}$.

We seek to model this situation, which we do by introducing a probability distribution vector $\mathcal{N} = (\mathcal{N}_1, \dots, \mathcal{N}_k) \in \mathcal{P}\left(\mathbb{N}_0^k\right)$. Each $\mathcal{N}_i$ is a probability distribution on $\mathbb{N}_0$, although in general they may be dependent on each other. As mentioned informally earlier, we will also have an implicit parameter n, so $\mathcal{N} = \mathcal{N}(n)$, and we are interested in asymptotics as $n \to \infty$. Note that as in the example of factor graphs of hypergraphs above, and in many other examples, we could certainly have $\mathcal{N}_1 = n$ deterministically. As previously mentioned, we will often conflate random variables and their associated probability distributions; in particular we will use n_i instead of $\mathcal{N}_i$.

Definition 2.7. *For a k-type graph G, the type-degree of a vertex $v \in V(G)$, which we denote by $\boldsymbol{d}(v)$, is the sequence $(i, d_1, \dots, d_k) \in [k] \times \mathbb{N}_0^k$ where i is the type of v and where d_j is the number of neighbours of v of type j. Moreover, the* type-degree sequence *$\boldsymbol{D}(G)$ of G is the sequence $(\boldsymbol{d}(v))_{v \in V(G)}$ of the type-degrees of all the vertices of G.*

This is an obvious generalisation of the standard degree sequence in which we additionally keep track of the types of the vertices and their neighbours. We note that for $(\boldsymbol{d}(v))_{v \in V(G)}$ to be well defined, we need an order for the set of vertices $V(G)$. Since the order of the type-degree sequence will not play any role in future, we may choose such an order arbitrarily.

We also need to describe the local structure of the graph in terms of a branching process which depends on the degree distributions $\mathcal{Z}_1, \dots, \mathcal{Z}_k$.

Definition 2.8. *Let $\mathcal{Z}_1, \dots, \mathcal{Z}_k \in \mathcal{P}\left(\mathbb{N}_0^k\right)$ and for all $(i, j) \in \mathcal{K}$, let $\mathcal{Y}_{j,i}$ be as in Definition 2.2. For each $i \in [k]$, let $\mathcal{T}_i := \mathcal{T}_i(\mathcal{Z}_1, \dots, \mathcal{Z}_k)$ denote a k-type Galton-Waltson process defined as follows:*

(1) The process starts with a single vertex u of type i.
(2) Generate children of u with types according to $\mathcal{Z}_i$.
(3) Subsequently, starting from the children of u, further vertices are produced recursively according to the following rule: for every vertex w of type h with a parent w' of type ℓ, generate children of w with types according to $\mathcal{Y}_{\ell,h}$ independently.

Moreover, for $r \in \mathbb{N}_0$ we denote by $\mathcal{T}_i^r$ the branching process $\mathcal{T}_i$ truncated at depth r.

It will be part of our assumptions on $\mathbb{G}$ that the branching processes $\mathcal{T}_i$ do indeed describe the local structure of $\mathbb{G}$ w.h.p.. To quantify this statement, we will need to compare the distributions of the $\mathcal{T}_i$ with the empirical local structure of $\mathbb{G}$. Given a k-type graph G, a vertex $u \in V(G)$ and $r \in \mathbb{N}_0$, let $B_G(u, r)$ be the k-type subgraph of G induced by the neighbourhood of u up to depth r (i.e. all vertices that can be reached by a path of length at most r from u), rooted at the vertex u. We say that two (vertex-)rooted k-type graphs G and G' are *isomorphic*, which we denote by $G \cong G'$, if there exists a graph isomorphism between G and G' which preserves the roots and the types of the vertices. Let $\mathcal{G}_\star$ be the set of isomorphism classes of (vertex-)rooted k-type graphs (or more precisely, a set consisting of one representative from each isomorphism class). We define the following empirical neighbourhood distribution for a given k-type graph G.

Definition 2.9. *Let G be a k-type graph with parts $V_1(G), \dots, V_k(G)$, let $i \in [k]$ and $r \in \mathbb{N}_0$. Then for a graph $H \in \mathcal{G}_\star$, we define*

$$\mathfrak{U}_{i,r}^G(H) := \frac{1}{|V_i(G)|} \sum_{u \in V_i(G)} \mathbf{1}\{B_G(u, r) \cong H\}.$$

In other words, $\mathfrak{U}_{i,r}^G(H)$ is the proportion of vertices in the class $V_i(G)$ whose r-depth neighbourhood in G is isomorphic to H. When the graph G is clear from the context, we will drop the superscript G in $\mathfrak{U}_{i,r}^G$.

Note that $\mathfrak{U}_{i,r}^G$ defines a probability distribution on the class of rooted k-type graphs H of depth at most r, and therefore it can be compared with the truncated branching processes $\mathcal{T}_i^r$, which we will do in Assumption 2.10 (specifically **A4**). This assumption lays out the various properties that are required for our proofs. For parameters $a = a(n)$ and $b = b(n)$, we sometimes use the notation $a \ll b$ as a shorthand for $a = o(b)$, and similarly $a \gg b$ for $b = o(a)$.

Assumption 2.10. *There exist functions*

$$1 \ll \Delta_0 = \Delta_0(n) \ll n^{1/10} \tag{2.1}$$

and $\zeta = \zeta(x) \xrightarrow{x \to \infty} \infty$ and a probability distribution vector $\mathcal{Z} := (\mathcal{Z}_1, \dots, \mathcal{Z}_k) \in \left(\mathcal{P}\left(\mathbb{N}_0^k\right)\right)^k$ such that for all $i \in [k]$ and for all $x \in \mathbb{R}$, we have

$$\mathbb{P}\left(\|\mathcal{Z}_i\|_1 > x\right) \le \exp\left(-\zeta(x) \cdot x\right), \tag{2.2}$$

and such that the random graph $\mathbb{G}$ satisfies the following properties:

A1 *For all $i \in [k]$ we have $\mathbb{E}(n_i) = \Theta(n)$ and $\mathrm{Var}(n_i) = o\left(n^{8/5}\right)$.*
A2 *For any two simple k-type graphs G and H satisfying $\boldsymbol{D}(G) = \boldsymbol{D}(H)$, we have $\mathbb{P}(\mathbb{G} = G) = (1 + o(1))\,\mathbb{P}(\mathbb{G} = H)$.*
A3 *W.h.p. $\Delta(\mathbb{G}) \le \Delta_0$;*
A4 *For any $i \in [k]$ and $r \in \mathbb{N}_0$ we have*

$$d_{\mathrm{TV}}\left(\mathfrak{U}_i^r(\mathbb{G}), \mathscr{T}_i^r(\mathscr{Z})\right) \ll \frac{1}{\Delta_0^2} \quad \text{w.h.p.}$$

Note that informally, **A4** states that the local structure of $\mathbb{G}$ is asymptotically described by the branching processes $(\mathscr{T}_i)_{i\in[k]}$ with speed of convergence faster than $1/\Delta_0^2$. For most random graph models, it is rather easy to verify that (2.1), (2.2) and **A1**, **A2**, **A3** hold with the appropriate choice of parameters, and the main difficulty is to bound the speed of convergence of the local structure as required by **A4**.

2.3. **Choosing the parameters.** Given that the truth of the assumptions is fundamentally dependent on the choice of the parameters $\Delta_0, \zeta, \mathscr{Z}$, for which there may be many possibilities, let us briefly discuss how best to choose them.

The probability distribution vector $\mathscr{Z}$. First observe that given the graph model $\mathbb{G}$, due to **A4** there is only one sensible choice for the probability distribution vector $\mathscr{Z}$, namely the one which describes the local structure of $\mathbb{G}$ (in the sense of local weak convergence). For example, in the case of the Erdős-Rényi binomial random graph $G(n, d/n)$ for some constant d, we have $k = 1$ would choose $\mathscr{Z} = \mathscr{Z}_1 = \mathscr{Z}_{11}$ to be the $\mathrm{Po}(d)$ distribution. On the other hand, for the analogous balanced bipartite random graph $G(n, n, d/n)$ we would set $\mathscr{Z} = (\mathscr{Z}_1, \mathscr{Z}_2)$, where $\mathscr{Z}_1 = (\mathscr{Z}_{11}, \mathscr{Z}_{12}) = (0, \mathrm{Po}(d))$ and similarly for $\mathscr{Z}_2$.

The function ζ. This function only appears in the restriction, given by (2.2), that the tail bounds of the $\mathscr{Z}_i$ distributions decay super-exponentially fast. As such, we can simply set $\zeta(x) := \min_{i\in[k]} \frac{-\ln \mathbb{P}(\|\mathscr{Z}_i\|_1 > x)}{x}$ for all x. The assumption demands that this expression tends to infinity.

The degree bound Δ_0. The most critical property of Δ_0 is **A3**, which states that w.h.p. it is an upper bound on the maximum degree of $\mathbb{G}$. To make the task of proving **A4** easier, it is most convenient to choose Δ_0 as small as possible such that **A3** is satisfied. However, if in fact a bounded Δ_0 would suffice for this purpose (for example when considering random d-regular graphs), we would choose Δ_0 tending to infinity arbitrarily slowly in order to ensure that the lower bound in (2.1) is satisfied. In fact, the condition $\Delta_0 \gg 1$ in (2.1) is imposed purely for technical convenience later on, and (by choosing Δ_0 to grow arbitrarily slowly if necessary) does not actually impose any additional restrictions on the random model.

A typical non-regular scenario would be that we have $\Theta(n)$ vertices whose degrees are Poisson distributed with bounded expectation, in which case we could choose $\Delta_0 = \ln n$.

Assumption 2.10 actually contains a further hidden parameter which, for simplicity, we just chose to be $1/5$. More precisely, we have the following.

Remark 2.11. *In Assumption 2.10, the conditions **P1** and* (2.1) *can be replaced by the assumption that there exists some constant $0 < \beta < 1/3$ such that:*

(2.1)' $1 \ll \Delta_0 \ll n^{\beta/2}$;

(**A1**)' *For all $i \in [k]$, we have $\mathbb{E}(n_i) = \Theta(n)$, and $\mathrm{Var}(n_i) = o\left(n^{2(1-\beta)}\right)$.*

In Assumption 2.10 we arbitrarily chose $\beta = 1/5$ since the only additional restrictions this places on the model $\mathbb{G}$, once we account for being able to choose other parameters appropriately, are that w.h.p. $\Delta(\mathbb{G}) \ll n^{1/10}$ and $\mathrm{Var}(|V_i|) = o\left(n^{8/5}\right)$. It seems unlikely that there will be a natural model $\mathbb{G}$ for which this fails to hold, but for which it would be true for some different choice of β. Nevertheless, the proof would still go through in the more general case.

Let us make one further remark regarding **A2**, which states that any two graphs with the same type-degree sequence are asymptotically equally likely under $\mathbb{G}$. This condition is not satisfied for certain natural random graph models, for example random triangle-free graphs. However, a standard trick allows us to weaken the conditions a little such that this model would indeed be covered.

Remark 2.12. *Assumption 2.10 can be replaced by the following:*
There is a random graph model $\mathbb{G}^*$ and an event $\mathscr{E}$ such that

- $\mathbb{P}_{\mathbb{G}^*}(\mathscr{E}) = \Theta(1)$;
- $\mathbb{G} \sim \mathbb{G}^*|_{\mathscr{E}}$, *i.e.* $\mathbb{G}^*$ *conditioned on* $\mathscr{E}$ *is precisely* $\mathbb{G}$;
- $\mathbb{G}^*$ *satisfies Assumption 2.10.*

So for example when $\mathbb{G}$ is the random triangle-free graph, we would choose $\mathbb{G}^*$ to be the unconditioned random graph, and $\mathscr{E}$ to be the event that $\mathbb{G}^*$ is triangle-free. The reason the proof still goes through is that our results can be applied to $\mathbb{G}^*$ and give a high probability statement, which then also holds w.h.p. in the space conditioned on the $\Theta(1)$-probability event $\mathscr{E}$. We omit the details.

2.4. **Some simple consequences.** We next collect a few consequences of the assumptions that will be convenient later. Assumption 2.10 guarantees the existence of some parameters, but we will need to fix more for the proof. Specifically, we have the following.

Proposition 2.13. *If Assumption 2.10 holds, then there exists a function* $F : [0,\infty) \to [1,\infty)$ *and functions* $\omega_0 = \omega_0(n), c_0 = c_0(n), d_0 = d_0(n)$ *such that:*

F1 *F is monotonically increasing and invertible;*
F2 *For any sequences of real numbers $a = a(n)$ and $b = b(n)$, if $1 \le a \ll b$ then $F(a) \ll F(b)$;*
F3 *For any sequence of real numbers $a = a(n) \gg 1$ and for any constant $c > 0$ we have $F(a) \gg \exp(ca)$;*
F4 *There exists a sufficiently large $x_0 \ge 0$ such that for all $x > x_0$ and all $i \in [k]$, we have*

$$\mathbb{P}\left(\|\mathscr{Z}_i\|_1 > x\right) \le \frac{1}{F(x)}.$$

Moreover,

P1 $1 \ll \Delta_0^2 \ll \omega_0 \ll n^{1/5}$;
P2 $F^{-1}\left(\Delta_0^2\right) \ll d_0 \ll \ln\omega_0$;
P3 $\Delta_0 \exp(Cd_0), \Delta_0^2 \ll c_0 \ll F(d_0), \omega_0$ *for any constant* C,

and the random graph $\mathbb{G}$ satisfies the following.

B1 *For any $i \in [k]$ and $r \in \mathbb{N}_0$ we have*

$$d_{\mathrm{TV}}\left(\mathfrak{U}_i^r(\mathbb{G}), \mathscr{T}_i^r(\mathscr{Z})\right) \le \frac{1}{\omega_0} \quad \text{w.h.p.}$$

For the rest of the paper, we will fix parameters $\Delta_0, \omega_0, c_0, d_0$ and a function F as in Assumption 2.10 and Proposition 2.13. An obvious consequence of (**P3**) is that for any constant t_0,

$$\max\{d_0, \Delta_0\} \cdot |\Sigma|^{2(t_0+2)d_0} \le \Delta_0 \cdot |\Sigma|^{2(t_0+3)d_0} = o(c_0), \tag{2.3}$$

and this form will often be the most convenient in applications. Before proving Proposition 2.13, we prove an auxiliary claim which will be helpful both for this proof and later in the paper.

Claim 2.14. *If **P1**, **F1** and **F3** hold, then $F^{-1}\left(\Delta_0^2\right) \ll \ln\omega_0$.*

Proof. Suppose it is not true that $F^{-1}\left(\Delta_0^2\right) \ll \ln\omega_0$. Then (passing to a subsequence of necessary) there exists some constant $c > 0$ such that $F^{-1}\left(\Delta_0^2\right) \ge c\ln(\omega_0)$. Applying F to both sides, we deduce $\Delta_0^2 \ge F(c\ln(\omega_0))$, since F is monotonically increasing by **F1**. Moreover, by **F3** we have $F(c\ln(\omega_0)) \gg \omega_0$, so we conclude that $\Delta_0^2 \gg \omega_0$, which contradicts **P1**. □

In the proof of Proposition 2.13, for simplicity we will allow functions to take the values $\pm\infty$, and define expressions involving division by 0 or ∞ in the obvious way. This avoids annoying technical complications required to deal with some special cases—turning this into a formally correct proof would be an elementary exercise in analysis.

Proof of Proposition 2.13. First let us fix $F_1(x) := \min_{i\in[k]} \frac{1}{\mathbb{P}(\|\mathscr{Z}_i\|_1 > x)}$ and observe that $F_1(x) = \exp(\zeta_1(x)\cdot x)$ for some non-negative function $\zeta_1(x) \xrightarrow{x\to\infty} \infty$. This means that F_1 satisfies conditions **F3** and **F4**, but not necessarily conditions **F1** and **F2**. We therefore modify this function slightly. More precisely, we can modify the function ζ_1 to obtain ζ_2 satisfying:

- $\zeta_2(0) = 0$;
- $\zeta_2(x)$ is continuous and monotonically strictly increasing;

- $\zeta_2(x) \le \zeta_1(x)$ for all sufficiently large $x \in \mathbb{R}$;
- $\zeta_2(x) \xrightarrow{x\to\infty} \infty$.

We now set $F(x) := \exp(\zeta_2(x)\cdot x)$. It can be easily checked that F satisfies all the necessary conditions.

Now let us set $\omega_0 := \Delta_0^2 \cdot \omega$, where $\omega = \omega(n)$ is a function tending to infinity arbitrarily slowly. Since $1 \ll \Delta_0^2 \ll n^{1/5}$, if ω grows sufficiently slowly, **P1** is also satisfied. Similarly, since **A4** is satisfied, if ω grows sufficiently slowly, we also have **B1**.

We also set $d_0 := F^{-1}\left(\Delta_0^2\right)\cdot\omega$. Then the lower bound in **P2** is clearly satisfied. Furthermore Claim 2.14 shows that the upper bound also holds provided ω tends to infinity slowly enough.

Finally we will show that, provided ω grows slowly enough, $\Delta_0 \exp(Cd_0) \ll \Delta_0^2 \ll F(d_0), \omega_0$, and then picking $c_0 := \Delta_0^2 \cdot \omega$, we have that **P3** holds.

We first recall that $F(x) = \exp(\zeta_2(x)\cdot x)$, where $\zeta_2(x) \xrightarrow{x\to\infty} \infty$. Thus $F^{-1}(x) = \frac{\ln x}{\zeta_3(x)}$, where $\zeta_3(x) = \zeta_2\left(F^{-1}(x)\right) \xrightarrow{x\to\infty} \infty$. It follows that, for any constant $C > 0$, we have $\exp(Cd_0) = \exp\left(\frac{C(\ln\Delta_0)\omega}{\zeta_3(\Delta_0^2)}\right) \le \exp\left(\frac{(\ln\Delta_0)\omega}{\zeta_4(n)}\right)$ for sufficiently large n and for some appropriate function $\zeta_4(n) \xrightarrow{n\to\infty} \infty$ (which is independent of C). By choosing $\omega \ll \zeta_4$, we have $\exp(Cd_0) \ll \Delta_0$ and therefore also $\Delta_0\exp(Cd_0) \ll \Delta_0^2$. Now to complete the proof, observe that $d_0 \gg F^{-1}\left(\Delta_0^2\right)$ by definition, and therefore **F2** implies that $\Delta_0^2 \ll F(d_0)$. On the other hand, $\Delta_0^2 \ll \omega_0$ by definition of ω_0. □

A further consequence of the assumptions is that the degree distributions have bounded moments.

Remark 2.15. *Claim 2.14 and **F4** together imply that for all $i \in [k]$, the distribution $\|\mathcal{Z}_i\|_1$ of the total degree of a vertex of type i has finite moments, i.e. $\mathbb{E}\left(\|\mathcal{Z}_i\|_1^s\right)$ is finite for any $s \in \mathbb{N}$, and in particular for any $i, j \in [k]$ and $s \in \mathbb{N}$ the moment $\mathbb{E}\left(\mathcal{Z}_{ij}^s\right)$ are finite. It also follows that for every admissible pair $(i,j) \in \mathcal{K}$, the moments $\mathbb{E}\left(\left\|\mathcal{Y}_{j,i}\right\|_1^s\right)$ are finite (this can be verified with an elementary check). We will often use these facts during the proofs.*

We will also need the simple observation that the class sizes are reasonably concentrated around their expectations.

Claim 2.16. *W.h.p. for all $i \in [k]$ we have $n_i = \left(1 + o\left(\frac{1}{\omega_0}\right)\right)\mathbb{E}(n_i)$.*

Proof. By **A1**, for all $i \in [k]$, we have $\mathbb{E}(n_i) = \Theta(n)$ and $\mathrm{Var}(n_i) = o\left(n^{8/5}\right)$. Let $\omega = \omega(n) := \frac{n^{8/5}}{\max_{i\in[k]}\mathrm{Var}(n_i)}$, so in particular $\omega \to \infty$. (Note that if $\mathrm{Var}(n_i) = 0$ for all i, then the claim is trivial, so we may assume that ω is well-defined.) Then Chebyshev's inequality implies that

$$\mathbb{P}\left(\left|n_i - \mathbb{E}(n_i)\right| \ge n^{4/5}\right) \le \mathbb{P}\left(\left|n_i - \mathbb{E}(n_i)\right| \ge \sqrt{\omega\cdot\mathrm{Var}(n_i)}\right) \le \frac{1}{\omega} = o(1).$$

In other words, w.h.p. $n_i = \left(1 + O\left(\frac{1}{n^{1/5}}\right)\right)\mathbb{E}(n_i)$, and since $\omega_0 \ll n^{1/5}$ by **P1**, taking a union bound over all $i \in [k]$ gives the desired result. □

3. An alternative model

Although our main result is primarily a statement about $\mathbb{G}$, a key method in this paper is to switch focus away from this model to a second model, denoted $\hat{\mathbb{G}}$, which is easier to analyse. To introduce this second model, we need some more definitions.

3.1. **Message histories.** Let $\mathcal{G}_n$ denote the set of Σ-*messaged graphs* on vertex set $[n]$, i.e. graphs on $[n]$ in which each edge uv comes equipped with directed messages $\mu_{u\to v}, \mu_{v\to u} \in \Sigma$.

We will denote by $\mu_{u\to v}(t)$ the message from u to v after t iterations of WP, and refer to this as the *t-message* from u to v. Alternatively, we refer to the *t-in-message* at v or the *t-out-message* at u (this terminology will be especially helpful later when considering half-edges). In all cases, we may drop t from the notation if it is clear from the context.

In fact, we will need to keep track not just of the current Warning Propagation messages along each edge, but of the entire history of messages. For two adjacent vertices u, v, define the *t-history from u to v* to be the vector

$$\boldsymbol{\mu}_{u\to v}(\le t) := \left(\mu_{u\to v}(0), \dots, \mu_{u\to v}(t)\right) \in \Sigma^{t+1}.$$

We will also refer to $\boldsymbol{\mu}_{u\to v}(\le t)$ as the *t-in-story* at v, and as the *t-out-story* at u. The *t-story* at v consists of the pair $\left(\boldsymbol{\mu}_{u\to v}(\le t), \boldsymbol{\mu}_{v\to u}(\le t)\right)$, i.e. the t-in-story followed by the t-out-story. It will sometimes be more convenient to

consider the sequence consisting of the t-in-story followed by just the 0-out-message, which we call the *t-input*. In all cases, we may drop t from the notation if it is clear from the context.

We denote by $\mathscr{G}_n^{(t)}$ the set of Σ^{t+1}-messaged graphs on vertex set $[n]$ – the labels along each directed edge, which come from Σ^{t+1}, will be the t-histories. [3]

With a slight abuse of notation, for $t_1 < t_2$ we will identify two graphs $G \in \mathscr{G}_n^{(t_1)}$ and $H \in \mathscr{G}_n^{(t_2)}$, whose messages are given by $\mu^{(G)}$ and $\mu^{(H)}$ respectively, if

- $E(G) = E(H)$;
- $\mu^{(G)}_{u\to v}(t) = \mu^{(H)}_{u\to v}(t)$ for all $t \le t_1$;
- $\mu^{(H)}_{u\to v}(t) = \mu^{(H)}_{u\to v}(t_1)$ for all $t_1 < t \le t_2$.

In other words, the underlying graphs are identical, the t_1-histories are identical, and subsequently no messages change in H. In particular, this allows us to talk of *limits* of messaged graphs $G_t \in \mathscr{G}_n^{(t)}$ as $t \to \infty$.

Definition 3.1. *For any $t \in \mathbb{N}$ and probability distribution matrix Q_0 on Σ, let $\mathbb{G}_t = \mathbb{G}_t(n, Q_0) \in \mathscr{G}_n^{(t)}$ be the random Σ^{t+1}-messaged graph produced as follows.*

(1) Generate the random graph $\mathbb{G}$.
(2) Initialise each message $\mu_{u\to v}(0)$ for each directed edge (u,v) independently at random according to $Q_0[i,j]$ where i and j are the types of u and v respectively.
(3) Run Warning Propagation for t rounds according to update rule φ.
(4) Label each directed edge (u,v) with the story $\big(\mu_{u\to v}(0), \dots, \mu_{u\to v}(t)\big)$ up to time t.

We also define $\mathbb{G}_* := \lim_{t\to\infty} \mathbb{G}_t$, if this limit exists.

We aim to move away from looking at $\mathbb{G}_t$ and instead to consider a random graph model $\hat{\mathbb{G}}_t$ in which we first generate half-edges at every vertex, complete with stories in both directions, and only subsequently reveal which half-edges are joined to each other; thus we construct a graph in which the WP messages are known a priori. The trick is to do this in such a way that the resulting random messaged graph looks similar to $\mathbb{G}_t$.

In order to define this random model, we need a way of generating a history randomly, but accounting for the fact that the entries of a history are, in general, heavily dependent on each other, which we do in Definition 3.3. We first need to define a variant of the $\mathscr{T}_i$ branching trees.

An *edge-rooted graph* is a simple graph with a distinguished directed edge designated as root edge. When we have an edge-rooted *tree* rooted at the directed edge (u,v), we will think of v as the parent of u, and in all such situations v will have no other children. More generally, whenever we talk of messages along an edge of such a tree, we mean along the directed edge from child to parent.

We will also need to describe the part of the local structure that influences a message along a directed edge (u,v). This motivates the following definition.

Definition 3.2. *Let $\mathscr{Z}_1, \dots, \mathscr{Z}_k$ be probability distributions on $\mathbb{N}_0^k$ and for all $i,j \in [k]$, let $\mathscr{Y}_{j,i}$ be as in Definition 2.2. For each $(i,j) \in \mathscr{K}$, let $\mathscr{T}_{ij} := \mathscr{T}_{ij}(\mathscr{Z}_1, \dots, \mathscr{Z}_k)$ denote a k-type Galton-Waltson process defined as follows:*

(1) The process starts with a directed root edge (u,v) where u has type i and v has type j. We refer to v as the parent of u, and v will have no further children.
(2) Subsequently, starting at u, vertices are produced recursively according to the following rule: for every vertex w of type h with a parent w' of type ℓ, generate children of w with types according to $\mathscr{Y}_{\ell,h}$ independently.

Moreover, for $r \in \mathbb{N}_0$ we denote by $\mathscr{T}_{ij}^r$ the branching $\mathscr{T}_{ij}$ truncated at depth r.

Note that the process $\mathscr{T}_{ij}$ can equivalently be produced by taking the process $\mathscr{T}_i$ conditioned on the root u having at least one child v of type j, deleting the entire subtree induced by the descendants of v and rooting the resulting tree at the directed edge (u,v).

Definition 3.3. *Given a probability distribution matrix Q on Σ, for each $i,j \in [k]$ we define random variables $X_{ij}^{(0)}, X_{ij}^{(1)}, X_{ij}^{(2)}, \dots$ as follows. Let T_{ij} be a randomly generated instance of the process $\mathscr{T}_{ij}$ defined in Definition 3.2.*

(1) Initialise all messages in T_{ij} according to Q.
(2) For each $t \in \mathbb{N}_0$, let $X_{ij}^{(t)} := \mu_{u\to v}(t)$ be the message from u to v after t iterations of Warning Propagation according to the update rule φ where v is the root of T_{ij} and u its only child.

[3] Note that the definition of $\mathscr{G}_n^{(t)}$ makes no assumption that the histories along directed edges arise from running Warning Propagation – in principle, they could be entirely inconsistent – although of course in our applications, this will indeed be the case.

Finally, for each $t \in \mathbb{N}_0$, let $\boldsymbol{\phi}_{\varphi}^{t}(Q)$ be the probability distribution matrix R on Σ^{t+1} where each entry $R[i,j]$ is the distribution of $\left(X_{ij}^{(0)},\dots,X_{ij}^{(t)}\right)$. As in Definition 2.4, in order to ease notation, we sometimes denote $\boldsymbol{\phi}_{\varphi}^{t}(Q)$ by $Q^{(\leq t)}$.

Note that $Q^{(\leq t)}$ is *not* a vector $\left(Q^{(0)},\dots,Q^{(t)}\right)$ of probability distribution matrices, but is instead a matrix in which every entry is a probability distribution on vectors of length $t+1$.

Note also that while it is intuitively natural to expect that the marginal distribution of $Q^{(\leq t)}[i,j]$ on the ℓ-th entry has the distribution of $Q^{(\ell)}[i,j]$, which motivates the similarity of the notation, this fact is not completely trivial. We will therefore formally prove this in Claim 4.1.

3.2. **The random construction.** We define the *t-in-compilation* at a vertex v to be the multiset of t-inputs at v, and the *t-in-compilation sequence* is the sequence of t-in-compilations over all vertices of $[n]$. As before, we often drop the parameter t from the terminology when it is clear from the context.

We can now define the alternative random graph model to which we will switch our focus.

Definition 3.4. *Given a probability distribution matrix Q_0 on Σ, a sequence $\mathcal{Z} = (\mathcal{Z}_1,\dots,\mathcal{Z}_k)$ of probability distributions on $\mathbb{N}_0^k$, a probability distribution vector $\mathcal{N} = \mathcal{N}(n) \in \mathscr{P}\left(\mathbb{N}_0^k\right)$ and an integer t_0, we construct a random messaged graph $\hat{\mathbb{G}}_{t_0} = \hat{\mathbb{G}}_{t_0}(n,\mathcal{N},\mathcal{Z},Q_0)$ by applying the following steps.*

(1) Generate $n_1,\dots,n_k$ according to the probability distribution vector $\mathcal{N}$, and for each $i \in [k]$ generate a vertex set V_i with $|V_i| = n_i$.

(2) For each $i \in [k]$ and for each vertex v in V_i independently, generate an in-compilation by:

(a) Generating half edges with types (i,j) for each $j \in [k]$ according to $\mathcal{Z}_i$;

(b) Giving each half-edge of type (i,j) a t_0-in-story according to $Q_0^{(\leq t_0)}[j,i]$ independently;

(c) Giving each half-edge of type (i,j) a 0-out-message according to $Q_0[i,j]$ independently of each other and of the in-stories.

(3) Generate t-out-messages for each time $1 \leq t \leq t_0$ according to the rules of Warning Propagation based on the $(t-1)$-in-messages, i.e. if the t_0-in-stories at v, from dummy neighbours $u_1,\dots,u_j$, are $\boldsymbol{\mu}_{u_i\to v}(\leq t_0)$, we set

$$\mu_{v\to u_i}(t) = \varphi\left(\left\{\!\!\left\{\mu_{u_1\to v}(t-1),\dots,\mu_{u_{i-1}\to v}(t-1),\mu_{u_{i+1}\to v}(t-1),\dots,\mu_{u_j\to v}(t-1)\right\}\!\!\right\}\right).$$

(4) Consider the set of matchings of the half-edges which are maximum subject to the following conditions:

- *Consistency: a half-edge with in-story $\boldsymbol{\mu}_1 \in \Sigma^{t_0+1}$ and out-story $\boldsymbol{\mu}_2 \in \Sigma^{t_0+1}$ is matched to a half-edge with in-story $\boldsymbol{\mu}_2$ and out-story $\boldsymbol{\mu}_1$;*
- *Simplicity: the resulting graph (ignoring unmatched half-edges) is simple.*

Select a matching uniformly at random from this set and delete the remaining unmatched half-edges.

From now on we will always implicitly assume that the choice of various parameters is the natural one to compare $\hat{\mathbb{G}}_{t_0}$ with $\mathbb{G}_{t_0}$, i.e. that $\mathcal{N}$ is precisely the distribution of the class sizes of $\mathbb{G}$ and $\mathcal{Z}$ is the probability distribution vector which describes the local structure of $\mathbb{G}$ as required in Assumption 2.10, while Q_0 will be the probability distribution matrix according to which we initialise messages in $\mathbb{G}$.

We will show later (Claim 4.2) that the distribution of an out-story is identical to the distribution of an in-story, which means that the expected number of half-edges with story $(\boldsymbol{\mu}_1,\boldsymbol{\mu}_2)$ is (almost) identical to the expected number of half-edges with the dual story $(\boldsymbol{\mu}_2,\boldsymbol{\mu}_1)$. Heuristically, this suggests that almost all half-edges can be matched up and therefore few will be deleted in Step 4. This will be proved formally in Proposition 5.5.

Remark 3.5. *Note that Step 3 of the construction is an entirely deterministic one – the t-out-messages at time $t \geq 1$ are fixed by the incoming messages at earlier times. Therefore all in-stories and out-stories (before the deletion of half-edges) are in fact determined by the outcome of the random construction in Steps 1 and 2.*

3.3. **Contiguity.** Observe that $\hat{\mathbb{G}}_{t_0}$ and $\mathbb{G}_{t_0}$ both define random variables in $\mathscr{G}_n^{(t_0)}$. With a slight abuse of notation, we also use $\hat{\mathbb{G}}_{t_0}$ and $\mathbb{G}_{t_0}$ to denote the *distribution* of the respective random variables. Given a Σ^{t+1}-messaged graph $G \in \mathscr{G}_n^{(t)}$, we will denote by $\overline{G}$ the Σ-messaged graph in $\mathscr{G}_n$ obtained by removing all messages from each history except for the message at time t, i.e. the "current" message.

There are two main steps in the proof of Theorem 1.3:

(1) Show that $\hat{\mathbb{G}}_t$ and $\mathbb{G}_t$ have similar distributions for any constant $t \in \mathbb{N}$ (Lemma 3.7).

(2) Use this approximation to show that, for some large constant $t_0 \in \mathbb{N}$, the messaged graphs $\overline{\mathbb{G}}_{t_0}$ and $\overline{\mathbb{G}}_*$ are also very similar, i.e. very few further changes are made after t_0 steps of Warning Propagation.

In particular, we must certainly choose t_0 to be large enough that $\phi_\varphi^{t_0}(Q_0)$ is very close to the stable WP limit P of Q_0. It will follow that the distribution of a message along a randomly chosen directed edge in $\overline{\hat{\mathbb{G}}}_{t_0}$ (and therefore also in $\overline{\mathbb{G}}_{t_0}$) of type (i,j) is approximately $P[i,j]$ (see Claim 4.1).

We need a way of quantifying how "close" two messaged graphs are to each other. Given sets A and B, we use $A \Delta B := (A \setminus B) \cup (B \setminus A)$ to denote the symmetric difference.

Definition 3.6. *Given $t \in \mathbb{N}_0$, two Σ^{t+1}-messaged graphs $G_1, G_2 \in \mathscr{G}_n^{(t)}$ and $\delta > 0$, we say that $G_1 \sim_\delta G_2$ if:*

(1) $E(G_1) \Delta E(G_2) \le \delta n$;

(2) The messages on $E(G_1) \cap E(G_2)$ in the two graphs agree except on a set of size at most δn.

We further say that $G_1 \approx_\delta G_2$ if in fact the underlying graphs are identical (i.e. $E(G_1) \Delta E(G_2) = \emptyset$).

The crucial lemma that justifies our definition of the $\hat{\mathbb{G}}$ model is the following.

Lemma 3.7. *For any integer $t_0 \in \mathbb{N}$ and real number $\delta > 0$, the random Σ^{t_0+1}-messaged graphs $\hat{\mathbb{G}}_{t_0}, \mathbb{G}_{t_0}$ can be coupled in such a way that w.h.p. $\hat{\mathbb{G}}_{t_0} \sim_\delta \mathbb{G}_{t_0}$.*

This lemma is proved in Section 5.

3.4. **Message Terminology.** We have introduced several pieces of terminology related to messages in the graph, which we recall and collect here for easy reference. For a fixed time parameter $t \in \mathbb{N}$ and a directed edge, the *t-history* is the sequence of messages at times $0, 1, \dots, t$ along this directed edge. Further, for a (half-)edge or set of (half-)edges incident to a specified vertex, we have the following terminology.

- The *t-in-message* is the incoming message at time t.
- The *t-out-message* is the outgoing message at time t.
- The *t-in-story* is the sequence of t'-in-messages for $t' = 0, \dots, t$.
- The *t-out-story* is the sequence of t'-out-messages at times $t' = 0, \dots, t$.
- The *t-story* is the ordered pair consisting of the t-in-story and t-out-story.
- The *t-input* is the ordered pair consisting of the t-in-story and 0-out-message.
- The *t-in-compilation* is the multiset of t-inputs over all half-edges at a vertex.
- The *t-in-compilation sequence* is the sequence of t-in-compilations over all vertices.

When the parameter t is clear from the context, we often drop it from the terminology.

4. Preliminary results

We begin with some fairly simple observations which help to motivate some of the definitions made so far, or to justify why they are reasonable. The first such observation provides a slightly simpler way of describing the individual "entries", i.e. the marginal distributions, of the probability distribution $\boldsymbol{\phi}_\varphi^t(Q_0)[i,j] \in \mathscr{P}(\Sigma^{t+1})$.

Claim 4.1. *For any $t', t \in \mathbb{N}_0$ with $t' \le t$ and for any $i, j \in [k]$, the marginal distribution of $\boldsymbol{\phi}_\varphi^t(Q_0)[i,j]$ on the t'-th entry is precisely $\phi_\varphi^{t'}(Q_0)[i,j]$, i.e. for any $\mu \in \Sigma$ we have*

$$\mathbb{P}\left(\left(\boldsymbol{\phi}_\varphi^t(Q_0)[i,j]\right)[t'] = \mu\right) = \left(\sum_{\substack{\boldsymbol{\mu}=(\mu_0,\dots,\mu_t)\in\Sigma^{t+1}\\ \mu_{t'}=\mu}} \mathbb{P}\left(\boldsymbol{\phi}_\varphi^t(Q_0)[i,j] = \boldsymbol{\mu}\right)\right) = \mathbb{P}\left(\phi_\varphi^{t'}(Q_0)[i,j] = \mu\right).$$

Proof. Using the notation from Definition 3.3, we have

$$\sum_{\substack{\boldsymbol{\mu}=(\mu_0,\dots,\mu_t)\in\Sigma^{t+1}\\ \mu_{t'}=\mu}} \mathbb{P}\left(\boldsymbol{\phi}_\varphi^t(Q_0)[i,j] = \boldsymbol{\mu}\right) = \sum_{\substack{\boldsymbol{\mu}=(\mu_0,\dots,\mu_t)\in\Sigma^{t+1}\\ \mu_{t'}=\mu}} \mathbb{P}\left(X_{ij}^{(0)} = \mu_0, \dots, X_{ij}^{(t)} = \mu_t\right) = \mathbb{P}\left(X_{ij}^{(t')} = \mu\right).$$

We will prove by induction that $\mathbb{P}\left(X_{ij}^{(t')} = \mu\right) = \mathbb{P}\left(\phi_\varphi^{t'}(Q_0)[i,j] = \mu\right)$. For $t' = 0$, again using Definition 3.3 the distribution of $X_{ij}^{(0)}$ is simply $Q_0[i,j]$, so suppose that $t' \ge 1$, that the result holds for $0, \dots, t'-1$ and for any pair $(h,\ell) \in [k]^2$. Let $x_1, \dots, x_d$ be the children of the root node u in the $\mathscr{T}_{ij}$ branching tree defined in Definition 3.2 so the numbers and types of the children are given by the distribution $\mathscr{Y}_{j,i}$. By the recursive nature of the $\mathscr{T}_{ij}$

branching tree and the induction hypothesis, the message from any x_m of type h to u at time $t'-1$ has distribution $\phi_\varphi^{t'-1}(Q_0)[h,i]$ and this is independent for all vertices. Thus, in order to get the message from u to v at time t', we generate a multiset of messages $\mathscr{M}\left(\mathscr{Y}_{j,i}, \phi_\varphi^{t'-1}(Q_0)[i]\right)$ as in Definition 2.3 and apply the Warning Propagation rule φ. By Definition 2.4, the distribution of $\varphi\left(\mathscr{M}\left(\mathscr{Y}_{j,i}, \phi_\varphi^{t'-1}(Q_0)[i]\right)\right)$ is $\phi_\varphi\left(\phi_\varphi^{t'-1}(Q_0)\right)[i,j] = \phi_\varphi^{t'}(Q_0)[i,j]$. □

Claim 4.2. *Given a half-edge of type (i,j) at a vertex u of type i in the graph $\hat{\mathbb{G}}_{t_0}$* before *any half-edges are deleted, the distribution of its out-story is given by $\boldsymbol{\phi}_\varphi^{t_0}(Q_0)[i,j]$.*

We note also that *after* half-edges are deleted, this distribution will remain asymptotically the same, since w.h.p. only $o(n)$ half-edges will be deleted (see Proposition 5.5).

Proof. Given such a half-edge at u, let us add a dummy vertex v of type j to model the corresponding neighbour of u. Apart from (u,v), the vertex u has some number d of half-edges with types connected to dummy vertices $c_1,\dots,c_d$ generated according to $\mathscr{Y}_{j,i}$. For each $d' \in [d]$, let $r_{d'}$ be the type of the vertex $c_{d'}$. Each half-edge $(c_{d'},u)$ receives t_0-in-story according to $\boldsymbol{\phi}_\varphi^{t_0}(Q_0)[r'_d, i]$. This is equivalent to endowing each $c_{d'}$ with a $\mathscr{T}_{r_{d'}i}$ tree independently where the root edge is $(c_{d'},u)$, initialising the messages from children to parents in these trees according to Q_0 and running t_0 rounds of Warning Propagation. Combining all these (now unrooted) trees with the additional root edge (u,v), whose message is also initialised according to Q_0 independently of all other messages, we have a $\mathscr{T}_{ij}$ tree in which all messages are initialised independently according to Q_0. Then by Definition 3.3, $\boldsymbol{\mu}_{u\to v}(\leq t_0)$ is distributed as $\boldsymbol{\phi}_\varphi^{t_0}(Q_0)[i,j]$. □

Recall that for each $\mu \in \Sigma$, its source and target types are encoded in it. We define a function to denote these types.

Definition 4.3. *For a message $\mu \in \Sigma$ with source type i and target type j, we define*

$$g(\mu) = (i,j), \qquad g_1(\mu) = i, \qquad g_2(\mu) = j, \qquad \bar{g}(\mu) = (j,i). \tag{4.1}$$

Recall that not all messages can appear along any edge, and for the same reason not all vectors of messages are possible as message histories, which motivates the following definition.

Definition 4.4. *We say that a vector $\boldsymbol{\mu} = (\mu_0, \mu_1, \dots, \mu_t) \in \Sigma^{t+1}$ is* consistent *if the $g(\mu_{t'})$ are all equal for all $0 \leq t' \leq t$, in other words, the source types of the $\mu_{t'}$ are equal and the target types of the $\mu_{t'}$ are equal. Let $\mathscr{C}_t \subseteq \Sigma^{t+1}$ be the set of consistent vectors in Σ^{t+1}. For $\boldsymbol{\mu} \in \mathscr{C}_t$ we slightly abuse the notation and define*

$$g(\boldsymbol{\mu}) = g(\mu_0), \qquad g_1(\boldsymbol{\mu}) = g_1(\mu_0), \qquad g_2(\boldsymbol{\mu}) = g_2(\mu_0), \qquad \bar{g}(\boldsymbol{\mu}) = \bar{g}(\mu_0).$$

Furthermore, we say that $\boldsymbol{\mu}_1, \boldsymbol{\mu}_2 \in \mathscr{C}_t$ are compatible *if $g(\boldsymbol{\mu}_1) = \bar{g}(\boldsymbol{\mu}_2)$, i.e. the source type of $\boldsymbol{\mu}_1$ is the target type of $\boldsymbol{\mu}_2$ and vice versa. Let $\mathscr{D}_t \subseteq \mathscr{C}_t^2$ be the set of directed pairs of compatible vectors.*

Note that even with this definition, not all consistent vectors are necessarily possible as message histories, since for example there may be some monotonicity conditions which the vector fails to satisfy.

Definition 4.5. *Let Q be a probability distribution matrix on Σ, let $\sigma \in \Sigma$ and $\boldsymbol{\mu} \in \mathscr{C}_t$ for some $t \in \mathbb{N}$. We define*

$$\mathbb{P}_{Q^{(t)}}(\sigma) := \mathbb{P}\left(Q^{(t)}[g(\sigma)] = \sigma\right) \text{ and } \mathbb{P}_{Q^{(\leq t)}}(\boldsymbol{\mu}) := \mathbb{P}\left(Q^{(\leq t)}[g(\boldsymbol{\mu})] = \boldsymbol{\mu}\right).$$

In other words, $\mathbb{P}_{Q^{(t)}}(\sigma)$ and $\mathbb{P}_{Q^{(\leq t)}}(\boldsymbol{\mu})$ are the probabilities of obtaining σ and $\boldsymbol{\mu}$ if we sample from $Q^{(t)}$ and $Q^{(\leq t)}$ in the appropriate entry $g(\sigma)$ and $g(\boldsymbol{\mu})$ of those matrices respectively, the only entries which could conceivably give a non-zero probability.

Given an integer t and $\boldsymbol{\mu}_1, \boldsymbol{\mu}_2 \in \Sigma^{t+1}$, let $m_{\boldsymbol{\mu}_1,\boldsymbol{\mu}_2}$ denote the number of half-edges in $\hat{\mathbb{G}}_t$ with story $(\boldsymbol{\mu}_1, \boldsymbol{\mu}_2)$, i.e. with in-story $\boldsymbol{\mu}_1$ and out-story $\boldsymbol{\mu}_2$, after Step 3 of the random construction (in particular *before* unmatched half-edges are deleted). Observe that at a single half-edge of type $(i,j) := (g_1(\boldsymbol{\mu}_1), g_2(\boldsymbol{\mu}_1))$, the in-story is distributed as $Q_0^{(\leq t)}[j,i]$ and by Claim 4.2 the out-story is distributed as $Q_0^{(\leq t)}[i,j]$. Moreover, the in-story and out-story are independent of each other. Therefore the probability that the half-edge has in-story $\boldsymbol{\mu}_1$ and out-story $\boldsymbol{\mu}_2$ is precisely

$$q_{\boldsymbol{\mu}_1,\boldsymbol{\mu}_2} := \begin{cases} \mathbb{P}_{Q_0^{(\leq t)}}(\boldsymbol{\mu}_1) \cdot \mathbb{P}_{Q_0^{(\leq t)}}(\boldsymbol{\mu}_2) & \text{if } (\boldsymbol{\mu}_1, \boldsymbol{\mu}_2) \in \mathscr{D}_t, \\ 0 & \text{otherwise.} \end{cases}$$

The following fact follows directly from the definition of $q_{\boldsymbol{\mu}_1,\boldsymbol{\mu}_2}$.

Fact 4.6. *For any* $(\boldsymbol{\mu}_1, \boldsymbol{\mu}_2) \in \Sigma^{t+1}$ *we have* $q_{\boldsymbol{\mu}_1,\boldsymbol{\mu}_2} = q_{\boldsymbol{\mu}_2,\boldsymbol{\mu}_1}$.

We will also define

$$\overline{m}_{\boldsymbol{\mu}_1,\boldsymbol{\mu}_2} := \begin{cases} \mathbb{E}\left(\mathscr{Z}_{g(\boldsymbol{\mu}_1)}\right)\mathbb{E}\left(n_{g_1(\boldsymbol{\mu}_1)}\right) q_{\boldsymbol{\mu}_1,\boldsymbol{\mu}_2} & \text{if } (\boldsymbol{\mu}_1,\boldsymbol{\mu}_2) \in \mathscr{D}_t, \\ 0 & \text{otherwise.} \end{cases} \tag{4.2}$$

Claim 4.7. *For any* $i, j \in [k]$, *we have* $\mathbb{E}(\mathscr{Z}_{ij})\mathbb{E}(n_i) = \left(1 + O\left(\frac{\Delta_0}{\omega_0}\right)\right)\mathbb{E}(\mathscr{Z}_{ji})\mathbb{E}(n_j)$. *In particular,*

$$\overline{m}_{\boldsymbol{\mu}_1,\boldsymbol{\mu}_2} = \left(1 + O\left(\frac{\Delta_0}{\omega_0}\right)\right)\overline{m}_{\boldsymbol{\mu}_2,\boldsymbol{\mu}_1}.$$

Proof. Let us fix $i, j \in [k]$. The statement is trivial if $i = j$, and therefore we may assume that this is not the case. Let us consider the number of edges of $e_{i,j}, e_{j,i}$ of types (i,j) and (j,i) respectively in $\mathbb{G}$, which must of course be identical. This can be expressed as $\sum_{v \in V_i} d_{\mathbb{G},j}(v)$, where $d_{\mathbb{G},j}(v)$ denotes the number of neighbours of v which have type j.

Now for each $d \in \mathbb{N}$, define $\mathscr{S}_d$ to be the family of (vertex-)rooted k-type graphs of depth 1 rooted at a vertex of type i, and with exactly d vertices of type j. Then we have

$$e_{i,j} = \sum_{v \in V_i} d_{\mathbb{G},j}(v) = \sum_{v \in V_i}\sum_{d \in \mathbb{N}} d \cdot \mathbf{1}\left\{d_{\mathbb{G},j}(v) = d\right\} = \sum_{v \in V_i}\sum_{d \in \mathbb{N}}\sum_{H \in \mathscr{S}_d} d \cdot \mathbf{1}\left\{B_{\mathbb{G}}(v,1) \cong H\right\}.$$

Now conditioning on the high probability event that $n_i = \left(1 + o\left(\frac{1}{\omega_0}\right)\right)\mathbb{E}(n_i)$ (see Claim 2.16) and that there are no vertices of degree larger than Δ_0 (see **A3**), we have w.h.p.

$$e_{i,j} = n_i \cdot \left(\sum_{d \le \Delta_0} d \sum_{H \in \mathscr{S}_d} \mathbb{P}(\mathscr{T}_i \cong H) \pm \Delta_0 \cdot d_{\mathrm{TV}}\left(\mathfrak{U}^{\mathbb{G}}_{i,1}, \mathscr{T}_i\right)\right) = n_i\left(\sum_{d \le \Delta_0} d\mathbb{P}(\mathscr{Z}_{ij} = d) + O\left(\frac{\Delta_0}{\omega_0}\right)\right) = \mathbb{E}(n_i)\left(\mathbb{E}(\mathscr{Z}_{ij}) + O\left(\frac{\Delta_0}{\omega_0}\right)\right).$$

By symmetry we also have $e_{i,j} = e_{j,i} = \mathbb{E}(n_j)\left(\mathbb{E}(\mathscr{Z}_{ji}) + O\left(\frac{\Delta_0}{\omega_0}\right)\right)$. It easily follows that $\mathbb{E}(\mathscr{Z}_{ij}) = 0 \Leftrightarrow \mathbb{E}(\mathscr{Z}_{ji}) = 0$, in which case the statement follows trivially. On the other hand, if these expectations are non-zero, then we have $\mathbb{E}(\mathscr{Z}_{ij}) + O\left(\frac{\Delta_0}{\omega_0}\right) = \left(1 + O\left(\frac{\Delta_0}{\omega_0}\right)\right)\mathbb{E}(\mathscr{Z}_{ij})$, and similarly for $\mathbb{E}(\mathscr{Z}_{ji})$, so the result follows by rearranging. □

5. Contiguity: Proof of Lemma 3.7

The aim of this section is to prove Lemma 3.7, the first of our two main steps, which states that $\hat{\mathbb{G}}_{t_0}$ and $\mathbb{G}_{t_0}$ have approximately the same distribution. We begin with an overview.

5.1. Proof strategy.

The overall strategy for the proof is to show that every step of the construction of $\hat{\mathbb{G}}_{t_0}$ closely reflects the situation in $\mathbb{G}_{t_0}$. More precisely, the following are the critical steps in the proof. Recall from Definition 3.1 that $\mathbb{G}$ is the underlying *unmessaged* random graph corresponding to $\mathbb{G}_{t_0}$, and similarly let $\hat{\mathbb{G}}$ denote the underlying unmessaged random graph corresponding to $\hat{\mathbb{G}}_{t_0}$. The following either follow directly from our assumptions or will be shown during the proof.

(1) The vectors representing the numbers of vertices of each type in $\hat{\mathbb{G}}_{t_0}$ and $\mathbb{G}_{t_0}$ are identically distributed.
(2) The local structure of $\mathbb{G}$ is described by the $\mathscr{T}_i$ branching processes for $i \in [k]$.
(3) After initialising Warning Propagation on $\mathbb{G}$ according to Q_0 and proceeding for t_0 rounds, the distribution of the in-story along a random edge of type (i,j) is approximately $\boldsymbol{\phi}^{t_0}_{\varphi}(Q_0)[j,i]$.
(4) Given a particular compilation sequence, i.e. multiset of stories (which consist of in-stories and out-stories) on half-edges at each vertex, each graph with this compilation sequence is almost equally likely to be chosen as $\mathbb{G}$.
(5) If we run Warning Propagation on $\hat{\mathbb{G}}$, with initialisation identical to the constructed 0-messages in $\hat{\mathbb{G}}_{t_0}$, for t_0 steps, w.h.p. the message histories are identical to those generated in the construction of $\hat{\mathbb{G}}_{t_0}$ except on a set of $o(n)$ edges.

The first step is trivially true since we chose the vector $\mathscr{N}$ to be the distribution of the class sizes in $\mathbb{G}$. The second step is simply **B1**, and the third step is a direct consequence of the second (see Proposition 5.6). One minor difficulty to overcome in this step is how to handle the presence of short cycles, which are the main reason the approximations are not exact. However, since the local structure is a tree by **B1**, w.h.p. there are few vertices which lie close to a short cycle (see Claim 5.3).

We will need to show that, while the presence of such a cycle close to a vertex may alter the distribution of incoming message histories at this vertex (in particular they may no longer be independent), it does not fundamentally alter which message histories are *possible* (Proposition 5.1). Therefore while the presence of a short cycle will change some distributions in its close vicinity, the fact that there are very few short cycles means that this perturbation will be masked by the overall random "noise".

The fourth step is precisely **A2**, while the fifth step is almost an elementary consequence of the fact that we constructed the message histories in $\hat{\mathbb{G}}_{t_0}$ to be consistent with Warning Propagation (Proposition 5.10). In fact, it would be obviously true that *all* message histories are identical were it not for the fact that some half-edges may be left unmatched in the construction of $\hat{\mathbb{G}}$ and therefore deleted, which can cause the out-messages along other half-edges at this vertex to be incorrect. This can then have a knock-on effect, but it turns out (see Proposition 5.5) that w.h.p. not too many edges are affected.

5.2. **Plausibility of inputs.** We begin by showing that, if we initialise messages in a (deterministic) graph in a way which is admissible according to Q_0, any t_0-input at a half-edge of type (i,j) produced by Warning Propagation has a non-zero probability of appearing under the probability distribution $\boldsymbol{\phi}_{\varphi}^{t_0}(Q_0)[j,i]$.

Proposition 5.1. *Let G be any k-type graph in which the type-degree of each vertex of type i has positive probability under $\mathcal{Z}_i$ and let (u,v) be a directed edge of G of type (i,j). Suppose that messages are initialised in G arbitrarily subject to the condition that each initial message is consistent with the vertex types and has non-zero probability under Q_0, i.e. for every directed edge (u',v') of type (i',j'), the initial message $\sigma \in \Sigma$ from u' to v' satisfies $g(\sigma) = (i',j')$ and furthermore $\mathbb{P}_{Q_0}(\sigma) \neq 0$. Run Warning Propagation with update rule φ for t_0 steps and let $\boldsymbol{\mu}_{\mathrm{in}} := \boldsymbol{\mu}_{u\to v}(\leq t_0)$ and $\mu_{\mathrm{out}} := \mu_{v\to u}(0)$ be the resulting t_0-in-story and 0-out-story at v along (u,v) respectively.*

Then

$$\mathbb{P}\Big(\Big(\boldsymbol{\phi}_{\varphi}^{t_0}(Q_0)[i,j], Q_0[j,i]\Big) = \big(\boldsymbol{\mu}_{\mathrm{in}}, \mu_{\mathrm{out}}\big)\Big) \neq 0.$$

Proof. We construct an auxiliary tree G', in which each vertex has a corresponding vertex in G. For a vertex w' in G', the corresponding vertex in G will be denoted by w. We construct G' as follows. First generate u' as the root of the tree, along with its parent v'. Subsequently, recursively for each $t \in \{0\} \cup [t_0 - 1]$, for each vertex x' at distance t below u' with parent y', we generate children for all neighbours of the vertex x in G except for y.

Note that another way of viewing G' is that we replace walks beginning at u in G (and whose second vertex is *not* v) by paths, where two paths coincide for as long as the corresponding walks are identical, and are subsequently disjoint. A third point of view is to see G' as a forgetful search tree of G, where (apart from the parent) we don't remember having seen vertices before and therefore keep generating new children.

We will initialise messages in G' from each vertex to its parent (and also from v to u) according to the corresponding initialisation in G, and run Warning Propagation with update rule φ for t_0 rounds.

Let $\boldsymbol{\mu}'_{\mathrm{in}} = \boldsymbol{\mu}'_{u'\to v'}(\leq t_0)$ be the resulting t_0-in-story and $\mu'_{\mathrm{out}} = \mu'_{v'\to u'}(0)$ be the 0-out-story at v' along (u',v') in G'. Recall that $\boldsymbol{\mu}_{\mathrm{in}}$ and μ_{out} are the corresponding t_0-in-story and 0-out-story at v in G . The crucial observation is the following.

Claim 5.2. $\boldsymbol{\mu}'_{\mathrm{in}} = \boldsymbol{\mu}_{\mathrm{in}}$ *and* $\mu'_{\mathrm{out}} = \mu_{\mathrm{out}}$.

We delay the proof of this claim until after the proof of Proposition 5.1, which we now complete. Since each initial message has non-zero probability under Q_0, we have $\mathbb{P}_{Q_0}(\mu_{\mathrm{out}}) \neq 0$. Recall that $\boldsymbol{\phi}_{\varphi}^{t_0}(Q_0)[i,j]$ was defined as the probability distribution of $\left(X_{ij}^{(0)}, \ldots, X_{ij}^{(t_0)}\right)$, the message history in a $\mathcal{T}_{ij}$ tree in which messages are initialised according to Q_0. Therefore the probability that $\boldsymbol{\phi}_{\varphi}^{t_0}(Q_0)[i,j] = \boldsymbol{\mu}_{\mathrm{in}} = \boldsymbol{\mu}'_{\mathrm{in}}$ is certainly at least the probability that a $\mathcal{T}_{ij}^{t_0}$ tree has exactly the structure of G' (up to depth t_0) and that the initialisation chosen at random according to Q_0 is precisely the same as the initialisation in G'. Since G' is a finite graph whose type-degrees for all vertices not at distance t_0 from u has positive probability under $\mathcal{Z}$, there is a positive probability that a random instance of $\mathcal{T}_{ij}^{t_0}$ is isomorphic to G'. Furthermore, since each initial message has a positive probability under Q_0, the probability of choosing the same initialisation as in G' is also nonzero, as required. □

We now go on to prove the auxiliary claim.

Proof of Claim 5.2. By construction the 0-out-message at v' along (v',u') is identical to the corresponding 0-out-message in G so $\mu'_{\text{out}} = \mu_{\text{out}}$. It remains to prove that the t_0-in-stories are identical.

For any vertex $x' \in G' \setminus \{v'\}$, let x'_+ denote the parent of x'. In order to prove Claim 5.2, we will prove a much stronger statement from which the initial claim will follow easily. More precisely, we will prove by induction on t that for all $x' \in G' \setminus \{v'\}$, $\boldsymbol{\mu}'_{x'\to x'_+}(\le t) = \boldsymbol{\mu}_{x\to x_+}(\le t)$. For $t = 0$, by construction $\mu'_{x'\to x'_+}(0) = \mu_{x\to x_+}(0)$ for any $x' \in G' \setminus \{v'\}$ because messages in G' are initialised according to the corresponding initialisation in G. Suppose that the statement is true for some $t \le t_0 - 1$. It remains to prove that $\mu'_{x'\to x'_+}(t+1) = \mu_{x\to x_+}(t+1)$. By the induction hypothesis, $\mu'_{y'\to x'}(t) = \mu_{y\to x}(t)$ for all $y' \in \partial_{G'} x' \setminus \{x'_+\}$. Hence,

$$\left\{\left\{\mu'_{y'\to x'}(t) : y' \in \partial_{G'} x' \setminus \{x'_+\}\right\}\right\} = \left\{\left\{\mu_{y\to x}(t) : y' \in \partial_{G'} x' \setminus \{x'_+\}\right\}\right\} = \left\{\left\{\mu_{z\to x}(t) : z \in \partial_G x \setminus \{x_+\}\right\}\right\},$$

i.e. the multisets of incoming messages to the directed edge (x', x'_+) in G' and to the directed edge (x, x_+) in G at time t are identical. Therefore also

$$\mu'_{x'\to x'_+}(t+1) = \varphi\left(\left\{\left\{\mu_{y'\to x'}(t) : y' \in \partial_G x' \setminus \{x'_+\}\right\}\right\}\right) = \varphi\left(\left\{\left\{\mu_{z\to x}(t) : z \in \partial_G x \setminus \{x_+\}\right\}\right\}\right) = \mu_{x\to x_+}(t+1),$$

as required. □

Proposition 5.1 tells us that no matter how strange or pathological a messaged graph looks locally, there is still a positive probability that we will capture the resulting input (and therefore w.h.p. such an input will be generated a linear number of times in $\hat{\mathbb{G}}_{t_0}$). In particular, within distance t_0 of a short cycle the distribution of an input may be significantly different from $\left(\boldsymbol{\phi}_\varphi^{t_0}(Q_0)[i,j], Q_0[j,i]\right)$. However, we next show that there are unlikely to be many edges this close to a short cycle.

Claim 5.3. *Let W_0 be the set of vertices which lie on some cycle of length at most t_0 in $\mathbb{G}$, and recursively define $W_t := W_{t-1} \cup \partial W_{t-1}$ for $t \in \mathbb{N}$.*

Then w.h.p. $|W_{t_0}| = O\left(\frac{n}{\omega_0}\right)$.

Proof. Any vertex which lies in W_{t_0} certainly has the property that its neighbourhood to depth $2t_0$ contains a cycle. However, since for any $i \in [k]$, the branching process $\mathcal{T}_i^{2t_0}$ certainly does *not* contain a cycle, Assumption **B1** (together with the fact that w.h.p. there are $O(n)$ vertices in total due to **A1**) shows that w.h.p. at most $O(n/\omega_0)$ vertices have such a cycle in their depth $2t_0$ neighbourhoods. □

5.3. **The deleted half-edges.** In the construction of $\hat{\mathbb{G}}$ we deleted some half-edges which remained unmatched in Step 4, and it is vital to know that there are not very many such half-edges. We therefore define E_0 to be the set of half-edges which are deleted in Step 4 of the random construction of $\hat{\mathbb{G}}$.

Definition 5.4. *Given integers $d, t \in \mathbb{N}_0$, a messaged graph $G \in \mathscr{G}_n^{(t_0)}$ and a multiset $A \in \left(\!\!\binom{\Sigma^{t+2}}{d}\!\!\right)$, define $n_A = n_A(G)$ to be the number of vertices of G which receive in-compilation A.*

Further, let $\gamma_A^i = \gamma_A^i(t)$ denote the probability that the t-in-compilation at a vertex of type i when generating $\hat{\mathbb{G}}_t$ is A.

Observe that for any $d, t \in \mathbb{N}_0$, the expression $\sum_{A\in\left(\!\!\binom{\Sigma^{t+2}}{d}\!\!\right)} n_A(G)$ is simply the number of vertices of degree d, and therefore for any $t \in \mathbb{N}_0$ we have $\sum_{d\in\mathbb{N}_0}\sum_{A\in\left(\!\!\binom{\Sigma^{t+2}}{d}\!\!\right)} n_A(G) = |V(G)|$.

Recall that in Proposition 2.13, apart from the function F and the parameter ω_0, we also fixed parameters c_0, d_0, which we will now make use of.

Proposition 5.5. *W.h.p. $|E_0| = o\left(\frac{n}{\sqrt{c_0}}\right)$.*

Proof. Let us fix two t_0-in-stories $\boldsymbol{\mu}_1, \boldsymbol{\mu}_2 \in \Sigma^{t_0+1}$ and consider the number of half-edges $m_{\boldsymbol{\mu}_1,\boldsymbol{\mu}_2}$ with t_0-in-story $\boldsymbol{\mu}_1$ and t_0-out-story $\boldsymbol{\mu}_2$. We aim to show that $m_{\boldsymbol{\mu}_1,\boldsymbol{\mu}_2}$ is concentrated around its expectation $\overline{m}_{\boldsymbol{\mu}_1,\boldsymbol{\mu}_2}$ as defined in (4.2). Recall that the multiset of t_0-stories at a vertex is determined by the t_0-in-compilation, i.e. the multiset of t_0-inputs. For each $d_1, d_2 \in \mathbb{N}$, let $B_{d_1,d_2} = B_{d_1,d_2}(\boldsymbol{\mu}_1,\boldsymbol{\mu}_2)$ denote the set of t_0-in-compilations $A \in \left(\!\!\binom{\Sigma^{t_0+2}}{d_2}\!\!\right)$ consisting of d_2 many t_0-inputs which lead to d_1 half-edges with t_0-story $(\boldsymbol{\mu}_1,\boldsymbol{\mu}_2)$, and let x_A denote the number of vertices which

receive t_0-in-compilation A in Step 3 of the construction of $\hat{\mathbb{G}}_{t_0}$ (in particular *before* the deletion of half-edges). Then we have

$$m_{\boldsymbol{\mu}_1,\boldsymbol{\mu}_2} = \sum_{d_1,d_2\in\mathbb{N}} \sum_{A\in B_{d_1,d_2}} d_1 x_A$$

We split the sum into two cases, depending on d_2. Consider first the case when $d_2 > d_0$. By **A1** w.h.p. the total number of vertices is $\Theta(n)$, and by **F4** the probability that any vertex has degree larger than d_0 is at most $1/F(d_0)$, and it follows that w.h.p. the number of half-edges attached to vertices of degree larger than d_2 is dominated by $d_2 \cdot \mathrm{Bin}\left(\Theta(n), \frac{1}{F(d_2)}\right)$. Thus the expected number of half-edges attached to such high degree vertices is at most

$$\Theta(1) \sum_{d_2\geq d_0} \frac{d_2 n}{F(d_2)} = \Theta(1)\frac{d_0 n}{F(d_0)},$$

Now by (**P3**) we have $F(d_0) \gg c_0$ and also $d_0 \leq \sqrt{\exp(d_0)} \ll \sqrt{c_0}$, and therefore $\frac{d_0 n}{F(d_0)} = o\left(\frac{n}{\sqrt{c_0}}\right)$. An application of Markov's inequality shows that w.h.p. the number of half-edges attached to vertices of degree at least d_0 is $o\left(\frac{n}{\sqrt{c_0}}\right)$.

We now turn our attention to the case $d_2 \leq d_0$. Here we observe that for any A each vertex of V_i is given t_0-in-compilation A with probability γ_A^i independently, and so the number of vertices which receive A is distributed as

$$X := \sum_{i=1}^{k} X_i = \sum_{i=1}^{k} \mathrm{Bin}\left(n_i, \gamma_A^i\right).$$

Conditioning on the high probability event that $n_i = \left(1 + o\left(\frac{1}{\omega_0}\right)\right)\mathbb{E}(n_i)$ (see Claim 2.16), and in particular is $\Theta(n)$, a standard Chernoff bound shows that with probability at least $1 - \exp\left(-\Theta\left((\ln n)^2\right)\right)$ the random variable X is within an additive factor $\sqrt{n}\ln n$ of its expectation, and a union bound over all at most $|\Sigma|^{(t_0+1)d_0} \overset{(2.3)}{=} o(c_0) \ll n^{1/5}$ choices for A of size at most d_0 shows that w.h.p. this holds for all such A simultaneously.

It follows that w.h.p.

$$\begin{aligned}\left|m_{\boldsymbol{\mu}_1,\boldsymbol{\mu}_2} - \overline{m}_{\boldsymbol{\mu}_1,\boldsymbol{\mu}_2}\right| &\leq \left|m_{\boldsymbol{\mu}_1,\boldsymbol{\mu}_2} - \mathbb{E}\left(\mathcal{Z}_{g(\boldsymbol{\mu}_1)}\right) q_{\boldsymbol{\mu}_1,\boldsymbol{\mu}_2} n_{g_1(\boldsymbol{\mu}_1)}\right| + \left|\mathbb{E}\left(\mathcal{Z}_{g(\boldsymbol{\mu}_1)}\right) q_{\boldsymbol{\mu}_1,\boldsymbol{\mu}_2} n_{g_1(\boldsymbol{\mu}_1)} - \overline{m}_{\boldsymbol{\mu}_1,\boldsymbol{\mu}_2}\right| \\ &\leq |\Sigma|^{(t_0+1)d_0}\sqrt{n}\ln n + o\left(\frac{n}{\sqrt{c_0}}\right) + o\left(\frac{n}{\omega_0}\right) = o\left(\frac{n}{\sqrt{c_0}}\right), \end{aligned} \tag{5.1}$$

To see the last estimate, note that by (2.3) we have $|\Sigma|^{(t_0+1)d_0}\sqrt{n}\ln n \ll c_0\sqrt{n}\ln n = o\left(n/\sqrt{c_0}\right)$, where second estimate follows since $c_0 \ll \omega_0 \ll n^{1/5}$ by **P1** and **P3**. This last fact also implies that $\sqrt{c_0} \ll c_0 \ll \omega_0$.

Since this is true for any arbitrary t_0-stories $\boldsymbol{\mu}_1, \boldsymbol{\mu}_2$, we can deduce that w.h.p.

$$\left|m_{\boldsymbol{\mu}_1,\boldsymbol{\mu}_2} - m_{\boldsymbol{\mu}_2,\boldsymbol{\mu}_1}\right| = \left|\overline{m}_{\boldsymbol{\mu}_1,\boldsymbol{\mu}_2} - \overline{m}_{\boldsymbol{\mu}_2,\boldsymbol{\mu}_1}\right| + o\left(\frac{n}{\sqrt{c_0}}\right).$$

Moreover, by Claim 4.7 we have $\left|\overline{m}_{\boldsymbol{\mu}_1,\boldsymbol{\mu}_2} - \overline{m}_{\boldsymbol{\mu}_2,\boldsymbol{\mu}_1}\right| = O\left(\frac{n\Delta_0}{\omega_0}\right) \overset{\mathbf{P3}}{=} o\left(\frac{n}{\sqrt{c_0}}\right)$. Hence $\left|m_{\boldsymbol{\mu}_1,\boldsymbol{\mu}_2} - m_{\boldsymbol{\mu}_2,\boldsymbol{\mu}_1}\right| = o\left(\frac{n}{\sqrt{c_0}}\right)$, and a union bound over all of the at most $|\Sigma|^{2(t_0+1)} = O(1)$ choices for $\boldsymbol{\mu}_1, \boldsymbol{\mu}_2$ implies that w.h.p. the same is true for *all* choices of $\boldsymbol{\mu}_1, \boldsymbol{\mu}_2$ simultaneously.

Finally, we observe that (deterministically) the number $|E_0|$ of half-edges left unmatched is

$$|E_0| = \sum_{\boldsymbol{\mu}_1\neq\boldsymbol{\mu}_2} \frac{1}{2}\left|m_{\boldsymbol{\mu}_1,\boldsymbol{\mu}_2} - m_{\boldsymbol{\mu}_2,\boldsymbol{\mu}_1}\right| + \sum_{\boldsymbol{\mu}_1} \mathbf{1}\left\{m_{\boldsymbol{\mu}_1,\boldsymbol{\mu}_1} \notin 2\mathbb{N}\right\}.$$

The first term is $o\left(\frac{n}{\sqrt{c_0}}\right)$ w.h.p. by the arguments above, while the second term is deterministically at most the number of $\boldsymbol{\mu}_1$ over which the sum ranges, which is at most $|\Sigma|^{t_0+1} = O(1)$. Therefore w.h.p. $|E_0| = o\left(\frac{n}{\sqrt{c_0}}\right)$, as required. □

5.4. **Similar in-compilations.** Our next goal is to show that the in-compilation sequence distribution in $\mathbb{G}_{t_0}$ is essentially the same as that in $\hat{\mathbb{G}}_{t_0}$.

Proposition 5.6. *Let t_0 be some (bounded) integer. Then w.h.p. the following holds.*

(1) For every integer $d \leq d_0$ and for every $A \in \left(\!\!\binom{\Sigma^{t_0+2}}{d}\!\!\right)$ we have $n_A\left(\mathbb{G}_{t_0}\right), n_A\left(\hat{\mathbb{G}}_{t_0}\right) = \left(\sum_{i\in[k]} \gamma_A^i n_i\right) + o\left(\frac{n}{\sqrt{c_0}}\right)$.

(2) $\hat{\mathbb{G}}_{t_0}, \mathbb{G}_{t_0}$ *each contains at most* $\frac{n}{c_0}$ *vertices of degree at least* d_0.

Proof. The proof is technical, but ultimately standard and we give only a short overview. The proofs of the two statements for $\hat{\mathbb{G}}_{t_0}$ essentially already appear in the proof of Proposition 5.5, which estimated the same parameters in the random model *before* half-edges were deleted. We therefore only need to additionally take account of the fact that some half-edges were deleted, but Proposition 5.5 itself implies that this will not affect things too much.

To prove the first statement for $\mathbb{G}_{t_0}$ we apply **B1**. More precisely, the sets of local neighbourhoods up to depth t_0 in $\mathbb{G}$ of all vertices of V_i look similar to n_i independent copies of $\mathscr{T}_i^{t_0}(\mathscr{Z})$. Furthermore, since the message initialisation in $\mathbb{G}$ is according to Q_0, and since there are very few dependencies between the local neighbourhoods, the same is true if we consider the *messaged* local neighbourhoods at time 0. Since these messaged neighbourhoods determine the corresponding t_0-input at the root, a Chernoff bound shows that w.h.p. we have concentration of $n_A(\mathbb{G}_{t_0})$ around its expectation. Importantly the $1/\omega_0$ term that describes the speed of convergence of the local structure to $\mathscr{T}_i^{t_0}$ is smaller than $1/\sqrt{c_0}$, the (normalised) error term in the statement.

For the second statement, we also apply **B1**, although here we only need to go to depth 1 and need not consider any messages. We also use **A3** to bound the number of half-edges attached to vertices at which $\mathbb{G}$ and the copies of $\mathscr{T}_i^1$ disagree. Otherwise the proof is similar. □

Let $a_0 := \frac{\sqrt{c_0}}{4d_0|\Sigma|^{(t_0+2)d_0}}$. As a corollary of Proposition 5.6, we obtain the following result.

Corollary 5.7. *After re-ordering vertices if necessary, w.h.p. the number of vertices whose in-compilations are different in* $\hat{\mathbb{G}}_{t_0}$ *and* $\mathbb{G}_{t_0}$ *is at most* $\frac{n}{a_0}$.

Proof. Assuming the high probability event of Proposition 5.6 holds, the number of vertices with differing in-compilations is at most

$$\left(\sum_{d=0}^{d_0}\sum_{A\in\left(\!\!\binom{\Sigma^{t_0+2}}{d}\!\!\right)}\frac{2n}{\sqrt{c_0}}\right)+\frac{2n}{c_0}\leq\frac{2n}{\sqrt{c_0}}\left(\sum_{d=0}^{d_0}|\Sigma|^{(t_0+2)d}\right)+\frac{2n}{c_0}$$
$$\leq\frac{2n}{\sqrt{c_0}}d_0|\Sigma|^{(t_0+2)d_0}+\frac{2n}{c_0}=\frac{2n}{4a_0}+\frac{2n}{c_0}\leq\frac{n}{a_0},$$

where the last approximation follows by definition of a_0. □

5.5. **Matching up.** Next, we show that choosing the random matching as we did in Step 4 of the construction of $\hat{\mathbb{G}}_{t_0}$ is an appropriate choice. We already defined the type-degree sequence of a graph, which generalises the degree sequence, but we need to generalise this notion still further to also track the in-coming stories at a vertex.

Definition 5.8. *For any* Σ^{t_0+1}*-messaged graph* $G\in\mathscr{G}_n^{(t_0)}$*, let* $H_i=H_i(G)$ *denote the in-compilation at vertex* i*, for* $i\in[n]$ *and let* $\boldsymbol{H}(G):=(H_1,\dots,H_n)$ *be the in-compilation sequence.*

Claim 5.9. *Suppose that* G_1,G_2 *are two graphs on* $[n]$ *with* $\boldsymbol{H}(G_1)=\boldsymbol{H}(G_2)$*. Then* $\mathbb{P}(\mathbb{G}=G_1)=(1+o(1))\,\mathbb{P}(\mathbb{G}=G_2)$.

Proof. If $\boldsymbol{H}(G_1)=\boldsymbol{H}(G_2)$, then in particular $\boldsymbol{D}(G_1)=\boldsymbol{D}(G_2)$. Then by Assumption **A2**, we have that $\mathbb{P}(\mathbb{G}=G_1)=(1+o(1))\,\mathbb{P}(\mathbb{G}=G_2)$. □

5.6. **Message consistency.** We also need to know that the message histories generated in the construction of $\hat{\mathbb{G}}_{t_0}$ match those that would be produced by Warning Propagation. Let $\hat{\mathbb{G}}_{\mathrm{WP}}$ denote the graph with message histories generated by constructing $\hat{\mathbb{G}}_{t_0}$, stripping all the message histories except for the messages at time 0 and running Warning Propagation for t_0 steps with this initialisation. Furthermore, let X_0 be the set of vertices at which some half-edges were deleted in Step 4 of the construction of $\hat{\mathbb{G}}_{t_0}$, and for $t\in\mathbb{N}$ let X_t be the set of vertices at distance at most t from X_0 in $\hat{\mathbb{G}}_{t_0}$.

Proposition 5.10. *Deterministically we have* $\hat{\mathbb{G}}_{\mathrm{WP}}=\hat{\mathbb{G}}_{t_0}$ *except on those edges incident to* X_{t_0}*. Furthermore, on those edges incident to* X_{t_0} *but not* X_{t_0-1}*, the message histories in* $\hat{\mathbb{G}}_{\mathrm{WP}}$ *and* $\hat{\mathbb{G}}_{t_0}$ *are identical up to time* t_0-1.

Proof. Since the two underlying unmessaged graphs are the same, we just need to prove that at any time $0\leq t\leq t_0$, the incoming and outgoing messages at a given vertex $v\notin X_{t-1}$ are the same for $\hat{\mathbb{G}}_{t_0}$ and $\hat{\mathbb{G}}_{\mathrm{WP}}$ (where we set $X_{-1}:=\emptyset$). We will prove the first statement by induction on t. At time $t=0$, the statement is true by construction

of $\hat{\mathbb{G}}_{\mathrm{WP}}$. Now suppose it is true up to time t for some $0 \le t \le t_0 - 1$ and consider an arbitrary directed edge (u, v) between vertices $u, v \notin X_t$. By Definition 3.4 (2), the $(t+1)$-out-message from u in $\hat{\mathbb{G}}_{t_0}$ is produced according to the rules of Warning Propagation based on the t-in-messages to u at time t. Since $u \notin X_t$, none of its neighbours lie in X_{t-1} and therefore by the induction hypothesis, these t-in-messages are the same for $\hat{\mathbb{G}}_{t_0}$ and $\hat{\mathbb{G}}_{\mathrm{WP}}$. Hence, the $(t+1)$-out-message along (u, v) is also the same in $\hat{\mathbb{G}}_{t_0}$ and $\hat{\mathbb{G}}_{\mathrm{WP}}$. This proves the first statement of the proposition, while the second follows from the inductive statement for $t = t_0 - 1$. □

In view of Proposition 5.10, we need to know that not too many edges are incident to X_{t_0}.

Proposition 5.11. *Let $t \in \mathbb{N}$ be any constant. W.h.p. the number of edges of $\hat{\mathbb{G}}$ incident to X_t is $o(n)$.*

Proof. The statement for $t = 0$ is implied by the (slightly stronger) statement of Proposition 5.5. For general t, the statement follows since the average degree in $\hat{\mathbb{G}}$ is bounded. More precisely, the expected number of edges of $\hat{\mathbb{G}}$ incident to X_t is $(O(1))^t |X_0| = O(1)|X_0| = o(n)$, and an application of Markov's inequality completes the proof. □

5.7. **Final steps.** We can now complete the proof of Lemma 3.7.

Proof of Lemma 3.7. We use the preceding auxiliary results to show that every step in the construction of $\hat{\mathbb{G}}_{t_0}$ closely mirrors a corresponding step in which we reveal partial information about $\mathbb{G}_{t_0}$. Let us first explicitly define these steps within $\mathbb{G}_{t_0}$ by revealing information one step at a time as follows.

(1) First reveal the in-compilation at each vertex, modelled along half-edges.
(2) Next reveal all out-stories along each half-edge.
(3) Finally, reveal which half-edges together form an edge.

Corollary 5.7 shows that Step 2 in the construction of $\hat{\mathbb{G}}_{t_0}$ can be coupled with Step 2 in revealing $\mathbb{G}_{t_0}$ above in such a way that w.h.p. the number of vertices on which they produce different results is at most $\frac{n}{a_0} = o(n)$. Furthermore, Proposition 5.10 shows that, for those vertices for which the in-compilations are identical in Step 2, the out-stories generated in Step 3 of the construction of both $\hat{\mathbb{G}}_{t_0}$ and $\mathbb{G}_{t_0}$ must also be identical (deterministically). Therefore before the deletion of unmatched half-edges in Step 4 of the definition of $\hat{\mathbb{G}}_{t_0}$, w.h.p. Condition (2) of Definition 3.6 is satisfied. On the other hand, Proposition 5.5 states that w.h.p. $o\left(n/\sqrt{c_0}\right) = o(n)$ half-edges are deleted, and therefore the condition remains true even after this deletion.

Now in order to prove that we can couple the two models in such a way that the two edge sets are almost the same (and therefore Condition (1) of Definition 3.6 is satisfied), we consider each potential story $\boldsymbol{\mu} \in \Sigma^{2(t_0+1)}$ in turn, and construct coupled random matchings of the corresponding half-edges. More precisely, let us fix $\boldsymbol{\mu}$ and let $\hat{m}$ be the number of half-edges with this story in $\hat{\mathbb{G}}_{t_0}$. Similarly, define m to be the corresponding number of half-edges in $\mathbb{G}_{t_0}$. Furthermore, let $\hat{r}_1$ be the number of half-edges with story $\boldsymbol{\mu}$ in $\hat{\mathbb{G}}_{t_0} \setminus \mathbb{G}_{t_0}$, let $\hat{r}_2$ be the number of half-edges with the "dual story" $\boldsymbol{\mu}^*$, i.e. the story with in-story and out-story switched, and correspondingly r_1, r_2 in $\mathbb{G}_{t_0} \setminus \hat{\mathbb{G}}_{t_0}$.

For convenience, we will assume that $\boldsymbol{\mu}^* \neq \boldsymbol{\mu}$; the case when they are equal is very similar.

Let us call an edge of a matching *good* if it runs between two half-edges which are common to both models. Note that this does not necessarily mean it is common to both matchings, although we aim to show that we can couple in such a way that this is (mostly) the case. Observe that, conditioned on the number of good edges in a matching, we may first choose a matching of this size uniformly at random on the common half-edges, and then complete the matching uniformly at random (subject to the condition that we never match two common half-edges).

Observe further that the matching in $\hat{\mathbb{G}}_{t_0}$ must involve at least $\hat{m} - \hat{r}_1 - \hat{r}_2$ good edges, and similarly the matching in $\mathbb{G}_{t_0}$ must involve at least $m - r_1 - r_2$, and therefore we can couple in such a way that at least $\min\{\hat{m} - \hat{r}_1 - \hat{r}_2, m - r_1 - r_2\}$ edges are identical, or in other words, the symmetric difference of the matchings has size at most $\max\{\hat{r}_1 + \hat{r}_2, r_1 + r_2\}$.

Repeating this for each possible $\boldsymbol{\mu}$, the total number of edges in the symmetric difference is at most twice the number of half-edges which are not common to both models. We have already shown that there are at most $o\left(\frac{n}{a_0}\right) + o\left(\frac{n}{\sqrt{c_0}}\right) = o\left(\frac{n}{a_0}\right)$ vertices at which the in-compilations differ, and applying the second statement of Proposition 5.6, we deduce that w.h.p.the number of half-edges which are not common to both models is at most $d_0 \cdot o\left(\frac{n}{a_0}\right) + 2 \cdot \frac{n}{c_0} = o(n)$ as required. □

6. SUBCRITICALITY: THE IDEALISED CHANGE PROCESS

With Lemma 3.7 to hand, which tells us that $\mathbb{G}_{t_0}$ and $\hat{\mathbb{G}}_{t_0}$ look very similar, we break the rest of the proof of Theorem 1.3 down into two further steps.

First, in this section, we describe an idealised approximation of how a change propagates when applying WP repeatedly to $\overline{\mathbb{G}}_{t_0}$, and show that this approximation is a subcritical process, and therefore quickly dies out. The definition of this idealised change process is motivated by the similarity to $\hat{\mathbb{G}}_{t_0}$.

In the second step, in Section 7 we will use Lemma 3.7 to prove formally that the idealised change process closely approximates the actual change process, which therefore also quickly terminates.

Definition 6.1. *Given a probability distribution matrix Q on Σ, we say that a pair of messages (σ_0,τ_0) is a* potential change *with respect to Q if there exist some $t\in\mathbb{N}$ and some $\boldsymbol{\mu}=(\mu_0,\mu_1,\dots,\mu_t)\in\mathscr{C}_{t+1}$ such that*

- $\mu_{t-1}=\sigma_0$;
- $\mu_t=\tau_0$;
- $\mathbb{P}\left(\boldsymbol{\phi}^t_\varphi(Q)\left[\bar{g}(\mu)\right]=\boldsymbol{\mu}\right)>0$.

We denote the set of potential changes by $\mathscr{P}(Q)$.

In other words, (σ_0,τ_0) is a potential change if there is a positive probability of making a change from σ_0 to τ_0 in the message at the root edge at some point in the Warning Propagation algorithm on a $\mathscr{T}_{g(\sigma_0)}$ branching tree when initialising according to Q. The following simple claim will be important later.

Claim 6.2. *If P is a fixed point and $(\sigma_0,\tau_0)\in\mathscr{P}(P)$ with $g(\sigma_0)=(i,j)$, then $P[i,j](\sigma_0)>0$ and $P[i,j](\tau_0)<1$.*

Proof. The definition of $\mathscr{P}(P)$ implies in particular that there exist a $t\in\mathbb{N}$ and a $\boldsymbol{\mu}\in\mathscr{C}_{t+1}$ such that $\mu_{t-1}=\sigma_0$ and $\mathbb{P}\left(\boldsymbol{\phi}^t_\varphi(P)[i,j]=\boldsymbol{\mu}\right)>0$. Furthermore, by Claim 4.1, the marginal distribution of the t-th entry of $\boldsymbol{\phi}^t_\varphi(P)[i,j]$ is $\phi^t_\varphi(P)[i,j]=P[i,j]$ (since P is a fixed point), and therefore we have $P[i,j](\sigma_0)\geq\mathbb{P}\left(\boldsymbol{\phi}^t_\varphi(P)[i,j]=\boldsymbol{\mu}\right)>0$.

On the other hand, since $P[i,j]$ is a probability distribution on Σ, clearly $P[i,j](\tau_0)\leq 1-P[i,j](\sigma_0)<1$. □

6.1. **The idealised change branching process.** Given a probability distribution matrix Q on Σ and a pair $(\sigma_0,\tau_0)\in\mathscr{P}(Q)$, we define a branching process $\mathfrak{T}=\mathfrak{T}(\sigma_0,\tau_0,Q)$ as follows. We generate an instance of $\mathscr{T}_{ij}$, where $(i,j)=\bar{g}(\sigma_0)$, in particular including messages upwards to the directed root edge (v,u), so u is the parent of v. We then also initialise two messages downwards along this root edge, $\mu^{(1)}_{u\to v}=\sigma_0$ and $\mu^{(2)}_{u\to v}=\tau_0$. We track further messages down the tree based on the message that a vertex receives from its parent and its children according to the WP update rule φ. Given a vertex y with parent x, let $\mu^{(1)}_{x\to y}$ be the resultant message when the input at the root edge is $\mu^{(1)}_{u\to v}=\sigma_0$, and similarly $\mu^{(2)}_{x\to y}$ the resultant message when the input is $\mu^{(2)}_{u\to v}=\tau_0$. Finally, delete all edges (x,y) for which $\mu^{(1)}_{x\to y}=\mu^{(2)}_{x\to y}$, so we keep only edges at which messages change (along with any subsequently isolated vertices). It is an elementary consequence of the construction that $\mathfrak{T}$ is necessarily a tree.

6.2. **Subcriticality.** Intuitively, $\mathfrak{T}$ approximates the cascade effect that a single change in a message from time t_0-1 to time t_0 subsequently causes (this is proved more precisely in Section 7). Therefore while much of this paper is devoted to showing that $\mathfrak{T}$ is indeed a good approximation, a very necessary task albeit an intuitively natural outcome, the following result is the essential heart of the proof of Theorem 1.3.

Proposition 6.3. *If P is a stable fixed point, then for any $(\sigma_0,\tau_0)\in\mathscr{P}(P)$, the branching process $\mathfrak{T}=\mathfrak{T}(\sigma_0,\tau_0,P)$ is subcritical.*

Proof. Let us suppose for a contradiction that for some $(\sigma_0,\tau_0)\in\mathscr{P}(P)$, the branching process has survival probability $\rho>0$. We will use the notation $a\ll b$ to indicate that given b, we choose a sufficiently small as a function of b.[4]

Given ρ and also Σ,φ,P, let us fix further parameters $\varepsilon,\delta\in\mathbb{R}$ and $t_1\in\mathbb{N}$ according to the following hierarchy:

$$0<\varepsilon\ll\frac{1}{t_1}\ll\delta\ll\rho,\frac{1}{|\Sigma|}\leq 1.$$

[4] In the literature this is often denoted by $a\ll b$, but we avoid this notation since it has a very different meaning elsewhere in the paper. In particular, here we aim to fix several parameters which are all constants rather than functions in n.

In the following, given an integer t and messages $\sigma_t, \tau_t \in \Sigma$, we will use the notation $\boldsymbol{\sigma}_t := (\sigma_t, \tau_t)$. Let us define a new probability distribution matrix Q on Σ as follows. For each $(i,j) \in [k]^2$ and for all $\mu \in \Sigma$

$$Q[i,j](\mu) := \begin{cases} P[i,j](\mu) - \varepsilon & \text{if } (i,j) = g(\boldsymbol{\sigma}_0) \text{ and } \mu = \sigma_0; \\ P[i,j](\mu) + \varepsilon & \text{if } (i,j) = g(\boldsymbol{\sigma}_0) \text{ and } \mu = \tau_0; \\ P[i,j](\mu) & \text{otherwise.} \end{cases}$$

In other words, we edit the probability distribution in the $g(\boldsymbol{\sigma}_0)$ entry of the matrix P to shift some weight from σ_0 to τ_0, but otherwise leave everything unchanged. Note that since $(\sigma_0, \tau_0) \in \mathscr{P}(P)$ is a potential change, for sufficiently small ε, each entry $Q[i,j]$ of Q is indeed a probability distribution (by Claim 6.2 for $(i,j) = g(\boldsymbol{\sigma}_0)$ or trivially otherwise).

Let us generate the t_1-neighbourhood of a root vertex u of type i in a $\mathscr{T}_i$ branching process and initialise messages from the leaves at depth t_1 according to both Q and P, where we couple in the obvious way so that all messages are identical except for some which are σ_0 under P and τ_0 under Q. We call such messages *changed* messages.

We first track the messages where we initialise with P through the tree (both up and down) according to the Warning Propagation rules, but without ever updating a message once it has been generated. Since P is a fixed point of φ, each message μ either up or down in the tree has the distribution $P[g(\mu)]$ (though clearly far from independently).

We then track the messages with initialisation according to Q through the tree, and in particular track where differences from the first set of messages occur. Let $x_s(\boldsymbol{\sigma}_1)$ denote the probability that a message from a vertex at level $t_1 - s$ to its parent changes from σ_1 to τ_1. Thus in particular we have

$$x_0(\boldsymbol{\sigma}_1) = \begin{cases} \varepsilon & \text{if } \boldsymbol{\sigma}_1 = \boldsymbol{\sigma}_0, \\ 0 & \text{otherwise.} \end{cases}$$

Observe also that messages coming down from parent to child "don't have time" to change before we consider the message up (the changes from below arrive before the changes from above). Since we are most interested in changes which are passed *up* the tree, we may therefore always consider a message coming down as being distributed according to P (more precisely, according to $P[i,j]$, where i,j are the types of the parent and child respectively).

We aim to approximate $x_{s+1}(\boldsymbol{\sigma}_1)$ based on x_s, so let us consider a vertex u at level $t_1 - (s+1)$ and its parent v. Let us define $C_d = C_d(u)$ to be the event that u has precisely d children. Furthermore, let us define $D_u(\boldsymbol{\sigma}_2)$ to be the event that exactly one change is passed up to u from its children, and that this change is of type $\boldsymbol{\sigma}_2$. Finally, let $b_u(\boldsymbol{\sigma}_1)$ be the number of messages from u (either up or down) which change from σ_1 to τ_1 (there may be more changes of other types).

The crucial observation is that given the neighbours of u and their types, each is equally likely to be the parent – this is because the tree $\mathscr{T}_i$ is constructed in such a way that, conditioned on the presence and type of the parent, the type-degree distribution of a vertex of type j is $\mathscr{Z}_j$, regardless of what the type of the parent was. Therefore conditioned on the event $D_u(\boldsymbol{\sigma}_2)$ and the values of d and $b_u(\boldsymbol{\sigma}_1)$, apart from the one child from which a change of type $\boldsymbol{\sigma}_2$ arrives at u, there are d other neighbours which could be the parent, of which $b_u(\boldsymbol{\sigma}_1)$ will receive a change of type $\boldsymbol{\sigma}_1$. Thus the probability that a change of type $\boldsymbol{\sigma}_1$ is passed up to the parent is precisely $\frac{b_u(\boldsymbol{\sigma}_1)}{d}$.

Therefore in total, conditioned on C_d and $D_u(\boldsymbol{\sigma}_2)$, the probability $a_{d;\boldsymbol{\sigma}_1,\boldsymbol{\sigma}_2}$ that a change of type $\boldsymbol{\sigma}_1$ is passed on from u to v is

$$a_{d;\boldsymbol{\sigma}_1,\boldsymbol{\sigma}_2} = \sum_{\ell=1}^{d} \left(\mathbb{P}(b_u(\boldsymbol{\sigma}_1) = \ell \mid C_d \wedge D_u(\boldsymbol{\sigma}_2)) \cdot \frac{\ell}{d} \right) = \frac{1}{d} \cdot \mathbb{E}(b_u(\boldsymbol{\sigma}_1) \mid C_d \wedge D_u(\boldsymbol{\sigma}_2)).$$

Now observe that this conditional expectation term is exactly as in the change process. More precisely, in the $\mathfrak{T}$ process we know automatically that only one change arrives at a vertex, and therefore if we have a change of type $\boldsymbol{\sigma}_2$, the event $D_u(\boldsymbol{\sigma}_2)$ certainly holds. Therefore, letting $h = g_1(\sigma_2)$ and $\ell = g_2(\sigma_2)$,

$$\sum_{d \geq 1} \sum_{\boldsymbol{d} \in \mathrm{Se}(d)} \mathbb{P}(\mathscr{Y}_{\ell,h} = \boldsymbol{d})\, d\, a_{d;\boldsymbol{\sigma}_1,\boldsymbol{\sigma}_2} = T[\boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2], \tag{6.1}$$

where $\mathrm{Se}(d)$ is the set of sequences $\boldsymbol{d} := (d_1, \dots, d_k) \in \mathbb{N}_0^k$ such that $\sum_{\ell'=1}^{k} d_{\ell'} = d$ and T is the $|\Sigma|^2 \times |\Sigma|^2$ transition matrix associated with the $\mathfrak{T}$ change process, i.e. the entry $T[\boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2]$ is equal to the expected number of changes of type $\boldsymbol{\sigma}_1$ produced in the next generation by a change of type $\boldsymbol{\sigma}_2$.

On the other hand, defining E_u to be the event that at least two children of u send changed messages (of any type) to u, we also have

$$\begin{aligned} x_{s+1}(\boldsymbol{\sigma}_1) &\geq \sum_{d\geq 1} \sum_{\boldsymbol{d}\in \mathrm{Se}(d)} \mathbb{P}\left(\mathscr{Y}_{\ell,h} = \boldsymbol{d}\right) \sum_{\boldsymbol{\sigma}_2 \in \Sigma^2} a_{d;\boldsymbol{\sigma}_1,\boldsymbol{\sigma}_2} \mathbb{P}\left(D_u(\boldsymbol{\sigma}_2) \,|C_d\right) \\ &\geq \sum_{d\geq 1} \sum_{\boldsymbol{d}\in \mathrm{Se}(d)} \mathbb{P}\left(\mathscr{Y}_{\ell,h} = \boldsymbol{d}\right) \sum_{\boldsymbol{\sigma}_2 \in \Sigma^2} a_{d;\boldsymbol{\sigma}_1,\boldsymbol{\sigma}_2} \Big(d x_s(\boldsymbol{\sigma}_2) - \mathbb{P}\left(E_u | C_d\right) \Big). \end{aligned} \tag{6.2}$$

For each $s \in \mathbb{N}$, let $\boldsymbol{x}_s$ be the $|\Sigma|^2$-dimensional vector whose entries are $x_s(\boldsymbol{\sigma})$ for $\boldsymbol{\sigma} \in \Sigma^2$ (in some arbitrary order). We now observe that, since P is a stable fixed point, i.e. ϕ_φ is a contraction on a neighbourhood of P, and since $d_{\mathrm{TV}}(P,Q) = \varepsilon$, for small enough ε we have

$$\sum_{\boldsymbol{\sigma}\in\Sigma^2} x_s(\boldsymbol{\sigma}) = \|\boldsymbol{x}_s\|_1 = d_{\mathrm{TV}}\Big(P, \phi_\varphi^s(Q)\Big) \leq d_{\mathrm{TV}}(P,Q) = \|\boldsymbol{x}_0\|_1 = \varepsilon,$$

and so we further have

$$\mathbb{P}\left(E_u | C_d\right) \leq \binom{d}{2} \varepsilon^2 \leq d^2 \varepsilon^2. \tag{6.3}$$

Furthermore, we observe that since $a_{d;\boldsymbol{\sigma}_1,\boldsymbol{\sigma}_2}$ is a probability term by definition, we have

$$\sum_{\boldsymbol{\sigma}_2\in\Sigma^2} a_{d;\boldsymbol{\sigma}_1,\boldsymbol{\sigma}_2} \leq \sum_{\boldsymbol{\sigma}_2\in\Sigma^2} 1 = |\Sigma|^2. \tag{6.4}$$

Substituting (6.1), (6.3) and (6.4) into (6.2), we obtain

$$x_{s+1}(\boldsymbol{\sigma}_1) \geq \sum_{\boldsymbol{\sigma}_2\in\Sigma^2} T[\boldsymbol{\sigma}_1,\boldsymbol{\sigma}_2]\, x_s(\boldsymbol{\sigma}_2) - |\Sigma|^2 \varepsilon^2 \sum_{d\geq 1} d^2 \sum_{\boldsymbol{d}\in\mathrm{Se}(d)} \mathbb{P}\left(\mathscr{Y}_{\ell,h} = \boldsymbol{d}\right).$$

Moreover, we have

$$\sum_{d\geq 1} d^2 \sum_{\boldsymbol{d}\in\mathrm{Se}(d)} \mathbb{P}\left(\mathscr{Y}_{\ell,h} = \boldsymbol{d}\right) = \sum_{d\geq 1} d^2 \mathbb{P}\left(\left\|\mathscr{Y}_{\ell,h}\right\|_1 = d\right) = \mathbb{E}\left(\left\|\mathscr{Y}_{\ell,h}\right\|_1^2\right).$$

Now for any $h, \ell \in [k]$ we have that $\mathbb{E}\left(\left\|\mathscr{Y}_{\ell,h}\right\|_1^2\right)$ is finite by Remark 2.15, so defining $c := \max_{h,\ell\in[k]} \mathbb{E}\left(\left\|\mathscr{Y}_{\ell,h}\right\|_1^2\right)$, we have

$$|\Sigma|\, \boldsymbol{x}_{s+1} \geq T \boldsymbol{x}_s - c|\Sigma|^2 \varepsilon^2$$

(where the inequality is pointwise). As a direct consequence we also have $\boldsymbol{x}_s \geq T^s \boldsymbol{x}_0 - sc|\Sigma|^2\varepsilon^2$ (pointwise), and therefore

$$\|\boldsymbol{x}_s\|_1 \geq \|T^s \boldsymbol{x}_0\|_1 - sc|\Sigma|^4 \varepsilon^2.$$

Now since the change process has survival probability $\rho > 0$ for the appropriate choice of $\boldsymbol{\sigma}_0 = (\sigma_0, \tau_0)$, choosing $\boldsymbol{x}_0 = \varepsilon \boldsymbol{e}_{\boldsymbol{\sigma}_0}$ (where $\boldsymbol{e}_{\boldsymbol{\sigma}_0}$ is the corresponding standard basis vector) we have

$$\|\boldsymbol{x}_s\|_1 \geq \|T^s \boldsymbol{x}_0\|_1 - sc|\Sigma|^4\varepsilon^2 \geq \rho\|\boldsymbol{x}_0\|_1 - sc|\Sigma|^4\varepsilon^2 = \varepsilon\left(\rho - sc|\Sigma|^4\varepsilon\right).$$

On the other hand, since P is a stable fixed point, there exists some $\delta > 0$ such that for small enough ε we have $\|\boldsymbol{x}_s\|_1 \leq (1-\delta)^s \varepsilon$ for all s. In particular choosing $s = t_1$, we conclude that

$$\varepsilon\left(\rho - t_1 c|\Sigma|^4\varepsilon\right) \leq \|\boldsymbol{x}_{t_1}\|_1 \leq (1-\delta)^{t_1}\varepsilon.$$

However, since we have $\varepsilon \ll 1/t_1 \ll \delta \ll \rho, 1/|\Sigma|$, we observe that

$$(1-\delta)^{t_1} \leq \rho/2 < \rho - t_1 c|\Sigma|^4\varepsilon,$$

which is clearly a contradiction. □

7. Applying subcriticality: Proof of Theorem 1.3

Our goal in this section is to use Proposition 6.3 to complete the proof of Theorem 1.3.

7.1. **A consequence of subcriticality.** Recall that during the proof of Proposition 6.3 we defined the transition matrix T of the change process $\mathfrak{T}$, which is a $|\Sigma|^2 \times |\Sigma|^2$ matrix where the entry $T[\boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2]$ is equal to the expected number of changes of type $\boldsymbol{\sigma}_1$ that arise from a change of type $\boldsymbol{\sigma}_2$. The subcriticality of the branching process is equivalent to $T^n \xrightarrow{n\to\infty} 0$ (meaning the zero matrix), which is also equivalent to all eigenvalues of T being strictly less than 1 (in absolute value). We therefore obtain the following corollary of Proposition 6.3.

Corollary 7.1. *There exist a constant $\gamma > 0$ and a positive real $|\Sigma|^2$-dimensional vector $\boldsymbol{\alpha}$ (with no zero entries) such that*

$$T\boldsymbol{\alpha} \leq (1-\gamma)\boldsymbol{\alpha}$$

(where the inequality is understood pointwise). We may further assume that $\|\boldsymbol{\alpha}\|_1 = 1$.

Proof. Given some $\epsilon > 0$, let $T' = T'(\epsilon)$ be the matrix obtained from T by adding ϵ to each entry. Thus T' is a strictly positive real matrix and we may choose ϵ to be small enough such that all the eigenvalues of T' are still less than 1 in absolute value. By the Perron-Frobenius theorem, there exists a positive real eigenvalue that matches the spectral radius $\rho(T') < 1$ of T'. In addition, there exists a corresponding eigenvector to $\rho(T')$, say $\boldsymbol{\alpha}$, all of whose entries are non-negative; since every entry of T' is strictly positive, it follows that in fact every entry of $\boldsymbol{\alpha}$ is also strictly positive. We have $T'\boldsymbol{\alpha} = \rho(T')\boldsymbol{\alpha}$, and we also note that $T\boldsymbol{\alpha} < T'\boldsymbol{\alpha}$ since every entry of T' is strictly greater than the corresponding entry of T. Thus we deduce that $T\boldsymbol{\alpha} < \rho(T')\boldsymbol{\alpha}$, and setting $\gamma := 1 - \rho(T') > 0$, we have the desired statement.

The final property that $\|\boldsymbol{\alpha}\|_1 = 1$ can be achieved simply through scaling by an appropriate (positive) normalising constant, which does not affect any of the other properties of $\boldsymbol{\alpha}$. □

However, let us observe that in fact the change process that we want to consider is slightly different – rather than having in-messages distributed according to P, they should be distributed according to $\phi_\varphi^{t_0-1}(Q_0)$. Since P is the stable limit of Q_0, this is arbitrarily close, but not exactly equal, to P. We therefore need the following.

Corollary 7.2. *There exists $\delta_0 > 0$ sufficiently small that for any probability distribution Q on Σ which satisfies $d_{\mathrm{TV}}(P,Q) \leq \delta_0$, the following holds. Let $\mathfrak{T}_1 = \mathfrak{T}(\sigma_0, \tau_0, Q)$ and let T_1 be the transition matrix of $\mathfrak{T}_1$. Then there exist a constant $\gamma > 0$ and a positive real $|\Sigma|^2$-dimensional vector $\boldsymbol{\alpha}$ (with no zero entries) such that*

$$T_1\boldsymbol{\alpha} \leq (1-\gamma)\boldsymbol{\alpha}$$

(where the inequality is understood pointwise).

In other words, the same statement holds for T_1, the transition matrix of this slightly perturbed process, as for T. In particular, $\mathfrak{T}_1$ is also a subcritical branching process.

Proof. Observe that since $d_{\mathrm{TV}}(P,Q) \leq \delta_0$, for any ϵ we may pick $\delta_0 = \delta(\epsilon)$ sufficiently small such that T_1 and T differ by at most ϵ in each entry. In other words, we have $T_1 \leq T'$ pointwise, where $T' = T'(\epsilon)$ is as defined in the proof of Corollary 7.1. Thus we also have $T_1\boldsymbol{\alpha} \leq T'\boldsymbol{\alpha} = \rho(T')\boldsymbol{\alpha} = (1-\gamma)\boldsymbol{\alpha}$ as in the previous proof. □

For the rest of the proof, let us fix δ as in Theorem 1.3 and a constant $\delta_0 \ll \delta$ small enough that the conclusion of Corollary 7.2 holds, and also such that w.h.p. $\sum_{i=1}^k n_i \leq \delta_0^{-1/100} n$, which is possible because by Claim 2.16 we have $n_i = (1+o(1))\mathbb{E}(n_i) = \Theta(n)$ w.h.p.. Moreover, suppose that t_0 is large enough that $P' := \phi_\varphi^{t_0-1}(Q_0)$ satisfies $d_{\mathrm{TV}}(P,P') \leq \delta_0$ (this is possible since $\phi_\varphi^*(Q_0) = P$).

7.2. **The marking process.** We now use the idealised form $\mathfrak{T}_1$ of the change process to give an upper bound on the (slightly messier) actual process. For an upper bound, we will slightly simplify the process of changes made by WP to obtain $\mathrm{WP}^*\left(\overline{\mathbb{G}}_{t_0}\right) = \mathrm{WP}^*\left(\overline{\mathbb{G}}_0\right)$ from $\overline{\mathbb{G}}_{t_0}$. [5]

We will reveal the information in $\mathbb{G}_{t_0}$ a little at a time as needed.

- Initialisation
  - We first reveal the t_0-inputs at each vertex, and the corresponding out-stories according to the update rule φ. We also generate the outgoing messages at time t_0+1. Any half-edge whose t_0-out-message is σ_0 and whose (t_0+1)-out-message is $\tau_0 \neq \sigma_0$ is called a *change of type* $\boldsymbol{\sigma}_0$.
  - For each out-story which includes a change, this half-edge is *marked*.

[5] Note here that with a slight abuse of notation, we use WP to denote the obvious function on $\mathcal{G}_n$ which, given a graph G with messages $\boldsymbol{\mu} \in \mathcal{M}(G)$, maps $(G,\boldsymbol{\mu})$ to $\mathrm{WP}(G,\boldsymbol{\mu}) := (G, \mathrm{WP}_G(\boldsymbol{\mu}))$.

- We continue with a *marking process*:
  - Whenever a half-edge at u is marked, we reveal its partner v. The edge uv is marked.
  - If v is a new vertex (at which nothing was previously marked), if the degree of v is at most k_0 and if the inputs are identical in $\mathbb{G}_{t_0}$ and $\hat{\mathbb{G}}_{t_0}$, we consider the remaining half-edges at v and apply the rules of Warning Propagation to determine whether any out-messages will change. Any that do become marked. We call such a vertex a *standard vertex*.
  - If v does not satisfy all three of these conditions, we say that we have *hit a snag*. In particular:
    - If v is a vertex that we have seen before, it is called a *duplicate* vertex;
    - If v is a vertex of degree at most d_0 whose inputs are different according to $\mathbb{G}_{t_0}$ and $\hat{\mathbb{G}}_{t_0}$, it is called an *error* vertex; [6]
    - If v is a vertex of degree larger than d_0, it is called a *freak* vertex.

    In each case, all of the half-edges at v become marked. Such half-edges are called *spurious* edges, and are further classified as *defective*, *erroneous* and *faulty* respectively, according to the type of snag we hit. The corresponding messages can change arbitrarily (provided each individual change is in $\mathscr{P}(P)$).

Note that a duplicate vertex may also be either an error or a freak vertex. However, by definition, no snag is both an error and a freak vertex.

We first justify that this gives an upper bound on the number of changes made by Warning Propagation. Let $\mathscr{E}_{\mathrm{WP}}$ be the set of edges on which the messages are different in $\overline{\mathbb{G}}_{t_0}$ and in $\mathrm{WP}^*\left(\overline{\mathbb{G}}_{t_0}\right)$, and let $\mathscr{E}_{\mathrm{mark}}$ be the set of edges which are marked at the end of the marking process. Note that the set $\mathscr{E}_{\mathrm{mark}}$ is not uniquely defined, but depends on the arbitrary choices for the changes which are made at snags.

Proposition 7.3. *There exists some choice of the changes to be made at snags such that* $\mathscr{E}_{\mathrm{WP}} \subseteq \mathscr{E}_{\mathrm{mark}}$.

Proof. We proceed in rounds indexed by $t \in \mathbb{N}_0$. We define $\mathscr{E}_{\mathrm{WP}}(t)$ to be the set of edges on which the messages are different in $\mathrm{WP}^t\left(\overline{\mathbb{G}}_{t_0}\right)$ compared to $\overline{\mathbb{G}}_{t_0}$, while $\mathscr{E}_{\mathrm{mark}}(t)$ is the set of edges which are marked after t steps of the marking process. Since $\mathscr{E}_{\mathrm{WP}} = \lim_{t\to\infty}\mathscr{E}_{\mathrm{WP}}(t)$ and $\mathscr{E}_{\mathrm{mark}} = \lim_{t\to\infty}\mathscr{E}_{\mathrm{mark}}(t)$, it is enough to prove that for each $t \in \mathbb{N}_0$ we have $\mathscr{E}_{\mathrm{WP}}(t) \subseteq \mathscr{E}_{\mathrm{mark}}(t)$, which we do by induction on t.

The base case $t = 0$ is simply the statement that the set of initial marks contains the changes from $\overline{\mathbb{G}}_{t_0}$ to $\overline{\mathbb{G}}_{t_0+1}$, which is clearly true by construction.

For the inductive step, each time we reveal the incoming partner of a marked outgoing half-edge, if this is a vertex at which nothing was previously marked, i.e. a standard vertex, then we proceed with marking exactly according to Warning Propagation.

On the other hand, if at least one edge was already marked at this vertex we simply mark *all* the outgoing half-edges, and if we choose the corresponding changes according to the changes that will be made by Warning Propagation, the induction continues. □

In view of Proposition 7.3, our main goal is now the following.

Lemma 7.4. *At the end of the marking process, w.h.p. at most* $\sqrt{\delta_0}n$ *edges are marked.*

During the proof of Lemma 7.4, we will make extensive use of the following fact.

Claim 7.5. *W.h.p., for every* $\boldsymbol{\mu} \in \Sigma^{t_0+1}$ *such that* $\mathbb{P}_{Q^{(\leq t)}}(\boldsymbol{\mu}) \neq 0$*, the total number of inputs of* $\boldsymbol{\mu}$ *over all vertices is at least* $\delta_0^{1/100}n$.

Proof. Since $\mathbb{P}_{Q^{(\leq t)}}(\boldsymbol{\mu}) \neq 0$, there certainly exists some $d \in \mathbb{N}$ and some $A \in \left(\!\!\binom{\Sigma^{t_0+1}}{d}\!\!\right)$ such that $\boldsymbol{\mu} \in A$ and $\gamma_A > 0$. Since we chose δ_0 sufficiently small, so in particular $\delta_0^{1/100} < \gamma_A$, Proposition 5.6 implies that w.h.p. there are certainly at least $\gamma_A n - o(n) \geq \delta_0^{1/100}n$ vertices which receive input A, which is clearly sufficient. □

Given a positive real number d and a probability distribution $\mathscr{D}$ on $\mathbb{N}_0^k$, we denote by $\mathscr{D}|_{\leq d}$ the probability distribution $\mathscr{D}$ conditioned on the event $\|\mathscr{D}\|_1 \leq d$. Recall that $P' := \phi_\varphi^{t_0-1}(Q_0)$, and recall also from Definition 2.3 that $\mathscr{M}(\mathscr{D}, \boldsymbol{q})$ is a random multiset of messages. With a slight abuse of notation, we will also use $\mathscr{M}(\mathscr{D}, \boldsymbol{q})$ to refer to the *distribution* of this random multiset.

[6] Note that error vertices include in particular those at which we deleted unmatched half-edges in Step 4 of the construction of $\hat{\mathbb{G}}_{t_0}$.

Proposition 7.6. *Whenever a standard vertex v is revealed in the marking process from a change of type $\boldsymbol{\sigma}_1$, the further changes made at outgoing half-edges at v have asymptotically the same distribution as in the branching process $\mathfrak{T}(\sigma_1, \tau_1, P')$ below a change of type $\boldsymbol{\sigma}_1$.*

Proof. First, we note that v is revealed in the marking process from a change of type $\boldsymbol{\sigma}_1$ so the vertex v has type $i := g_1(\sigma_1)$ and its parent (i.e its immediate predecessor in the branching process $\mathfrak{T}(\sigma_1, \tau_1, P')$) has type $j := g_2(\sigma_1)$. Now, given that v is a standard vertex , we may use $\hat{\mathbb{G}}_{t_0}$ instead of $\mathbb{G}_{t_0}$ to model it. Moreover, there are $\mathscr{Y}_{j,i}|_{\leq d_0}$ further half-edges at v. By Remark 2.15 and Markov's inequality, the event $\|\mathscr{Y}_{j,i}\|_1 \leq d_0$ is a high probability event. Thus, the distribution $\mathscr{Y}_{j,i}|_{\leq d_0}$ tends asymptotically to the distribution $\mathscr{Y}_{j,i}$. Furthermore, by Claim 4.1, each of these further half-edges has a t_0-in-message distributed according to P' independently. Since v was a new vertex, these in-messages have not changed, and therefore are simply distributed according to $\mathscr{M}(\mathscr{Y}_{j,i}, P'[i])$, as in $\mathfrak{T}(\sigma_0, \tau_0, P')$.

Note that in the idealised process $\mathfrak{T}(\sigma_0, \tau_0, P')$ we additionally condition on these incoming messages producing ξ_0, the appropriate message to the parent. In this case we do not know the message that v sent to its "parent", in the marking process. However, this message is distributed as $P'[i, j]$, and letting X denote a random variable distributed as $\mathscr{M}(\mathscr{Y}_{j,i}, \boldsymbol{q}_i)$, the probability that the multiset of incoming messages at v is A is simply

$$\mathbb{P}\left(P'[i,j] = \varphi(A)\right)\mathbb{P}\left(X = A \mid \varphi(X) = \varphi(A)\right).$$

Since P' is asymptotically close to the stable fixed point P, we have that $\mathbb{P}\left(P'[i,j] = \varphi(A)\right)$ is asymptotically close to $\mathbb{P}\left(\varphi(X) = \varphi(A)\right)$ for each A, and so the expression above can be approximated simply by $\mathbb{P}\left(\{X = A\} \cap \left\{\varphi(X) = \varphi(A)\right\}\right)$ $= \mathbb{P}(X = A)$, as required. □

7.3. **Three stopping conditions.** In order to prove Lemma 7.4, we introduce some stopping conditions on the marking process. More precisely, we will run the marking process until one of the following three conditions is satisfied.

(1) *Exhaustion* - the process has finished.
(2) *Expansion* - there exists some $\boldsymbol{\sigma}_1 = (\sigma_1, \tau_1) \in \Sigma^2$ such that at least $\delta_0^{3/5}\alpha_{\boldsymbol{\sigma}_1} n$ messages have changed from σ_1 to τ_1 (where $\boldsymbol{\alpha}$ is the vector from Corollary 7.2).
(3) *Explosion* - the number of spurious edges is at least $\delta_0^{2/3} n$.

Lemma 7.4 will follow if we can show that w.h.p. neither expansion nor explosion occurs.

7.3.1. *Explosion.*

Proposition 7.7. *W.h.p. explosion does not occur.*

We will split the proof up into three claims, dealing with the three different types of spurious edges.

Claim 7.8. *W.h.p., the number of defective edges is at most $\delta_0^{2/3} n/2$.*

Proof. A type-i vertex v of degree d will contribute d defective edges if it is chosen at least twice as the partner of a marked half-edge. Using Claim 7.5, at each step there are at least $\delta_0^{1/100} n$ possible half-edges to choose from, of which certainly at most d are incident to v, and thus the probability that v is chosen twice in the at most $\sqrt{\delta_0} n$ steps is at most

$$\left(\frac{d}{\delta_0^{1/100} n}\right)^2 \left(\sqrt{\delta_0} n\right)^2 = \delta_0^{49/50} d^2.$$

Thus setting S to be the number of defective edges and $c := \max_{i \in [k]} \mathbb{E}\left(\|\mathscr{Z}_i\|_1^3\right)$, we have

$$\begin{aligned}\mathbb{E}(S) \leq \sum_{i=1}^{k} \sum_{d=0}^{\infty} d\left(\mathbb{P}\left(\|\mathscr{Z}_i\|_1 = d\right) n_i\right) \delta_0^{49/50} d^2 &= \delta_0^{49/50} \sum_{i=1}^{k} n_i \sum_{d=0}^{\infty} d^3 \mathbb{P}\left(\|\mathscr{Z}_i\|_1 = d\right) \\ &\leq \delta_0^{49/50} \cdot \delta_0^{-1/100} n \cdot c \leq \delta_0^{4/5} n.\end{aligned}$$

On the other hand, if two distinct vertices have degrees d_1 and d_2, then the probability that both become snags may be estimated according to whether or not they are adjacent to each other, and is at most

$$\frac{d_1 d_2}{\delta_0^{1/100} n} \cdot \frac{d_1 d_2}{\left(\delta_0^{1/100} n\right)^3} \left(\sqrt{\delta_0} n\right)^3 + \frac{d_1^2 d_2^2}{\left(\delta_0^{1/100} n\right)^4} \left(\sqrt{\delta_0} n\right)^4 \leq 2 d_1^2 d_2^2 \delta_0^{24/25}.$$

Therefore we have

$$\begin{aligned}\mathbb{E}\left(S^2\right) &\le \mathbb{E}\left(S\right) + \sum_{i,j,\ell,m\in[k]} \sum_{d_1,d_2=0}^{\infty} d_1 d_2 \mathbb{P}\left(\left\|\mathscr{Y}_{j,i}\right\|_1 = d_1\right) n_i \cdot \mathbb{P}\left(\left\|\mathscr{Y}_{\ell,m}\right\|_1 = d_2\right) n_m \cdot 2d_1^2 d_2^2 \delta_0^{49/25} \\ &\le \delta_0^{4/5} n + 2\delta_0^{49/25} \max_{i,j\in[k]} \left(\mathbb{E}\left(\left\|\mathscr{Y}_{j,i}\right\|_1^3\right)\right)^2 \left(\delta_0^{-1/100} n\right)^2 \\ &\le \delta_0^{4/5} n + \delta_0^{48/25} n^2 \max_{i,j\in[k]} \left(\mathbb{E}\left(\left\|\mathscr{Y}_{j,i}\right\|_1^3\right)\right)^2 \le \delta_0^{9/5} n^2,\end{aligned}$$

where the last line follows due to Remark 2.15 for sufficiently small δ_0. Finally, Chebyshev's inequality shows that w.h.p. the number of spurious is at most $\delta_0^{2/3} n/2$, as claimed. □

Recall that $a_0 := \frac{\sqrt{c_0}}{4d_0|\Sigma|^{(t_0+2)d_0}}$.

Claim 7.9. *W.h.p. the number of erroneous edges is at most* $\frac{d_0 n}{\sqrt{a_0}}$.

Proof. Observe that Corollary 5.7 implies in particular that the number of edges of $\mathbb{G}_{t_0}$ which are attached to vertices of degree at most d_0 where the incoming message histories differ from those in $\hat{\mathbb{G}}_{t_0}$ (i.e. which would lead us to an error vertex if chosen) is at most $d_0 \frac{n}{a_0}$, and therefore the probability that we hit an error in any one step is at most $\frac{d_0 n/a_0}{\delta_0^{1/100} n} = \frac{1}{\delta_0^{1/100}(a_0/d_0)}$. Furthermore, any time we meet an error we obtain at most d_0 erroneous edges, and since the marking process proceeds for at most $\delta_0^{3/5} n$ steps, therefore the expected number of erroneous edges in total is at most

$$\delta_0^{3/5} n \cdot \frac{d_0}{\delta_0^{1/100}\left(a_0/d_0\right)} = \delta_0^{59/100} n \cdot \frac{d_0^2}{a_0}.$$

Now, by (**P3**), we have $c_0 \gg \exp\left(Cd_0\right) \gg d_0^6 |\Sigma|^{2(t_0+2)d_0}$ so $\sqrt{c_0} \gg d_0^3 |\Sigma|^{(t_0+2)d_0}$ which implies that $a_0 \gg d_0^2$. Thus, application of Markov's inequality completes the proof. □

Claim 7.10. *W.h.p.the number of faulty edges is at most* $\Delta_0 \frac{n}{\sqrt{c_0}}$.

Proof. This is similar to the proof of Claim 7.9. By assumption **A3**, w.h.p. there are no vertices of degree larger than Δ_0. Moreover, by Proposition 5.6, w.h.p. the number of edges adjacent to vertices of degree at least d_0 is at most n/c_0, so the probability of hitting a freak is at most $\frac{\Delta_0}{c_0}$. If we hit a freak, at most Δ_0 half-edges become faulty, therefore the expected number of faulty edges is $\delta_0^{3/5} n \cdot O\left(\Delta_0 \cdot \frac{\Delta_0}{c_0}\right) = O\left(\frac{\Delta_0^2 n}{c_0}\right)$. By **P3** we have $c_0 \gg \Delta^2$ so an application of Markov's inequality completes the proof. □

Combining all three cases we can prove Proposition 7.7.

Proof of Proposition 7.7. By Claims 7.8, 7.9 and 7.10, w.h.p. the total number of spurious edges is at most

$$\frac{\delta_0^{2/3} n}{2} + \frac{d_0 n}{\sqrt{a_0}} + \frac{\Delta_0 n}{\sqrt{c_0}}$$

Again, by (**P3**), we have $c_0 \gg \exp\left(Cd_0\right) \gg d_0^6 |\Sigma|^{2(t_0+2)d_0}$ and $c_0 \gg \Delta_0^2$. Thus, we have $\sqrt{a_0} \gg d_0$ and $\sqrt{c_0} \gg \Delta_0$. Hence,

$$\frac{\delta_0^{2/3} n}{2} + \frac{d_0 n}{\sqrt{a_0}} + \frac{\Delta_0 n}{\sqrt{c_0}} \le \delta_0^{2/3} n$$

as required. □

7.3.2. *Expansion.*

Proposition 7.11. *W.h.p. expansion does not occur.*

Proof. By Proposition 7.7, we may assume that explosion does not occur, so we have few spurious edges. Therefore in order to achieve expansion, at least $\frac{2}{3}\sqrt{\delta_0} n$ edges would have to be marked in the normal way, i.e. by being generated as part of a $\mathfrak{T}$ branching process rather than as one of the $\delta_0 n$ initial half-edges or as a result of hitting a snag.

However, we certainly reveal children in $\mathfrak{T}$ of at most $\delta_0^{3/5}\alpha_{\boldsymbol{\sigma}_2}n$ changes from σ_2 to τ_2, for each choice of $\boldsymbol{\sigma}_2 = (\sigma_2,\tau_2) \in \Sigma^2$, since at this point the expansion stopping condition would be applied. Thus the expected number of changes from σ_1 to τ_1 is at most

$$\sum_{\boldsymbol{\sigma}_2\in\Sigma} \delta_0^{3/5}\alpha_{\boldsymbol{\sigma}_2} n T_{\boldsymbol{\sigma}_1,\boldsymbol{\sigma}_2} = (T\alpha)_{\boldsymbol{\sigma}_1}\delta_0^{3/5}n \le (1-\gamma)\,\alpha_{\boldsymbol{\sigma}_1}\delta_0^{3/5}n.$$

We now aim to show that w.h.p. the actual number of changes is not much larger than this (upper bound on the) expectation, for which we use a second moment argument. Let us fix some $\boldsymbol{\sigma}_2 \in \Sigma^2$. For simplicity, we will assume for an upper bound that we reveal precisely $s := \delta_0^{3/5}\alpha_{\boldsymbol{\sigma}_2}n$ changes of type $\boldsymbol{\sigma}_2$ in $\mathfrak{T}$. Then the number of changes of type $\boldsymbol{\sigma}_1$ that arise from these is the sum of s independent and identically distributed integer-valued random variables $X_1,\dots,X_s$, where for each $r \in [s]$ we have $\mathbb{E}(X_r) = T_{\boldsymbol{\sigma}_1,\boldsymbol{\sigma}_2}$ and $\mathbb{E}\left(X_r^2\right) \le c := \max_{i,j\in[k]}\mathbb{E}\left(\left\|\mathscr{Y}_{j,i}\right\|_1^2\right)$. Therefore we have $\mathrm{Var}(X_r) \le c^2 = O(1)$, and the central limit theorem tells us that $\mathrm{Var}\left(\sum_{r=1}^s X_r\right) = O\left(\sqrt{s}\right)$. Then the Chernoff bound implies that w.h.p.

$$\left|\sum_{r=1}^s X_r - \mathbb{E}\left(\sum_{r=1}^s X_r\right)\right| \le n^{1/4}O\left(\sqrt{s}\right) = O\left(n^{3/4}\right) \le \frac{\gamma}{2}\delta_0^{3/5}T_{\boldsymbol{\sigma}_1,\boldsymbol{\sigma}_2}\alpha_{\boldsymbol{\sigma}_2}n.$$

Taking a union bound over all $|\Sigma|^4$ choices of $\boldsymbol{\sigma}_1,\boldsymbol{\sigma}_2$, we deduce that w.h.p. the total number of changes of type $\boldsymbol{\sigma}_1$ is at most

$$(1-\gamma)\,\alpha_{\boldsymbol{\sigma}_1}\delta_0^{3/5}n + \sum_{\boldsymbol{\sigma}_2}\frac{\gamma}{2}\delta_0^{3/5}T_{\boldsymbol{\sigma}_1,\boldsymbol{\sigma}_2}\alpha_{\boldsymbol{\sigma}_2}n = (1-\gamma/2)\,\alpha_{\boldsymbol{\sigma}_1}\delta_0^{3/5}n$$

for any choice of $\boldsymbol{\sigma}_1$, as required. □

7.3.3. *Exhaustion.*

Proof of Lemma 7.4. By Propositions 7.7 and 7.11, neither explosion nor expansion occurs. Thus the process finishes with exhaustion, and (using the fact that $\|\boldsymbol{\alpha}\|_1 = 1$) the total number of edges marked is at most

$$\sum_{\boldsymbol{\sigma}_1\in\Sigma^2}\delta_0^{3/5}\alpha_{\boldsymbol{\sigma}_1}n + \delta_0^{2/3}n = \left(\delta_0^{3/5}+\delta_0^{2/3}\right)n \le \sqrt{\delta_0}n$$

as required. □

7.4. **Proof of Theorem 1.3.** We can now complete the proof of our main theorem.

Proof of Theorem 1.3. Recall from Proposition 7.3 that edges on which messages change when moving from $\mathrm{WP}^{t_0}(\mathbb{G}_0)$ to $\mathrm{WP}^*(\mathbb{G}_0)$, which are simply those in the set $\mathscr{E}_{\mathrm{WP}}$, are contained in $\mathscr{E}_{\mathrm{mark}}$.

Furthermore, Lemma 7.4 states that $|\mathscr{E}_{\mathrm{mark}}| \le \sqrt{\delta_0}n$. Since we chose $\delta_0 \ll \delta$, the statement of Theorem 1.3 follows. □

8. Concluding remarks

We remark that in the definition of the $\hat{\mathbb{G}}_{t_0}$ model, rather than deleting unmatched half-edges, an alternative approach would be to condition on the event that the statistics match up in such a way that no half-edges need be deleted, i.e. such that the number of half-edges with t_0-in-story $\boldsymbol{\mu}_1$ and t_0-out-story $\boldsymbol{\mu}_2$ is identical to the number of half-edges with t_0-in-story $\boldsymbol{\mu}_2$ and t_0-out-story $\boldsymbol{\mu}_1$, while the number of half-edges with both t_0-in-story and t_0-out-story $\boldsymbol{\mu}$ is even. Subsequently one would need to show that this conditioning does not skew the distribution too much, for which it ultimately suffices to show that the event has a probability of at least $n^{-\Theta(1)}$.

In some ways this might even be considered the more natural approach, and indeed it was the approach we initially adopted in early versions of this paper. However, while the statement that the conditioning event is at least polynomially likely is an intuitively natural one when one considers that, heuristically, the number of half-edges with each story should be approximately normally distributed with standard deviation $O\left(\sqrt{n}\right)$, proving this formally is surprisingly delicate and involves some significant technical difficulties.

Since at other points in the proof we already need to deal with "errors", and unmatched half-edges can be handled as a subset of these, this approach turns out to be far simpler and more convenient.

9. Acknowledgement

We are very grateful to Amin Coja-Oghlan and Mihyun Kang for their helpful contributions to an earlier version of this project.

REFERENCES

[1] D. Achlioptas: Lower Bounds for Random 3-SAT via Differential Equations. Theoretical Computer Science **265** (2001) 159–185.
[2] D. Achlioptas, A. Coja-Oghlan: Algorithmic barriers from phase transitions. Proc. 49th FOCS (2008) 793–802.
[3] D. Achlioptas, M. Molloy: The solution space geometry of random linear equations. Random Structures and Algorithms **46** (2015) 197–231.
[4] A. Coja-Oghlan, O. Cooley, M. Kang, J. Lee, J. Ravelomanana: The sparse parity matrix. ArXiv 2107.06123
[5] A. Coja-Oghlan, O. Cooley, M. Kang, K. Skubch: Core forging and local limit theorems for the k-core of random graphs. J. Comb. Theory, Ser. B **137** (2019) 178–231.
[6] A. Coja-Oghlan, U. Feige, M. Krivelevich, D. Reichman: Contagious Sets in Expanders. Proc. 26th SODA (2015) 1953–1987.
[7] O. Cooley, M. Kang, J. Zalla: Loose cores and cycles in random hypergraphs. ArXiv 2101.05008.
[8] C. Cooper: The cores of random hypergraphs with a given degree sequence. Random Structures and Algorithms **25** (2004) 353–375.
[9] R. Darling, J. Norris: Differential equation approximations for Markov chains. Probability Surveys **5** (2008) 37–79.
[10] O. Dubois, J. Mandler: The 3-XORSAT threshold. Proc. 43rd FOCS (2002) 769–778.
[11] D. Fernholz, V. Ramachandran: The giant k-core of a random graph with a specified degree sequence. Manuscript (2003).
[12] D. Fernholz, V. Ramachandran: Cores and connectivity in sparse random graphs. UTCS Technical Report TR04-13 (2004).
[13] A. Frieze, S. Suen: Analysis of Two Simple Heuristics on a Random Instance of k-SAT. J. Algorithms **20** (1996) 312–355.
[14] R. Gallager: Low-density parity check codes. IRE Trans. Inform. Theory **8** (1962) 21–28.
[15] R. van der Hofstad: Random Graphs and Complex Networks. Volume 2. Manuscript, `https://www.win.tue.nl/~rhofstad/NotesRGCNII.pdf`
[16] M. Ibrahimi, Y. Kanoria, M. Kraning, A. Montanari: The set of solutions of random XORSAT formulae. Ann. Appl. Probab. **25** (2015) 2743–2808.
[17] S. Janson, M. Luczak: A simple solution to the k-core problem. Random Structures and Algorithms **30** (2007) 50–62.
[18] S. Janson, M. Luczak: Asymptotic normality of the k-core in random graphs. Ann. Appl. Probab. **18** (2008) 1085–1137.
[19] J.H. Kim: Poisson cloning model for random graphs. Proceedings of the International Congress of Mathematicians (2006) 873–897.
[20] M. Mézard, A. Montanari: Information, physics and computation. Oxford University Press 2009.
[21] M. Molloy: Cores in random hypergraphs and Boolean formulas. Random Structures and Algorithms **27** (2005) 124–135.
[22] M. Molloy: The freezing threshold for k-colourings of a random graph. J. ACM **65** (2018) #7.
[23] M. Molloy, R. Restrepo: Frozen variables in random boolean constraint satisfaction problems. Proc. 24th SODA (2013) 1306–1318.
[24] B. Pittel, J. Spencer, N. Wormald: Sudden emergence of a giant k-core in a random graph. Journal of Combinatorial Theory, Series B **67** (1996) 111–151
[25] T. Richardson, R. Urbanke: Modern coding theory. Cambridge University Press (2008).
[26] O. Riordan: The k-core and branching processes. Combinatorics, Probability and Computing **17** (2008) 111–136.
[27] K. Skubch: The core in random hypergraphs and local weak convergence. ArXiv 1511.02048.
[28] N. Wormald: Differential equations for random processes and random graphs. Ann. Appl. Probab. **5** (1995) 1217–1235.

OLIVER COOLEY, `cooley@math.tugraz.at`, GRAZ UNIVERSITY OF TECHNOLOGY, INSTITUTE OF DISCRETE MATHEMATICS, STEYRERGASSE 30, 8010 GRAZ, AUSTRIA

JOON LEE, `joon.lee@tu-dortmund.de`, TU DORTMUND, FAKULTÄT FÜR INFORMATIK, 12 OTTO-HAHN-STRASSE, DORTMUND, 44227, GERMANY.

JEAN RAVELOMANANA, `jean.ravelomanana@tu-dortmund.de`, TU DORTMUND, FAKULTÄT FÜR INFORMATIK, 12 OTTO-HAHN-STRASSE, DORTMUND, 44227, GERMANY.

C

THE SPARSE PARITY MATRIX

AMIN COJA-OGHLAN, OLIVER COOLEY, MIHYUN KANG, JOON LEE, JEAN BERNOULLI RAVELOMANANA

ABSTRACT. Let $\boldsymbol{A}$ be an $n\times n$-matrix over $\mathbb{F}_2$ whose every entry equals 1 with probability d/n independently for a fixed $d>0$. Draw a vector $\boldsymbol{y}$ randomly from the column space of $\boldsymbol{A}$. It is a simple observation that the entries of a random solution $\boldsymbol{x}$ to $\boldsymbol{A}x=\boldsymbol{y}$ are asymptotically pairwise independent, i.e., $\sum_{i<j}\mathbb{E}|\mathbb{P}[\boldsymbol{x}_i=s,\boldsymbol{x}_j=t\mid\boldsymbol{A}]-\mathbb{P}[\boldsymbol{x}_i=s\mid\boldsymbol{A}]\mathbb{P}[\boldsymbol{x}_j=t\mid\boldsymbol{A}]|=o(n^2)$ for $s,t\in\mathbb{F}_2$. But what can we say about the *overlap* of two random solutions $\boldsymbol{x},\boldsymbol{x}'$, defined as $n^{-1}\sum_{i=1}^n\mathbf{1}\{\boldsymbol{x}_i=\boldsymbol{x}'_i\}$? We prove that for $d<\mathrm{e}$ the overlap concentrates on a single deterministic value $\alpha_*(d)$. By contrast, for $d>\mathrm{e}$ the overlap concentrates on a single value once we condition on the matrix $\boldsymbol{A}$, while over the probability space of $\boldsymbol{A}$ its conditional expectation vacillates between two different values $\alpha_*(d)<\alpha^*(d)$, either of which occurs with probability $1/2+o(1)$. This anti-concentration result provides an instructive contribution to both the theory of random constraint satisfaction problems and of inference problems on random structures. *MSC:* 05C80, 60B20, 94B05

1. INTRODUCTION

1.1. **Motivation and background.** Sharp thresholds are the hallmark of probabilistic combinatorics. The classic, of course, is the giant component threshold, below which the random graph decomposes into many tiny components but above which a unique giant emerges [26]. Its (normalised) size concentrates on a deterministic value. Similarly, once the edge probability crosses a certain threshold the random graph contains a Hamilton cycle w.h.p., which fails to be present below that threshold [32]. Monotone properties quite generally exhibit sharp thresholds [27]. Only inside the critical windows of phase transitions are we accustomed to deviations from this zero/one behaviour [7].

In this paper we investigate the simplest conceivable model of a sparse random matrix. There is one single parameter, the density $d>0$ of non-zero entries. Specifically, we obtain the $n\times n$-matrix $\boldsymbol{A}=\boldsymbol{A}(n,p)$ over $\mathbb{F}_2$ by setting every entry to one with probability $p=(d/n)\wedge 1$ independently. Remarkably, this innocuous random matrix exhibits a critical behaviour, deviant from the usual zero–one law, for all d outside a small interval. The result has ramifications for random constraint satisfaction and statistical inference.

To begin with constraint satisfaction (we will turn to inference in Section 1.3), consider a random vector $\boldsymbol{y}$ from the column space of $\boldsymbol{A}$. The random linear system $\boldsymbol{A}x=\boldsymbol{y}$ constitutes a random constraint satisfaction problem par excellence. Its space of solutions is a natural object of study. In fact, the problem is reminiscent of the intensely studied random k-XORSAT problem, where we ask for solutions to a Boolean formula whose clauses are XORs of k random literals [2, 10, 25, 23, 29, 35, 42]. Random k-XORSAT is equivalent to a random linear system over $\mathbb{F}_2$ whose every row contains precisely k ones.

The most prominent feature of random k-XORSAT is its sharp satisfiability threshold. Specifically, for any $k\geq 3$ there exists a critical value of the number of clauses up to which the random k-XORSAT formula possesses a solution, while for higher number of clauses no solution exists w.h.p. [23, 25, 42]. The satisfiability threshold is strictly smaller than the obvious point where the corresponding $\mathbb{F}_2$-matrix cannot have full row rank anymore because there are more rows than columns. Instead, the satisfiability threshold coincides with the threshold where due to long-range effects a linear number of variables *freeze*, i.e., are forced to take the same value in all solutions. Clearly, once an extensive number variables freeze, additional random constraints are apt to cause conflicts.

The precise freezing threshold can be characterised in terms of the 2-core of the random hypergraph underlying the k-XORSAT formula. We recall that the 2-core is what remains after recursively deleting variables of degree at most one along with the constraint that binds them (if any). If the 2-core is non-empty, then its constraints are more tightly interlocked than those of the original problem, which, depending on the precise numbers, may cause freezing. Indeed, the precise number of frozen variables can be calculated by way of a message passing process called Warning Propagation [29, 34]. The number of frozen variables concentrates on a deterministic value that

Amin Coja-Oghlan and Jean B. Ravelomanana are supported by DFG CO 646/4.
Oliver Cooley and Mihyun Kang are supported by Austrian Science Fund (FWF): I3747.

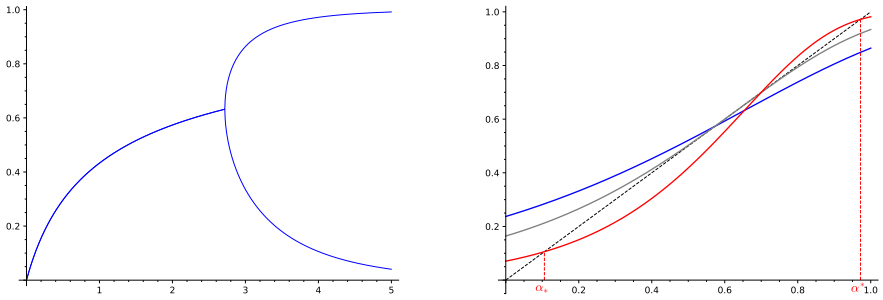

FIGURE 1. Left: the two fixed points $\alpha_* = \alpha_*(d)$ and $\alpha^* = \alpha^*(d)$ of ϕ_d. Right: the function ϕ_d for $d = 2.5$ (blue) possesses a unique fixed point, while for $d = 3$ (red) there are two stable fixed points and an unstable one in between.

comes out in terms of a fixed point problem. Although the k-XORSAT problem is conceptually far simpler than, say, the k-SAT problem, freezing plays a pivotal role in basically all other random constraint satisfaction problems as well [1, 24, 33, 34, 37, 39].

Surprisingly, our linear system $\boldsymbol{A}x = \boldsymbol{y}$ behaves totally differently as two competing combinatorial forces of exactly equal strength engage in a tug of war. As a result, for densities $d > \mathrm{e}$ the fraction of frozen variables fails to concentrate on a single value. Instead, that number and, in effect, the geometry of the solution space vacillate between two very different scenarios that both materialise with asymptotically equal probability. In other words, the model perennially remains in a critical state for all $d > \mathrm{e}$. Let us proceed to formulate the result precisely, and to understand how it comes about.

1.2. **Frozen variables.** One of the two forces resembles the emergence of the 2-core in random k-XORSAT. Indeed, we could run the process of peeling variables appearing in at most one equation of the linear system $\boldsymbol{A}x = \boldsymbol{y}$ as well. The size of the 2-core and the total number of coordinates that would freeze if the entire 2-core were to freeze can be calculated. Specifically, let

$$\phi_d : [0,1] \to [0,1], \qquad \alpha \mapsto 1 - \exp\left(-d\exp\left(-d(1-\alpha)\right)\right) \tag{1.1}$$

and let $\alpha^* = \alpha^*(d)$ be its *largest* fixed point. According to the "2-core heuristic", the number of frozen coordinates x_i comes to about $\alpha^* n$. A proof that w.h.p. precisely this many variables freeze (or actually a more general statement) has been posed as an exercise [34]. But as we shall see momentarily, this conclusion is erroneous.

For on the other hand we could trace the number of variables that freeze because of unary equations. Indeed, because the number of ones in a row of $\boldsymbol{A}$ has distribution $\mathrm{Po}(d)$, about $d\mathrm{e}^{-d}n$ equations contain just one variable. Naturally, each such variable freezes. Substituting these frozen values into the other equations likely produces more equations of degree one, etc. Interestingly enough, the number of frozen variables that this "unary equations heuristic" predicts equals $\alpha_* n$, with α_* the *least* fixed point of ϕ_d. While for $d < \mathrm{e}$ there is a unique fixed point and thus $\alpha_* = \alpha^*$, for $d > \mathrm{e}$ the two fixed points α_*, α^* are distinct. Indeed, apart from α_*, α^*, which are stable fixed points, there occurs a third unstable fixed point $\alpha_* < \alpha_0 < \alpha^*$; see Figure 1.

Which one of these heuristics provides the right answer? To find out we could try to assess the total number of solutions that the linear system $\boldsymbol{A}x = \boldsymbol{y}$ should possess according to either prediction. Indeed, [15, Theorem 1.1] yields an asymptotic formula for the number of solutions to a sparse random linear system in terms of a parameter α that, at least heuristically, should equal the fraction of frozen variables. For the random matrix $\boldsymbol{A}$ the formula shows that, in probability,

$$\lim_{n\to\infty}\frac{\mathrm{nul}\,\boldsymbol{A}}{n} = \max_{\alpha\in[0,1]}\Phi_d(\alpha), \quad \text{where} \quad \Phi_d(\alpha) = \exp\left(-d\exp(-d(1-\alpha))\right) + (1+d(1-\alpha))\exp(-d(1-\alpha)) - 1 \tag{1.2}$$

and where $\mathrm{nul}\,\boldsymbol{A}$ denotes the nullity, i.e. the dimension of the kernel, of $\boldsymbol{A}$. Hence, the correct answer should be the value $\alpha \in \{\alpha_*, \alpha^*\}$ that maximises Φ_d. But it turns out that $\Phi_d(\alpha_*) = \Phi_d(\alpha^*)$ for all $d > 0$. Accordingly, the main theorem shows that both predictions α_* and α^* are correct, or more precisely each of them is correct about half of the time. Formally, let

$$f(\boldsymbol{A}) = |\{i \in [n] : \forall x \in \ker \boldsymbol{A} : x_i = 0\}| \,/\, n$$

be the fraction of frozen variables.

Theorem 1.1. *(i) For $d \le \mathrm{e}$ the function ϕ_d has a unique fixed point and*

$$\lim_{n\to\infty} f(\boldsymbol{A}) = \alpha_* = \alpha^* \qquad \text{in probability.}$$

(ii) For $d > \mathrm{e}$ we have $\alpha_* < \alpha^*$ and for all $\varepsilon > 0$,

$$\lim_{n\to\infty} \mathbb{P}\left[|f(\boldsymbol{A}) - \alpha_*| < \varepsilon\right] = \lim_{n\to\infty} \mathbb{P}\left[|f(\boldsymbol{A}) - \alpha^*| < \varepsilon\right] = \frac{1}{2}.$$

Hence, the fraction of frozen variables fails to exhibit a zero–one behaviour for $d > \mathrm{e}$. Instead, it shows a critical behaviour as one would normally associate only with the critical window of a phase transition.

1.3. **The overlap.** Apart from considering the linear system $\boldsymbol{A}x = \boldsymbol{y}$ as a random constraint satisfaction problem, the random linear system can also be viewed as an inference problem. Indeed, we can think of the vector $\boldsymbol{y}$, which is chosen randomly from the column space of $\boldsymbol{A}$, as actually resulting from multiplying $\boldsymbol{A}$ with a uniformly random vector $\hat{\boldsymbol{x}} \in \mathbb{F}_2^n$. Then $\boldsymbol{y} = \boldsymbol{A}\hat{\boldsymbol{x}}$ turns into a noisy observation of the 'ground truth' $\hat{\boldsymbol{x}}$. Thus, it is natural to ask how well we can learn $\hat{\boldsymbol{x}}$ given $\boldsymbol{A}$ and $\boldsymbol{y}$.

These two viewpoints are actually equivalent because the posterior of $\hat{\boldsymbol{x}}$ given $(\boldsymbol{A}, \boldsymbol{y})$ is nothing but the uniform distribution on the set of solutions to the linear system $\boldsymbol{A}x = \boldsymbol{y}$. Hence,

$$\mathbb{P}\left[\hat{\boldsymbol{x}} = x \mid \boldsymbol{A}, \boldsymbol{y}\right] = \frac{\mathbf{1}\left\{\boldsymbol{A}x = \boldsymbol{y}\right\}}{|\ker \boldsymbol{A}|} \qquad (x \in \mathbb{F}_2^n). \tag{1.3}$$

Therefore, the optimal inference algorithm just draws a random solution $\boldsymbol{x}$ from among all solutions to the linear system. The number of bits that this algorithm recovers correctly reads

$$R(\boldsymbol{x}, \hat{\boldsymbol{x}}) = \frac{1}{n}\sum_{i=1}^{n} \mathbf{1}\left\{\boldsymbol{x}_i = \hat{\boldsymbol{x}}_i\right\}.$$

Adopting mathematical physics jargon, we call $R(\boldsymbol{x}, \hat{\boldsymbol{x}})$ the *overlap* of $\boldsymbol{x}, \hat{\boldsymbol{x}}$. Its average given $\boldsymbol{A}, \boldsymbol{y}$ boils down to

$$\bar{R}(\boldsymbol{A}) = \mathbb{E}[R(\boldsymbol{x}, \hat{\boldsymbol{x}}) \mid \boldsymbol{A}, \boldsymbol{y}] = \frac{1}{|\ker \boldsymbol{A}|^2} \sum_{x, x' \in \ker \boldsymbol{A}} R(x, x'),$$

which is independent of $\boldsymbol{y}$.

Conceived wisdom in the statistical physics-inspired study of inference problems holds that the overlap concentrates on a single value given the 'disorder', in our case $(\boldsymbol{A}, \boldsymbol{y})$ (see [44]). This property is called *replica symmetry*. We will verify that replica symmetry holds for the random linear system w.h.p. Additionally, in all the random inference problems that have been studied over the past 20 years the overlap concentrates on a single value that does not depend on the disorder, except perhaps at a few critical values of the model parameters where phase transitions occur [6]. This enhanced property is called *strong replica symmetry*. A natural question is whether strong replica symmetry holds universally. It does not. As the next theorem shows, the random linear system with $d > \mathrm{e}$ provides a counterexample: it is replica symmetric, but not strongly so.

Theorem 1.2. *(i) If $d < \mathrm{e}$ then $\lim_{n\to\infty} R(\boldsymbol{x}, \hat{\boldsymbol{x}}) = (1 + \alpha_*)/2$ in probability.*
(ii) For all $d > \mathrm{e}$ we have $\lim_{n\to\infty} \mathbb{E}\left|R(\boldsymbol{x}, \hat{\boldsymbol{x}}) - \bar{R}(\boldsymbol{A})\right| = 0$ while

$$\lim_{n\to\infty} \mathbb{P}\left[\left|\bar{R}(\boldsymbol{A}) - \frac{1+\alpha_*}{2}\right| < \varepsilon\right] = \lim_{n\to\infty} \mathbb{P}\left[\left|\bar{R}(\boldsymbol{A}) - \frac{1+\alpha^*}{2}\right| < \varepsilon\right] = \frac{1}{2} \qquad \text{for any } \varepsilon > 0.$$

The first part of the theorem posits that for $d < \mathrm{e}$ the overlap concentrates on the single value$(1 + \alpha_*)/2$. In light of Theorem 1.1 this means that the optimal inference algorithm, while, unsurprisingly, capable of correctly recovering the frozen coordinates, is at a loss when it comes to the unfrozen ones. Indeed, we can get only about half the unfrozen coordinates right, no better than a random guess.

The second part of the theorem is more interesting. While the random variable $R(\boldsymbol{x}, \hat{\boldsymbol{x}})$ concentrates on the conditional expectation $\bar{R}(\boldsymbol{A})$ given $\boldsymbol{A}, \boldsymbol{y}$, the conditional expectation $\bar{R}(\boldsymbol{A})$ itself fails to concentrate on its mean $\mathbb{E}[\bar{R}(\boldsymbol{A})]$. Instead it vacillates between two different values $(1 + \alpha_*)/2$ and $(1 + \alpha^*)/2$, each of which occurs with asymptotically equal probability. In fact, this failure to concentrate does not just occur at a few isolated points, but throughout the entire regime $d > \mathrm{e}$. This behaviour mirrors the anti-concentration of the number of frozen variables from Theorem 1.1. Moreover, as in the case $d < \mathrm{e}$ the optimal inference algorithm does, of course, correctly recover the frozen variables, but cannot outperform a random guess on the unfrozen ones.

We proceed to outline the key ideas behind the proofs of Theorems 1.1 and 1.2. Unsurprisingly, to prove the critical behaviour that these theorems assert we will need to conduct a rather subtle, accurate analysis of the random linear system and its space of solutions, far more so than one would normally have to undertake when aiming at a zero-one result. On the positive side the proofs reveal novel combinatorial insights that may have an impact on other random constraint satisfaction or inference problems as well. Let us thus survey the proof strategy.

1.4. **Techniques.** The main result of the paper is that for $d > \mathrm{e}$ the proportion $f(\boldsymbol{A})$ of frozen variables is asymptotically equal to either of the two stable fixed points α_*, α^* of the function ϕ_d with probability $1/2 + o(1)$ (see Figure 1). Proving this statement takes three strikes.

FIX: $f(\boldsymbol{A})$ concentrates on the fixed points of ϕ_d, either one of the two stable ones α_*, α^* or the third unstable fixed point α_0.
STAB: The unstable fixed point is an unlikely outcome.
EQ: The two stable fixed points are equally likely.

1.4.1. *Heuristics.* Why are these three statements plausibly true? Let us begin with **FIX**. The random matrix $\boldsymbol{A}$ naturally induces a bipartite graph called the *Tanner graph* $G(\boldsymbol{A})$. Its vertex classes are *variable nodes* $v_1, \ldots, v_n$ representing the columns of $\boldsymbol{A}$ and *check nodes* $a_1, \ldots, a_n$ representing the rows. There is an edge between a_i and v_j iff $\boldsymbol{A}_{ij} = 1$. The Tanner graph is distributed as a random bipartite graph with edge probability d/n. As a consequence, its local structure is roughly that of a $\mathrm{Po}(d)$ Galton-Watson tree.

Exploring the Tanner graph from a given variable node v_i, we may view v_i as the root of such a tree. The grandchildren of v_i, i.e. the variable nodes at distance two, are essentially uniformly random. Therefore, the grandchildren should each be frozen with probability $f(\boldsymbol{A}) + o(1)$ and behave very nearly independently. Further, for the obvious algebraic reason the root v_i itself is frozen iff it is parent to some check all of whose children are frozen. A few lines of calculations based on the Poisson tree structure then show that v_i ought to be frozen with probability $\phi_d(f(\boldsymbol{A}))$. But at the same time, since v_i was itself chosen randomly, it is frozen with probability $f(\boldsymbol{A})$. Hence, we are led to expect that $f(\boldsymbol{A}) = \phi_d(f(\boldsymbol{A}))$. In other words, **FIX** expresses that the local structure of $G(\boldsymbol{A})$ is given by a Poisson tree, and that freezing manifests itself locally.

Apart from the two stable fixed points α_*, α^*, Figure 1 indicates that ϕ_d possesses an unstable fixed point α_0 somewhere in between. How can we rule out that $f(\boldsymbol{A})$ will take this value? The nullity formula (1.2) suggests that $f(\boldsymbol{A})$ should be a *maximiser* of the function $\Phi_d(\alpha)$. But its maximisers are precisely the *stable* fixed points α_*, α^*, while the unstable fixed point is where the function takes its local minimum. That is why **STAB** appears plausible. However, we will see that this simplistic line of reasoning cannot be turned into a proof easily.

Finally, coming to **EQ**, we need to argue that for $d > \mathrm{e}$ both stable fixed points are equally likely. To this end we employ the Warning Propagation (WP) message passing scheme, where messages are sent along the edges of the Tanner graph in either direction. The message from v_j to a_i is updated at each time step according to the messages that v_j receives from its other neighbours, and similarly for the reverse message. WP does faithfully describe the local dynamics that cause freezing, but there remains a loose end: we must initialise messages somehow.

Two obvious initialisations suggest themselves. First, if we initialise assuming everything to be unfrozen, then because of **FIX** and the local geometry approximating a Galton-Watson branching tree, WP reduces to repeated application of the ϕ_d function starting from 0. Since $\lim_{t\to\infty} \phi_d^{\circ t}(0) = \alpha_*$, WP then predicts $f(\boldsymbol{A}) = \alpha_*$. Second, if we initialise assuming everything to be frozen, WP mimics iterating ϕ_d from 1 and thus predicts $f(\boldsymbol{A}) = \lim_{t\to\infty} \phi_d^{\circ t}(1) = \alpha^*$.

So which initialisation is correct? Neither, unfortunately. We thus need a more nuanced version of WP, in which we describe messages and ultimately variables as "frozen", "unfrozen" and "slush", the last meaning uncertain. Initialising WP with either all messages frozen or all messages unfrozen still leads to the same results as before. But initialising with all messages being "slush", WP predicts that approximately $\alpha_* n$ variables are frozen, $(1-\alpha^*)n$ variables are unfrozen, and $(\alpha^* - \alpha_*)n$ variables remain slush. Thus, there are actually *three* distinct categories.

How does this help? Since $f(\boldsymbol{A})$ is concentrated around the stable fixed points α_*, α^*, we know that actually the slush portion must be either (almost) entirely frozen or unfrozen; it is impossible that, say, half the slush variables freeze. To figure out whether the slush freezes, consider the minor $\boldsymbol{A}_{\mathtt{s}}$ of $\boldsymbol{A}$ induced on the corresponding variables and constraints. If this minor has fewer rows than columns, then the corresponding linear system is under-constrained. In effect, it is inconceivable that the slush freezes completely. On the other hand, if $\boldsymbol{A}_{\mathtt{s}}$ has more rows than columns, then by analogy to the random k-XORSAT problem we expect that the slush freezes.

Now, crucially, both the random matrix model $\boldsymbol{A}$ and the WP message passing process are invariant under transposition of the matrix. Hence, $\boldsymbol{A}_{\mathtt{s}}$ should be over-constrained just as often as it is under-constrained. We are thus led to believe that the slush freezes with probability about half, which explains the peculiar behaviour stated in the theorems. Once again, this simple reasoning, while plausible, cannot easily be converted into an actual proof.

1.4.2. *Formalising the heuristics.* Hence, how can we corroborate these heuristics rigorously? Concerning **FIX**, consider the following game of "thimblerig". The opponent generates two random graphs independently: one is simply the Tanner graph $G_1 \sim G(\boldsymbol{A})$ of $\boldsymbol{A}$, the other is an independent copy $G_2 \sim G(\boldsymbol{A})$ of the Tanner graph, but with some random alterations. Specifically, the trickster generates a $\mathrm{Po}(d)$ branching tree of height two, embeds the root and its children onto isolated variable and check nodes respectively, and embeds the remaining leaves onto variables chosen uniformly at random. The opponent then presents you with the two graphs and asks you to determine which is which. It turns out that the changes are so well-disguised that you can do no better than a random guess. To compound your misery, having told you which is the perturbed graph, your opponent asks you to guess which variable is the root of the added tree. Again, the changes are so well-disguised that you can do no better than a random guess. Not content with winning twice, your opponent wishes to assert their complete dominance and performs the same trick again, this time adding not just one tree but a slowly growing number (of order $o(\sqrt{n})$). For the third time, you can only resort to a random guess.

The point of this game is to demonstrate that the root variables of the trees added behave identically to randomly chosen variables of the original graph. In particular, the proportion of variables which are frozen is distributed as $f(\boldsymbol{A})$. But we can also calculate this proportion in a different way: by considering whether the *attachment* variables are frozen and tracking the effects down to the roots. This tells us that the proportion of frozen roots is $\phi_d(f(\boldsymbol{A}) + o(1))$, *provided that* the newly added constraints do not dramatically shift the overall number of frozen variables due to long-range effects. To rule this out we use a delicate argument drawing on ideas from the study of random factor graph models and involving replica symmetry and the cut metric for discrete probability distributions from [5, 14, 17, 18, 19].

Perhaps surprisingly, it takes quite an effort to verify the claim **STAB** that $f(\boldsymbol{A})$ is not likely to be near the unstable fixed point. The proof employs a combinatorial construction that we call *covers*. A cover is basically a designation of the variable nodes, checks and edges of the Tanner graph that encodes which variables are frozen, and because of which constraints they freeze. We will then pursue a novel "hammer and anvil" strategy to rule out the unstable fixed point. On the one hand, we will show that if $f(\boldsymbol{A})$ is near α_0, then the Tanner graph $G(\boldsymbol{A})$ must contain covers that each induce a cluster of solutions with about α_0 frozen variables. On the other hand, we will use a moment computation to show that w.h.p. the Tanner graph $G(\boldsymbol{A})$ only contains a sub-exponential number $\exp(o(n))$ of covers. Furthermore, another moment computation shows that w.h.p. each of them only extends to about $2^{\Phi_d(\alpha_0)n}$ solutions to the linear system $\boldsymbol{A}x = \boldsymbol{y}$. As a consequence, if $f(\boldsymbol{A})$ is near α_0, then the random linear system $\boldsymbol{A}x = \boldsymbol{y}$ would have far fewer solutions than provided by (1.2). Since the nullity of the random matrix is tightly concentrated, we conclude that the event $f(\boldsymbol{A}) \sim \alpha_0$ is unlikely. The novelty of this argument, and the source of its technical intricacy, is the two-step cover–solution consideration: first we verify that the set of solutions actually decomposes into clusters encoded by "covers". Then we calculate the number of covers (corresponding to solution clusters), and finally we estimate the number of solutions inside each cluster. This two-level approach is necessary as a direct first moment calculation of the expected number of solutions with a given Hamming weight seems doomed to fail, at least for d near the critical value e.

Coming to **EQ**, as indicated in the previous subsection, the "slush" portion of the matrix enjoys a symmetry property, in that it is also the slush portion of the transposed matrix. We will prove that, depending on the precise aspect ratio of the slush minor, the slush variables either do or do not freeze. But there is one subtlety: we need to to show that the number of rows and the number of columns are not *exactly* equal w.h.p. Indeed it is not hard to show that the both numbers have standard deviation $\Theta(\sqrt{n})$. Hence, if they were independent they would differ by $\Theta(\sqrt{n})$ w.h.p.. But this independence is quite clearly not satisfied. Thus, we need to argue that at least they have non-trivial covariance.

To show this, we perform a similar trick to the game of thimblerig: we show that the matrix can be randomly perturbed to decrease the number of slush columns, while preserving the number of slush rows. Furthermore, this can be achieved without an opponent being able to identify that a change has been made. Performing this trick carefully shows that it is unlikely that the slush portion of the matrix is approximately square. Symmetry then tells

us that with probability asymptotically 1/2 it has significantly more rows than columns, and also with probability asymptotically 1/2 it has significantly more columns than rows.

It remains to prove that these two cases are likely to lead to all slush variables being frozen, or all being unfrozen respectively. Unfortunately, a simple symmetry argument does not quite suffice. Instead we first prove that it is unlikely that there are significantly, say $\omega \gg 1$, more slush variables than slush checks, but that almost all slush variables are frozen. The number of slush variables that remain unfrozen must certainly be at least ω due to elementary consideration of the nullity. We are thus left to exclude that the number is between ω and εn, which we establish by way of an expansion argument.

We finally need to show that it is unlikely that there are significantly more slush checks (say $m_{\mathtt{s}}$) than slush variables ($n_{\mathtt{s}}$), but that these slush variables remain mostly unfrozen. Crucially, thanks to replica symmetry and the cut metric we can indeed show that a "typical" kernel vector will set approximately half of the slush variables to 1 and half to 0. Of course there are approximately $2^{n_{\mathtt{s}}}$ such vectors. On the other hand, imagine that a check with k slush variable neighbours chooses these neighbours uniformly at random (this can be made formally correct by conditioning on the degree distribution and using the configuration model). Then the probability that this check is satisfied by a vector of Hamming weight approximately $n_{\mathtt{s}}/2$ is approximately 1/2 (since e.g. based on the values of the first $k-1$ neighbours, the last must be chosen from the correct class). Therefore the expected number of kernel vectors should be approximately $2^{n_{\mathtt{s}}-m_{\mathtt{s}}} = o(1)$.

The problem with this basic calculation is that error terms occur which turn out to be too significant to ignore. These error terms ultimately come from check nodes of degree two in the slush minor. To deal with them, we employ a delicate percolation argument in which we contract check nodes of degree exactly two, since they just equalise their two adjacent variable nodes. Importantly, we can show that this process neither affects the number of kernel vectors nor the balance $m_{\mathtt{s}} - n_{\mathtt{s}}$. We can thus complete the moment calculation and show that the slush cannot have an excess of rows and still be entirely unfrozen.

1.5. **Discussion.** How do the techniques that we develop in this paper compare to previously known ones, and how can our techniques be extended to other problems?

The general Warning Propagation message passing scheme captures the local effects of constraint satisfaction problems; for example, in the context of satisfiability WP boils down to Unit Clause Propagation [34]. WP also yields the k-XORSAT threshold [29] as well as the freezing threshold in random graph colouring [37]. In addition, WP can also be used to study structural graph properties such as the k-core [12, 41]. In all these examples, the "correct" initialisation from which to launch WP is obvious, and the proof that random variable of interest converges to the fixed point is based on a direct and straightforward combinatorial analysis. Indeed, the standard strategy is then a two-stage one: first, show that WP quickly converges to something close to the conjectured limit; and second, show that after this initial convergence, not much else will change [11, 21].

However, this usual technique is not enough for our purposes, essentially because of the 2-point rather than 1-point concentration of $f(\boldsymbol{A})$. Naively one might imagine that WP will converge to one of the two fixed points, each with probability 1/2. But intriguingly, the dichotomy of the random variable $f(\boldsymbol{A})$ induces a dichotomy for WP in each *instance* of $\boldsymbol{A}$ – WP hedges its bets, identifying the two possible answers, but is unable to tell which is actually correct. As such, we are left with the "uncertain" portion of the matrix (or its Tanner graph).

To deal with this complication we enhance the WP message passing scheme to expressly identify the portion of the Tanner graph that may go either way. Along the way, we develop a versatile *indirect* method for proving convergence to *some* fixed point to replace the usual direct combinatorial argument. This technique is based on the thimblerig game that more or less justifies the WP heuristic in general. While the argument appears to be reasonably universal, it fails to identify precisely which fixed point is the correct one. As mentioned above, we follow WP up with a novel type of moment calculation based on covers to rule out the unstable fixed point. One could envisage a generalisation of this technique to other planted constraint satisfaction problems or, more generally, spin glass models. The place of the nullity formula (1.2) would then have to be filled by a formula for the leading exponential order of the partition function.

The thimblerig argument is enabled by the important observation that unfrozen variables, for the most part, behave more or less independently of each other and that the random variable $f(\boldsymbol{A})$ is fairly "robust" with respect to small numbers of local changes (see Proposition 2.9). We establish this robustness by way of a pinning argument, in which unary checks are added that freeze certain previously unfrozen variables, and we analyse the effect that

this has on the kernel. The thimblerig argument is an extension of arguments used in the study of random factor graph models [18, 19, 40], where the pinning operation also plays a crucial role [16, 17].

Because the slush minor of the matrix displays a peculiar critical phenomenon, such as one would normally associate only with critical regimes around a phase transition, new techniques are required to study it. In particular, while it seems intuitively natural that the uncertain proportion is unfrozen if $n_{\mathtt{s}} - m_{\mathtt{s}} \geq \omega$ is large and positive, but frozen if it is large and negative, proving this formally requires some significant new ideas. In particular, to prove the first statement we introduce *flippers*, induced subgraphs of the uncertain portion which could confound expectations by being frozen. These flippers must satisfy various properties, and the proof consists of showing that large flippers (or more precisely, large unions of flippers) are unlikely due to expansion properties. This sort of expansion argument appears by no means restricted to the present problem. A related combinatorial structure appeared in the proof of limit theorems for cores of random graphs [13].

Proving the second statement involves a delicate moment calculation. The modification involved in contracting the checks of degree 2, which are the reason that the naive version of the argument fails, is similar to the operation to construct the kernel of a graph from its 2-core. This moment calculation is the single place where we make critical use of the fact that we are studying a problem whose variables range over a finite domain, viz. the field $\mathbb{F}_2$.

What are potential generalisations? The random linear system $\boldsymbol{A}x = \boldsymbol{y}$ is one case of a class of constraint satisfaction problems known as *uniquely extendable problems* [20]. Such problems are characterised by the property that if all but one of the variables appearing in a constraint are fixed, there is precisely one choice for the value of the remaining variable such that the constraint is satisfied. Some of these problems are intractable, such as, for example, algebraic constraints with variables ranging over finite groups. It would be most interesting to see if and how the methods developed in this paper could be extended to uniquely extendable problems. Furthermore, since we study a critical phenomenon, namely the two-point concentration of the proportion of frozen variables, our ideas may help to understand the behaviour at the critical point of phase transitions of random constraint satisfaction problems. This type of question remains an essentially blank spot on the map.

1.6. **Further related work.** Perhaps surprisingly, apart from the article [15] that establishes a nullity formula for general sparse random matrices and in particular (1.2), there have been no prior studies of the random matrix $\boldsymbol{A}(n,p)$. However, random $m \times n$-matrix over finite fields $\mathbb{F}_q$ where every row contains an equal number $k \geq 2$ of non-zero entries have been studied extensively. In the case $k = q = 2$ this model is directly related to the giant component phase transition [30, 31], because each row constrains two random entries to be equal. Moreover, we already saw that for $k \geq 3$ and $q = 2$ the model is equivalent to random k-XORSAT. Dubois and Mandler [25] computed the critical aspect ratio m/n up to which such a matrix has full row rank for $k = 3$. The result was subsequently extended to $k > 3$ [23, 42]. Indeed, the threshold value of m up to which the random matrix has full rank can be interpreted in terms of the Warning Propagation message passing scheme [10]. Beyond its intrinsic interest as a basic model of a random constraint satisfaction problem [34], the random k-XORSAT model has found applications in hashing and data compression [23, 43].

The asymptotic rank of random matrices with a fixed number k of non-zero entries per row over finite fields has been computed independently via two different arguments by Ayre, Coja-Oghlan, Gao and Müller [3] and Cooper, Frieze and Pegden [22]. Additionally, Miller and Cohen [36] studied the rank of random matrices in which both the number of non-zero entries in each row and the number of non-zero entries in each column are fixed. However, they left out the critical case in which these two numbers are identical, which was solved recently by Huang [28]. Additionally, Bordenave, Lelarge and Salez [8] studied the rank over $\mathbb{R}$ of the adjacency matrix of sparse random graphs. Of course, a crucial difference between the random matrix model that we study here and the adjacency matrix of a random graph is that the latter is symmetric.

A problem that appears to be inherently related to the binomial random matrix problem studied here is the matching problem on random bipartite graphs [9]. It would be interesting to see if in some form the criticality observed in Theorems 1.1 and 1.2 extends to the matching problem or, equivalently, the independent set problem on random bipartite graphs. The critical value $d = \mathrm{e}$ appears to be related to the uniqueness of the Gibbs measure of the latter problem [4]. In the context of the matching problem, our function $\Phi_d(\alpha)$ appears (as $F(1-\alpha)$) in [9], in particular in the appendix where a figure shows the emergence of the two global maxima above the threshold $d = \mathrm{e}$. (In fact the discussion there is about the one-type graph $G(n, d/n)$ rather than the bipartite $G(n, n, d/n)$, which is the distribution of $G(\boldsymbol{A})$, but since the two graphs have the same local weak limit the more general results of [9] show that the matching problem displays similar behaviour.) In some sense it is not surprising that the same

function should arise in these two problems: the Warning propagation process to determine which variables are certainly frozen in essence mimics a one-sided version of the first stage of the Karp-Sipser algorithm in which leaves and their neighbours are removed. This removal results in a remaining "core", similar to our "slush", of minimum degree at least 2. This is where we encounter our first fixed point of ϕ_d (or maximum of Φ_d). For the matching problem, this first roadblock is easy to overcome: the core turns out to have an almost perfect matching w.h.p., which implies that it is always the same fixed point which gives the correct answer. By contrast, our situation is more delicate because the slush need not freeze.

2. Organisation

In this section, we state the intermediate results that lead up to the main theorems. We also detail where in the following sections the proofs of these intermediate results can be found.

2.1. **The functions ϕ_d and Φ_d.** The formula (1.2) yields the approximate number of solutions to the linear system $\boldsymbol{A}x = \boldsymbol{y}$. We already discussed the combinatorial intuition behind the maximiser α in (1.2): we will prove that the function Φ_d attains its global maxima at the conceivable values of $f(\boldsymbol{A})$. However, the proof of (1.2) in [15] falls short of already implying this fact as that proof strategy relies on a purely variational argument. For a start, we verify that the function ϕ_d actually has a unique fixed point for $d \le \mathrm{e}$ and two distinct stable fixed points for $d > \mathrm{e}$, and that these fixed points coincide with the local maxima of Φ_d.

Lemma 2.1. *For all $d > 0, d \neq \mathrm{e}$ the local maxima of Φ_d and the stable fixed points of ϕ_d coincide. For $d = \mathrm{e}$ the local maximum of Φ_{e} coincides with the lone fixed point, simultaneously the inflection point of ϕ_{e}.*

The proof of Lemma 2.1, based on a bit of calculus, can be found in Section 3.2. Additionally, for $d \le \mathrm{e}$ we define $\alpha_0 = \alpha_*$, while for $d > \mathrm{e}$ we let α_0 be the minimiser of Φ_d on the interval $[\alpha_*, \alpha^*]$. The following lemma, which we prove in Section 3.4, shows that the t-fold iteration $\phi_d^{\circ t}(x)$ converges to one of the stable fixed points, except if we start right at $x = \alpha_0$.

Lemma 2.2. *For any $d > 0$ we have*

$$\lim_{t\to\infty} \phi_d^{\circ t}(x) = \alpha_* \quad \text{for any } x < [0, \alpha_0), \qquad \lim_{t\to\infty} \phi_d^{\circ t}(x) = \alpha^* \quad \text{for any } x \in (\alpha_0, 1].$$

The fixed point characterisation of the maximisers of Φ_d enables us to show that the global maxima of Φ_d occur precisely at $\alpha_* = \alpha_*(d), \alpha^* = \alpha^*(d)$, the smallest and the largest fixed points of ϕ_d.

Proposition 2.3. *(i) If $d \le \mathrm{e}$ then ϕ_d has a unique fixed point, which is the unique global maximiser of Φ_d.*
(ii) If $d > \mathrm{e}$ then the function ϕ_d has precisely two stable fixed points, namely $0 < \alpha_* < \alpha^* < 1$, and

$$\Phi_d(\alpha_*) = \Phi_d(\alpha^*) > \Phi_d(\alpha) \qquad \text{for all } \alpha \in [0,1] \setminus \{\alpha_*, \alpha^*\}.$$

In addition, ϕ_d has its unique unstable fixed point at α_0, which satisfies the equation

$$1 - \alpha_0 = \exp(-d(1 - \alpha_0)). \tag{2.1}$$

Although both the functions ϕ_d, Φ_d are explicit, the proof of Proposition 2.3, which can be found in Section 3.3, turns out to be mildly involved.

2.2. **Warning Propagation.** One of our principal tools is an enhanced version of the Warning Propagation message passing algorithm that identifies variables as frozen, unfrozen or slush. Specifically, we will see that WP identifies about $\alpha_* n$ coordinates as positively frozen and another $(1-\alpha^*)n$ as likely unfrozen w.h.p. Because Proposition 2.3 shows that $\alpha_* = \alpha^*$ for $d < \mathrm{e}$, this already nearly suffices to establish the first part of Theorem 1.1. By contrast, in the case $d > \mathrm{e}$, where $\alpha_* < \alpha^*$, we need to conduct a more detailed investigation of the $(\alpha^* - \alpha_* + o(1))n$ coordinates that WP declares as slush.

To introduce WP, for a given $m \times n$ matrix A over $\mathbb{F}_2$ we represent the matrix by its bipartite *Tanner graph* $G(A)$. One of its vertex classes $V(A) = V(G(A)) = \{v_1, \ldots, v_n\}$ represents the columns of A; we refer to the v_i as the *variable nodes*. The second vertex class $C(A) = C(G(A)) = \{a_1, \ldots, a_m\}$ represents the rows of A; we refer to them as *check nodes*. There is an edge present between a_i and v_j iff $A_{ij} = 1$. Let $E(A)$ denote the edge set of $G(A)$. Moreover, let ∂u signify the set of neighbours of vertex $u \in V(A) \cup C(A)$. Further, let $\mathscr{F}(A)$ be the set of frozen coordinates $i \in [n]$, i.e., coordinates such that $x_i = 0$ for all $x \in \ker A$. By abuse of notation we identify $\mathscr{F}(A)$ with the corresponding set

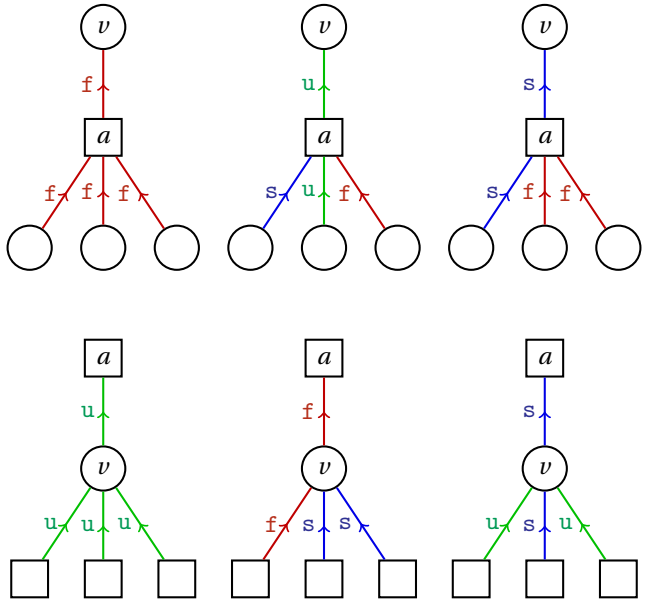

FIGURE 2. A local snapshot of the Warning Propagation rules. The check and variable nodes are represented by squares and circles respectively.

$\{v_i : i \in \mathscr{F}(A)\}$ of variable nodes. Also let $f(A) = |\mathscr{F}(A)|/n$ be the fraction of frozen coordinates. Conversely, for a given Tanner graph G we denote by $A(G)$ the adjacency matrix induced by G.

Our enhanced WP algorithm associates a pair of $\{\mathtt{f},\mathtt{s},\mathtt{u}\}$-valued messages with every edge of $G(A)$. Hence, let $\mathscr{W}(A)$ be the set of all vectors

$$w = (w_{v\to a}, w_{a\to v})_{v\in V(A), a\in C(A): a\in\partial v} \qquad \text{with entries } w_{v\to a}, w_{a\to v} \in \{\mathtt{f},\mathtt{s},\mathtt{u}\}.$$

We define the operator $\mathrm{WP}_A : \mathscr{W}(A) \to \mathscr{W}(A)$, $w \mapsto \hat{w}$, encoding one round of the message updates, by letting

$$\hat{w}_{a\to v} = \begin{cases} \mathtt{f} & \text{if } w_{y\to a} = \mathtt{f} \text{ for all } y \in \partial a \setminus \{v\}, \\ \mathtt{u} & \text{if } w_{y\to a} = \mathtt{u} \text{ for some } y \in \partial a \setminus \{v\}, \\ \mathtt{s} & \text{otherwise,} \end{cases} \qquad \hat{w}_{v\to a} = \begin{cases} \mathtt{u} & \text{if } \hat{w}_{b\to v} = \mathtt{u} \text{ for all } b \in \partial v \setminus \{a\}, \\ \mathtt{f} & \text{if } \hat{w}_{b\to v} = \mathtt{f} \text{ for some } b \in \partial v \setminus \{a\}, \\ \mathtt{s} & \text{otherwise} \end{cases} \tag{2.2}$$

as illustrated in Figure 2. Further, let $w(A,t) = \mathrm{WP}_A^t(\mathtt{s},\ldots,\mathtt{s})$ comprise the messages that result after t iterations of WP_A launched from the all-$\mathtt{s}$ message vector $w(A,0)$. Additionally, let $w(A) = \lim_{t\to\infty} w(A,t)$ be the fixed point to which WP_A converges; the (pointwise) limit always exists because WP_A only updates an $\mathtt{s}$-message to a $\mathtt{u}$-message or to an $\mathtt{f}$-message, while $\mathtt{u}$-messages and $\mathtt{f}$-messages will never change again.

What is the combinatorial idea behind WP? The intended semantics of the messages is that $\mathtt{f}$ stands for 'frozen', $\mathtt{u}$ for 'unfrozen' and $\mathtt{s}$ for 'slush'. Since we launch from all-$\mathtt{s}$ messages, (2.2) shows that in the first round $\mathtt{f}$-messages only emanate from check nodes of degree one, where the 'for all'-condition on the left of (2.2) is empty and therefore trivially satisfied. Hence, if a check node a_i is adjacent to $v_j \in V(A)$ only, then $w_{a_i\to v_j}(A,1) = \mathtt{f}$. This message reflects that the i-th row of A, having only one single non-zero entry, fixes the j-th entry of every vector of $\ker A$ to zero. Further, turning to the updates of the variable-to-check messages, if $w_{a_i\to v_j}(A,1) = \mathtt{f}$, then v_j signals its being forced to zero by passing to all its other neighbours $a_h \neq a_i$ the message $w_{v_j\to a_h}(A,1) = \mathtt{f}$. Now suppose that check a_i is adjacent to v_h and $w_{v_k\to a_i}(A,1) = \mathtt{f}$ for all $v_k \in \partial a_i \setminus \{v_h\}$. Thus, the k-th coordinate of every vector in $\ker A$ equals zero for all neighbours $v_k \neq v_h$ of a_i. Then the only way to satisfy the i-th row of A is by setting the h-th coordinate to zero as well. Accordingly, (2.2) provides that $w_{a_i\to v_h}(A,2) = \mathtt{f}$, and so on. Hence, defining

$$V_{\mathtt{f}}(A) = \{v \in V(A) : \exists a \in \partial v : w_{a\to v}(A) = \mathtt{f}\}, \qquad \text{we see that} \qquad V_{\mathtt{f}}(A) \subseteq \mathscr{F}(A). \tag{2.3}$$

The mechanics of the $\mathtt{u}$-messages is similar. In the first round any variable node v_j of degree one, for which the 'for all' condition on the right of (2.2) is trivially satisfied, starts to send out $\mathtt{u}$-messages. Subsequently, any check node a_i with an adjacent variable v_j of degree one will send a message $w_{a_i\to v_k}(A,2) = \mathtt{u}$ to all its other neighbours

$v_k \neq v_j$. Further, if a variable node v_j adjacent to a check a_i receives u-messages from all its other neighbours $a_h \neq a_i$, then v_j sends a u-message to a_i. Consequently, WP deems the variables

$$V_{\mathtt{u}}(A) = \{v \in V(A) : \forall a \in \partial v : w_{a\to v}(A) = \mathtt{u}\} \tag{2.4}$$

unfrozen. But while (2.3) shows that WP's designation of the variables in the set $V_{\mathtt{f}}(A)$ as frozen is deterministically correct, matters are more subtle when it comes to the set $V_{\mathtt{u}}(A)$. For example, short cycles might lead WP to include a variable in the set $V_{\mathtt{u}}(A)$ that is actually frozen. Yet the following lemma shows that on the random matrix $\boldsymbol{A}$ such misclassifications are rare.

Proposition 2.4. *For any $d > 0$ we have $|\mathscr{F}(\boldsymbol{A}) \cap V_{\mathtt{u}}(\boldsymbol{A})| = o(n)$ w.h.p.*

Further, tracing WP on the random graph $G(\boldsymbol{A})$, we will establish the following bounds.

Proposition 2.5. *For any $d > 0$ we have $|V_{\mathtt{f}}(\boldsymbol{A})|/n \geq \alpha_* + o(1)$ and $|V_{\mathtt{u}}(\boldsymbol{A})|/n \geq 1 - \alpha^* + o(1)$ w.h.p.*

The proofs of Proposition 2.4 and Proposition 2.5 can be found in Section 4.

Propositions 2.4 and 2.5 confine the number of frozen coordinates to the interval $[\alpha_* n + o(n), \alpha^* n + o(n)]$. In particular, the first part of Theorem 1.1, covering the regime $d < \mathrm{e}$, is an immediate consequence of Propositions 2.3, 2.4 and 2.5.

The case $d > \mathrm{e}$ is not quite so simple since $\alpha_* < \alpha^*$ for $d > \mathrm{e}$ by Proposition 2.3. Hence, Proposition 2.5 merely confines $f(\boldsymbol{A})$ to the interval $[\alpha_* + o(1), \alpha^* + o(1)]$. As we saw in Section 1.4, a vital step is to prove that $f(\boldsymbol{A})$ is actually close to one of the boundary points α_*, α^* w.h.p. To prove this statement we need to take a closer look at the minor induced by the variables that are neither identified as frozen nor unfrozen, i.e., the variables in the slush.

2.3. **The slush.** To this end we need to take a closer look at the inconclusive s-messages. Indeed, the s-messages naturally induce a minor $\boldsymbol{A}_{\mathtt{s}}$ of $\boldsymbol{A}$. Generally, for a given matrix A let

$$V_{\mathtt{s}}(A) = \{v \in V(A) : (\forall a \in \partial v : w_{a\to v}(A) \neq \mathtt{f}), |\{a \in \partial v : w_{a\to v}(A) = \mathtt{s}\}| \geq 2\}, \tag{2.5}$$

$$C_{\mathtt{s}}(A) = \{a \in C(A) : (\forall v \in \partial a : w_{v\to a}(A) \neq \mathtt{u}), |\{v \in \partial a : w_{v\to a}(A) = \mathtt{s}\}| \geq 2\}. \tag{2.6}$$

Hence, none of the variable nodes in $V_{\mathtt{s}}(A)$ receive any f-messages, but each receives at least two s-messages. Analogously, the check nodes in $C_{\mathtt{s}}(A)$ do not receive u-messages but get at least two s-messages. Let $G_{\mathtt{s}}(A)$ be the subgraph of $G(A)$ induced on $V_{\mathtt{s}}(A) \cup C_{\mathtt{s}}(A)$. Moreover, let $A_{\mathtt{s}}$ be the minor of A comprising the rows and columns whose corresponding variable or check nodes belong to $V_{\mathtt{s}}(A)$ and $C_{\mathtt{s}}(A)$, respectively. We observe that $G_{\mathtt{s}}(A)$ admits an alternative construction that resembles the construction of the 2-core of a random hypergraph. Indeed, $G_{\mathtt{s}}(A)$ results from $G(A)$ by repeating the following peeling operation:

> while there is a variable or check node of degree at most one, remove that node along with its neighbour (if any). (2.7)

To determine the size and the degree distribution of $G_{\mathtt{s}}(\boldsymbol{A})$ we employ a general result about WP-like message passing algorithms from [11, 21], which we will use in Section 4.2 to prove the following result.

Proposition 2.6. *Define*

$$\lambda = \lambda(d) = d(\alpha^* - \alpha_*), \qquad \nu = \nu(d) = \exp(-d\alpha_*) - \exp(-d\alpha^*)(1 + d(\alpha^* - \alpha_*)). \tag{2.8}$$

For any $d > \mathrm{e}$ we have $\nu > 0$ and

$$\lim_{n\to\infty} |V_{\mathtt{s}}(\boldsymbol{A})|/n = \lim_{n\to\infty} |C_{\mathtt{s}}(\boldsymbol{A})|/n = \nu \qquad \text{in probability.} \tag{2.9}$$

Moreover, for any integer $\ell \geq 2$ we have, in probability,

$$\lim_{n\to\infty} \frac{1}{n} \sum_{x \in V_{\mathtt{s}}(\boldsymbol{A})} \mathbf{1}\{|\partial x \cap C_{\mathtt{s}}(\boldsymbol{A})| = \ell\} = \lim_{n\to\infty} \frac{1}{n} \sum_{a \in C_{\mathtt{s}}(\boldsymbol{A})} \mathbf{1}\{|\partial a \cap V_{\mathtt{s}}(\boldsymbol{A})| = \ell\} = \mathbb{P}[\mathrm{Po}_{\geq 2}(\lambda) = \ell]. \tag{2.10}$$

Based on what we have learned about Warning Propagation, we are now in a position to establish items **FIX** and **STAB** from the outline from Section 1.4.

Proposition 2.7. *For all $d \in (\mathrm{e}, \infty)$ we have $\lim_{n\to\infty} \mathbb{E}\left[\left|f(\boldsymbol{A}) - \alpha_*\right| \wedge \left|f(\boldsymbol{A}) - \alpha_0\right| \wedge \left|f(\boldsymbol{A}) - \alpha^*\right|\right] = 0$.*

Proposition 2.8. *For any $d \in (\mathrm{e}, \infty)$ there exists $\varepsilon > 0$ such that $\lim_{n\to\infty} \mathbb{P}\left[\left|f(\boldsymbol{A}) - \alpha_0\right| < \varepsilon\right] = 0$.*

The proofs of Propositions 2.7–2.8 can be found in Sections 5 and 6.

2.4. **The aspect ratio.** We are left to deliver on item **EQ** from the proof outline. Thus, we need to show that $f(\boldsymbol{A})$ takes either value α_*, α^* with about equal probability if $d > \mathrm{e}$. The description (2.7) of $G_{\mathtt{s}}(\boldsymbol{A})$ in terms of the peeling process underscores that $|V_{\mathtt{s}}(\boldsymbol{A})|$ and $|C_{\mathtt{s}}(\boldsymbol{A})|$ are identically distributed. Yet in order to prove the second part of Theorem 1.1 we need to know that w.h.p. the slush matrix is not close to square. In Section 7 we prove the following.

Proposition 2.9. *For any $d_0 > \mathrm{e}$ there exists a function $\omega = \omega(n) \gg 1$ such that for all $d > d_0$ we have*

$$\lim_{n\to\infty} \mathbb{P}\left[|V_{\mathtt{s}}(\boldsymbol{A})| - |C_{\mathtt{s}}(\boldsymbol{A})| \geq \omega\right] = \lim_{n\to\infty} \mathbb{P}\left[|C_{\mathtt{s}}(\boldsymbol{A})| - |V_{\mathtt{s}}(\boldsymbol{A})| \geq \omega\right] = \frac{1}{2}.$$

2.5. **Moments and expansion.** Finally, to complete step **EQ** in Section 8 we prove that $f(\boldsymbol{A})$ is about equal to the higher possible value α^* if $\boldsymbol{A}_{\mathtt{s}}$ has more rows than columns, and equal to the lower value α_* otherwise.

Proposition 2.10. *For any $d > \mathrm{e}$, $\varepsilon > 0$, $\omega = \omega(n) \gg 1$ we have*

$$\limsup_{n\to\infty} \mathbb{P}\left[|f(\boldsymbol{A}) - \alpha^*| < \varepsilon,\ |V_{\mathtt{s}}(\boldsymbol{A})| - |C_{\mathtt{s}}(\boldsymbol{A})| \geq \omega\right] = 0, \qquad \limsup_{n\to\infty} \mathbb{P}\left[|f(\boldsymbol{A}) - \alpha_*| < \varepsilon,\ |C_{\mathtt{s}}(\boldsymbol{A})| - |V_{\mathtt{s}}(\boldsymbol{A})| \geq \omega\right] = 0.$$

We now have all the ingredients in place to complete the proof of the main theorem.

Proof of Theorem 1.1. (i) Suppose $d < \mathrm{e}$. Combining Propositions 2.4 and 2.5 with (2.3) and (2.4), we conclude that $\alpha_* - o(1) \leq f(\boldsymbol{A}) \leq \alpha^* + o(1)$ w.h.p. Since Proposition 2.3 yields $\alpha_* = \alpha^*$, the assertion follows.

(ii) Fix $d > \mathrm{e}$ and $\varepsilon > 0$ and let $\mathscr{E}_* = \{|f(\boldsymbol{A}) - \alpha_*| < \varepsilon\}$, $\mathscr{E}^* = \{|f(\boldsymbol{A}) - \alpha^*| < \varepsilon\}$. Then Propositions 2.7 and 2.8 imply that $\mathbb{P}[\mathscr{E}_* \cup \mathscr{E}^*] = 1 - o(1)$. Moreover, Propositions 2.9 and 2.10 show that $\mathbb{P}[\mathscr{E}_*] \leq 1/2 + o(1)$ and $\mathbb{P}[\mathscr{E}^*] \leq 1/2 + o(1)$. Hence, we conclude that $\mathbb{P}[\mathscr{E}_*], \mathbb{P}[\mathscr{E}^*] = 1/2 + o(1)$, as claimed. □

2.6. **The overlap.** Theorem 1.2 concerning the overlap follows relatively easily from Theorem 1.1. The single additional ingredient that we need is the following statement that provides asymptotic independence of the first few coordinates $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_\ell$ of a vector $\boldsymbol{x}$ drawn from the posterior distribution (1.3).

Proposition 2.11. *For every $\ell \geq 1$ there exists $\gamma > 0$ such that for all $d > 0$ and all $\sigma \in \mathbb{F}_2^\ell$ we have*

$$\lim_{n\to\infty} \mathbb{E}\left[n^\gamma \left| \mathbb{P}[\boldsymbol{x}_1 = \sigma_1, \ldots, \boldsymbol{x}_\ell = \sigma_\ell \mid \boldsymbol{A}] - \prod_{i=1}^{\ell} \mathbb{P}[\boldsymbol{x}_i = \sigma_i \mid \boldsymbol{A}] \right| \right] = 0.$$

Proposition 2.11, whose proof we defer to Appendix A, is a corollary to a random perturbation of the matrix $\boldsymbol{A}$ developed in [3]. As an easy consequence of Proposition 2.11 we obtain the following expression for the overlap. The proof can also be found in Appendix A.

Corollary 2.12. *For all $d > 0$ we have* $\lim_{n\to\infty} \mathbb{E}\left|R(\boldsymbol{x}, \boldsymbol{x}') - (1 + f(\boldsymbol{A}))/2\right| = 0$.

Proof of Theorem 1.2. The assertion is an immediate consequence of Theorem 1.1 and Corollary 2.12. □

2.7. **Preliminaries and notation.** Throughout the paper, we use the standard Landau notations for asymptotic orders and all asymptotics are taken as $n \to \infty$. Where asymptotics with respect to another additional parameter are needed, we indicate this fact by using an index. For example, $g(\varepsilon, n) = o_\varepsilon(1)$ means that

$$\limsup_{\varepsilon\to 0} \limsup_{n\to\infty} |g(\varepsilon, n)| = 0.$$

We ignore floors and ceilings whenever they do not significantly affect the argument.

Any $m \times n$ $\mathbb{F}_2$-matrix A is perfectly represented by its Tanner graph $G(A)$, as defined in Section 2.2. We simply identify A with its Tanner graph $G(A)$. For instance, we take the liberty of writing $f(G(A))$ instead of $f(A)$. Conversely, a bipartite graph G with designated sets of check nodes $C(G)$ and variable nodes $V(G)$ induces a $|C(G)| \times |V(G)|$ matrix $A(G)$. Once again we tacitly identify G with this matrix. Recall that for a Tanner graph G and a node $z \in C(G) \cup V(G)$ we let $\partial z = \partial_G z$ signify the set of neighbours. We further define $\partial^t z = \partial_G^t z$ to be the set of nodes at distance exactly t from z.

For a matrix A we generally denote by $\mathscr{F}(A) = \mathscr{F}(G(A))$ the set of frozen variables. In addition, we let $\hat{\mathscr{F}}(A)$ be the set of frozen checks, where a check node $a \in C(A)$ is called *frozen* if $\partial a \subseteq \mathscr{F}(A)$. Let $\hat{f}(A) = |\hat{\mathscr{F}}(A)|/|C(A)|$ be the fraction of frozen checks.

For a matrix A with Tanner graph G and a node z of G let $d_A(z) = d_G(z)$ denote the degree of z. Furthermore, let $d_A = (d_A(z))_{z\in C(A)\cup V(A)}$ signify the degree sequence of $G(A)$. In addition, let $d_{A,\mathtt{s}} = (d_{A,\mathtt{s}}(z))_{z\in C(A)\cup V(A)}$ encompass

the degrees of the subgraph $G_{\mathbf{s}}(A)$. Note that this sequence includes degrees of vertices which are not actually in $G_{\mathbf{s}}(A)$, whose degree in $G_{\mathbf{s}}(A)$ we define to be 0.

Returning to the random matrix $\boldsymbol{A}$, let $\mathscr{G}_{\mathbf{s}}$ be a random multigraph drawn from the pairing model with degree distribution $d_{\boldsymbol{A},\mathbf{s}}$.

Lemma 2.13. *The probability that $\mathscr{G}_{\mathbf{s}}$ is a simple graph is bounded away from* 0*. Furthermore, conditioned on being simple the graph $\mathscr{G}_{\mathbf{s}}$ has exactly the same distribution as $G_{\mathbf{s}}(\boldsymbol{A})$.*

The proof of this lemma is a standard exercise, which we include in Appendix B for completeness. We further need a routine estimate of the degree distribution of the random bipartite graph $G(\boldsymbol{A})$, whose proof can be found in Appendix C.

Lemma 2.14. *Let $d > 0$. W.h.p. the random graph $G(\boldsymbol{A})$ satisfies*

$$\max_{v\in V(\boldsymbol{A})\cup C(\boldsymbol{A})}|\partial v| \le \log n, \qquad \frac{1}{n}\sum_{x\in V(\boldsymbol{A})}\binom{|\partial x|}{\ell} \le (2d)^{\ell} \qquad \text{for any integer } \ell \ge 1. \tag{2.11}$$

Throughout the paper all logarithms are to the base e.

The *entropy* of a probability distribution μ on a finite set $\Omega \neq \emptyset$ is denoted by

$$H(\mu) = -\sum_{\omega\in\Omega}\mu(\omega)\log\mu(\omega).$$

As a further important tool we need the cut metric for probability measures on $\mathbb{F}_2^n$. Following [14], we define the *cut distance* of two probability measures μ,ν on $\mathbb{F}_2^n$ as

$$\Delta_{\square}(\mu,\nu) = \frac{1}{n}\min_{\substack{\boldsymbol{\sigma}\sim\mu\\ \boldsymbol{\tau}\sim\nu}}\max_{\substack{U\subseteq\mathbb{F}_2^n\times\mathbb{F}_2^n\\ I\subseteq[n]}}\left|\sum_{i\in I}\mathbb{P}\left[(\boldsymbol{\sigma},\boldsymbol{\tau})\in U,\boldsymbol{\sigma}_i=1\right]-\mathbb{P}\left[(\boldsymbol{\sigma},\boldsymbol{\tau})\in U,\boldsymbol{\tau}_i=1\right]\right|. \tag{2.12}$$

In words, we first minimise over couplings $(\boldsymbol{\sigma},\boldsymbol{\tau})$ of the probability measures μ,ν. Then, given such a coupling an adversary points out the largest remaining discrepancy. Specifically, the adversary puts their finger on the event U and the set of coordinates I where the frequency of 1-entries in $\boldsymbol{\sigma},\boldsymbol{\tau}$ differ as much as possible.

The cut metric is indeed a (very weak) metric. We need to point out a few of its basic properties. For a probability measure μ on $\mathbb{F}_2^n$ let $\boldsymbol{\sigma}^{(\mu)}$ denote a sample from μ. Moreover, let $\bar{\mu}$ be the product measure with the same marginals, i.e.,

$$\bar{\mu}(\sigma) = \prod_{i=1}^{n}\mu\left(\left\{\boldsymbol{\sigma}_i^{(\mu)}=\sigma_i\right\}\right) \qquad (\sigma\in\mathbb{F}_2^n).$$

It is easy to see that upper bounds on the cut distance of μ,ν carry over to $\bar{\mu},\bar{\nu}$, i.e.,

$$\Delta_{\square}(\bar{\mu},\bar{\nu}) \le \Delta_{\square}(\mu,\nu). \tag{2.13}$$

Moreover, upper bounds on the cut distance carry over to upper bounds on the marginal distributions, i.e.,

$$\frac{1}{n}\sum_{i=1}^{n}\left|\mu\left(\left\{\boldsymbol{\sigma}_i^{(\mu)}=1\right\}\right)-\nu\left(\left\{\boldsymbol{\sigma}_i^{(\nu)}=1\right\}\right)\right| \le \Delta_{\square}(\mu,\nu). \tag{2.14}$$

The distribution μ is *ε-extremal* if $\Delta_{\square}(\mu,\bar{\mu})<\varepsilon$. Furthermore, μ is *ε-symmetric* if

$$\sum_{1\le i<j\le n}\left|\mu\left(\left\{\boldsymbol{\sigma}_i^{(\mu)}=\boldsymbol{\sigma}_j^{(\mu)}=1\right\}\right)-\mu\left(\left\{\boldsymbol{\sigma}_i^{(\mu)}=1\right\}\right)\mu\left(\left\{\boldsymbol{\sigma}_j^{(\mu)}=1\right\}\right)\right|<\varepsilon n^2.$$

Hence, for most pairs i,j the entries $\boldsymbol{\sigma}_i,\boldsymbol{\sigma}_j$ are about independent. More generally, μ is *(ε,ℓ)-symmetric* if

$$\sum_{\tau\in\mathbb{F}_2^{\ell}}\sum_{1\le i_1<\cdots<i_{\ell}\le n}\left|\mu\left(\left\{\forall j\le\ell:\boldsymbol{\sigma}_{i_j}^{(\mu)}=\tau_j\right\}\right)-\prod_{j=1}^{\ell}\mu\left(\left\{\boldsymbol{\sigma}_{i_j}^{(\mu)}=\tau_j\right\}\right)\right|<\varepsilon n^{\ell}.$$

The following statement summarises a few results about the cut metric from [5, 14].

Proposition 2.15. *For any $\ell,\varepsilon>0$ there exist $\delta>0$ and $n_0>0$ such that for all $n>n_0$ and all probability measures μ on $\mathbb{F}_2^n$ the following statements hold.*

(i) If μ is δ-extremal, then μ is (ε,ℓ)-symmetric.
(ii) If μ is δ-symmetric, then μ is ε-extremal.

Furthermore, extremality of measures carries over to conditional measures so long as we do not condition on events that are too unlikely. More generally, we call two probability measures μ, ν on $\mathbb{F}_2^n$ *mutually c-contiguous* if $c^{-1}\mu(\sigma) \le \nu(\sigma) \le c\mu(\sigma)$ for all $\sigma \in \mathbb{F}_2^n$.

Proposition 2.16 ([19])**.** *For any $\varepsilon > 0$ there exist $\delta > 0$ and $n_0 > 0$ such that for all $n > n_0$, any δ-extremal probability measure μ on $\mathbb{F}_2^n$ and any probability measure ν on $\mathbb{F}_2^n$ such that μ, ν are mutually $(1/\varepsilon)$-contiguous, we have $\Delta_\square(\mu, \nu) < \varepsilon$.*

Moreover, we need an elementary observation about the kernel of $\mathbb{F}_2$-matrices.

Fact 2.17 ([3, Lemma 2.3])**.** *Let A be an $m \times n$-matrix over $\mathbb{F}_2$ and choose $\boldsymbol{\xi} = (\boldsymbol{\xi}_1, \ldots, \boldsymbol{\xi}_n) \in \ker A$ uniformly at random. Then for any $i, j \in [n]$ we have $\mathbb{P}[\boldsymbol{\xi}_i = 0] \in \{1/2, 1\}$ and $\mathbb{P}[\boldsymbol{\xi}_i = \boldsymbol{\xi}_j] \in \{1/2, 1\}$.*

Finally, in Appendix D we will prove the following auxiliary statement about weighted sums.

Lemma 2.18. *For any $c_0, c_1 > 0$ there exists $c_2 > 0$ such that for all $n > 0$ the following is true. Suppose that $w : [n] \to (0, \infty)$ is any function such that*

$$\frac{1}{n}\sum_{i=1}^{n} w_i \mathbf{1}\{w_i > t\} \le c_0 \exp(-c_1 t) \qquad \text{for any } t \ge 1.$$

Moreover, assume that $\mathscr{P} = (P_1, \ldots, P_\ell)$ is any partition of $[n]$ into pairwise disjoint sets such that

$$\frac{1}{n}\sum_{j=1}^{\ell} |P_j| \mathbf{1}\{|P_j| > t\} \le c_0 \exp(-c_1 t) \qquad \text{for any } t \ge 1.$$

Then $\frac{1}{n}\sum_{j=1}^{\ell} \left(\sum_{i \in P_j} w_i\right)^2 \le c_2$.

3. Fixed points and local maxima

In this section we prove Lemma 2.1 and Proposition 2.3. We begin with a bit of trite calculus.

3.1. **Getting started.** We introduce $D_d(\alpha) = \exp(-d(1-\alpha))$ so that

$$\phi_d(\alpha) = 1 - \exp(-d\exp(-d(1-\alpha))) = 1 - D_d(1 - D_d(\alpha)), \quad \Phi_d(\alpha) = D_d(1 - D_d(\alpha)) + (1 + d(1-\alpha))D_d(\alpha) - 1. \tag{3.1}$$

We need two derivatives of $\Phi_d(\alpha)$ and $\phi_d(\alpha)$:

$$\Phi_d'(\alpha) = d^2 D_d(\alpha)\left(\phi_d(\alpha) - \alpha\right), \qquad \phi_d'(\alpha) = d^2 D_d\left(1 - D_d(\alpha)\right) D_d(\alpha), \tag{3.2}$$

$$\Phi_d''(\alpha) = d^3 D_d(\alpha)\left(\phi_d(\alpha) - \alpha\right) + d^2 D_d(\alpha)\left(\phi_d'(\alpha) - 1\right), \qquad \phi_d''(\alpha) = d^3 D_d\left(1 - D_d(\alpha)\right) D_d(\alpha)\left(1 - dD_d(\alpha)\right). \tag{3.3}$$

Since $D_d(\alpha)$ is strictly increasing for all $d > 0$, so is $\phi_d(\alpha)$ due to (3.1). Thus,

$$\phi_d'(\alpha) > 0 \qquad \text{for all } \alpha \in [0,1]. \tag{3.4}$$

Moreover, (3.3) shows that the sign of ϕ_d'' only depends on the last term, denoted by

$$\psi_{d,\mathrm{sign}}(\alpha) = 1 - dD_d(\alpha). \tag{3.5}$$

We denote the unique zero of $\psi_{d,\mathrm{sign}}(\alpha)$ by $\bar{\alpha} = 1 - \frac{\log d}{d}$. The following claim comes down to an exercise in calculus.

Claim 3.1. *(i) $\bar{\alpha}$ is a fixed point of ϕ_d iff $d = \mathrm{e}$.*
(ii) $\phi_d''(0) > 0$.
(iii) $\phi_d''(\alpha)$ has one zero at $\bar{\alpha}$ in the interval $[0,1]$ if $d \ge 1$, none otherwise.
(iv) $\phi_{\mathrm{e}}'(\bar{\alpha}) = 1$ and $\Phi_{\mathrm{e}}''(\bar{\alpha}) = 0$.
(v) $\bar{\alpha}$ is the only fixed point of $\phi_{\mathrm{e}}(\alpha)$.
(vi) The fixed points of ϕ_d coincide with the stationary points of Φ_d.
(vii) $\Phi_d'(0) > 0 > \Phi_d'(1)$.
(viii) For any $d > 0$ the function ϕ_d has at least one stable fixed point.
(ix) For any $d > 0$ the function ϕ_d has at most three fixed points, no more than two of which are stable.
(x) For $d < \mathrm{e}$, we have $\phi_d'(\alpha) < 1$ for all $\alpha \in [0,1]$.
(xi) For $d < \mathrm{e}$, the function Φ_d attains a unique local maximiser $\alpha_d \in (0,1)$.
(xii) For $d > \mathrm{e}$, if $\alpha \in (0,1)$ is a fixed point of ϕ_d then so is $\hat{\alpha} = 1 - \exp(-d(1-\alpha)) \in (0,1)$.

Proof. (i) Observe that $\phi_d(\bar\alpha) = 1 - 1/\mathrm{e}$, which is a fixed point iff $\bar\alpha = 1 - \frac{\log d}{d} = 1 - \frac{1}{\mathrm{e}}$, i.e. iff $d = \mathrm{e}$.

(ii) Recall that the sign of $\phi_d''(\alpha)$ is determined by the sign of $\psi_{d,\mathrm{sign}}(\alpha)$, and we have $\psi_{d,\mathrm{sign}}(0) = 1 - d\exp(-d) > 0$ for all $d > 0$.

(iii) Since $\psi_{d,\mathrm{sign}}'(\alpha) = -d^2\exp(-d(1-\alpha)) < 0$, we see that $\psi_{d,\mathrm{sign}}$ is a decreasing function that has its unique zero at $\bar\alpha$. Furthermore, $\bar\alpha \le 1$ iff $d \ge 1$.

(iv) By (i), when $d = \mathrm{e}$ and $\alpha = \bar\alpha$, Equation (3.3) reduces to $\Phi_{\mathrm{e}}''(\bar\alpha) = \mathrm{e}^2 D_{\mathrm{e}}(\bar\alpha)\left(\phi_{\mathrm{e}}'(\bar\alpha) - 1\right)$. Since also $D_e(\bar\alpha) = 1/\mathrm{e}$, by (3.2) we have $\phi_{\mathrm{e}}'(\bar\alpha) = 1$, and therefore also $\Phi_{\mathrm{e}}''(\bar\alpha) = 0$.

(v) Due to (i) $\bar\alpha$ is a fixed point, and $\phi_{\mathrm{e}}'(\bar\alpha) = 1$ by (iv). Since $\phi_{\mathrm{e}}(\alpha)$ is convex for $\alpha < \bar\alpha$ and concave for $\alpha > \bar\alpha$ by (3.3), we deduce that $\phi_{\mathrm{e}}(\alpha) > \alpha$ for $\alpha < \bar\alpha$ and $\phi_{\mathrm{e}}(\alpha) < \alpha$ for $\alpha > \bar\alpha$, so $\bar\alpha$ is the unique fixed point of $\phi_{\mathrm{e}}(\alpha)$.

(vi) Since $d^2 D_d(\alpha) > 0$, (3.2) implies that $\Phi_d'(\alpha) = 0$ iff $\phi_d(\alpha) = \alpha$.

(vii) This follows from (3.2) since $\phi_d(0) > 0$ and $\phi_d(1) < 1$.

(viii) Since $\phi_d(0) > 0$ and $\phi_d(1) < 1$, and since ϕ_d is a continuous function, there must be at least one fixed point in $(0,1)$. Setting $\alpha_1 := \sup\{\alpha : \phi_d(\alpha) > \alpha\}$, we have that α_1 is a fixed point by continuity. Furthermore, α_1 is stable since there are points $\alpha < \alpha_1$ arbitrarily close to α_1 for which $\phi_d(\alpha) > \alpha$, but also for any $\alpha > \alpha_1$ we have $\phi_d(\alpha) \le \alpha$, and therefore $\phi_d'(\alpha_1) \le 1$. [1]

(ix) This is a consequence of (iii): between any two fixed points there must be a point with $\phi'(\alpha) = 1$, and between any two such points there must be a point with $\phi''(\alpha) = 0$; furthermore, between any two stable fixed points, there must be an unstable fixed point.

(x) If $d < 1$, (ii) and (iii) imply that $\phi''(\alpha) > 0$ on $[0,1]$. Therefore $\phi_d'(\alpha) \le \phi_d'(1) = d^2\mathrm{e}^{-d} < 1$. For $1 \le d < \mathrm{e}$, Property (iii) proves that for all $\alpha \in [0,1]$ we have $\phi_d'(\alpha) < \phi_d'(\bar\alpha) = d/\mathrm{e} < 1$.

(xi) By (vi), we may consider stable fixed points of ϕ_d rather than maximisers of Φ_d. The difference $h(\alpha) := \phi_d(\alpha) - \alpha$ is a decreasing function since $h'(\alpha) = \phi_d'(\alpha) - 1 < 0$ by (x). Since $h(0) > 0$ and $h(1) < 0$, $h(\alpha)$ has only one zero for $d < \mathrm{e}$. This shows that the stable fixed point from (viii) is the unique fixed point.

(xii) Using $\alpha = \phi_d(\alpha) = 1 - \exp(-d\exp(-d(1-\alpha)))$, we obtain

$$\exp(-d(1-\hat\alpha)) = \exp(-d\exp(-d(1-\alpha))) = 1 - \alpha = -\log(1-\hat\alpha)/d.$$

Rearranging this inequality shows that $\hat\alpha = \phi_d(\hat\alpha)$. □

3.2. **Proof of Lemma 2.1.** At a fixed point α of ϕ_d, (3.3) simplifies to

$$\Phi_d''(\alpha) = d^2 D_d(\alpha)\left(\phi_d'(\alpha) - 1\right). \tag{3.6}$$

This shows $\Phi_d''(\alpha) < 0$ iff $\phi_d'(\alpha) < 1$. Hence, for $d > 0$, $d \ne \mathrm{e}$, (3.4) and Claim 3.1 (vi) imply that the stable fixed points of ϕ_d are precisely the local maximisers of Φ_d. Claim 3.1 (v) proves the second assertion in the case $d = \mathrm{e}$.

3.3. **Proof of Proposition 2.3.** We make further observations on the existence and stability of fixed points of ϕ_d.

Lemma 3.2. *If $d > \mathrm{e}$ then Φ_d attains its unique local minimum $\alpha_0 \in [\alpha_*, \alpha^*]$ at the root of $1 - \alpha - \exp(-d(1-\alpha))$.*

Proof. The concave function $\alpha \in [0,1] \mapsto 1 - \exp(-d(1-\alpha))$ has a unique fixed point $\beta = \beta(d) \in (0,1)$, which satisfies

$$\phi_d(\beta) = 1 - \exp(-d\exp(-d(1-\beta)) = \beta, \qquad \phi_d'(\beta) = d^2\exp(-d(1-\beta))\exp(-d\exp(-d(1-\beta))) = d^2(1-\beta)^2.$$

Hence, Claim 3.1 (vi) and (3.6) yield

$$\Phi_d'(\beta) = 0, \qquad \Phi_d''(\beta) = d^2\exp(-d(1-\beta))\left(d^2(1-\beta)^2 - 1\right). \tag{3.7}$$

In order to determine the sign of the last expression we differentiate with respect to d, keeping in mind that $\beta = \beta(d)$ is a function of d. Rearranging the fixed point equation $\beta = 1 - \exp(-d(1-\beta))$, we obtain $d = -(1-\beta)^{-1}\log(1-\beta)$. The inverse function theorem therefore yields

$$\frac{\partial\beta}{\partial d} = \frac{(1-\beta)^2}{1 - \log(1-\beta)}.$$

Combining the chain rule with the fixed point equation $\beta = 1 - \exp(-d(1-\beta))$, we thus obtain

$$\frac{\partial}{\partial d} d^2(1-\beta)^2 = 2d(1-\beta)^2 - 2d^2(1-\beta)\frac{\partial\beta}{\partial d} = 2d(1-\beta)^2\left(1 - \frac{d(1-\beta)}{1-\log(1-\beta)}\right) = \frac{2d(1-\beta)^2}{1+d(1-\beta)} > 0. \tag{3.8}$$

[1] Note that at this point we could also have observed that Φ_d attains its maximum in the interior of $(0,1)$ and then applied Lemma 2.1 to prove the existence of a stable fixed point. This would be permissible since the proof of Lemma 2.1 only uses earlier points from this Claim and not (viii) or any later points, therefore the argument is not a circular one.

As in Claim 3.1, at $d = \mathrm{e}$ we obtain $\beta = \bar{\alpha} = 1 - 1/\mathrm{e}$ and thus $d^2(1-\beta)^2 = 1$. Therefore, (3.8) implies that $d^2(1-\beta)^2 > 1$ for all $d > \mathrm{e}$, and thus (3.7) shows that Φ_d attains its local minimum α_0 precisely at the point β. Finally, by Claim 3.1 (vi) and (ix) there is precisely one local minimum in the interval $[\alpha_*, \alpha^*]$. □

Corollary 3.3. *For $d > \mathrm{e}$ the function Φ_d attains its local maxima at the fixed points $0 < \alpha_* < \alpha^* < 1$ of ϕ_d. Moreover, $\Phi_d(\alpha_*) = \Phi_d(\alpha^*)$.*

Proof. Since by Claim 3.1 (vii) we have $\Phi_d'(0) > 0 > \Phi_d'(1)$, the existence of the local minimiser $\alpha_0 \in (0,1)$ provided by Lemma 3.2 implies that Φ_d has at least two local maximisers $0 < \alpha_1 < \alpha_0 < \alpha_2 < 1$. Lemma 2.1 and Claim 3.1 (vi) show that $\alpha_0, \alpha_1, \alpha_2$ are fixed points of ϕ_d. Hence, Claim 3.1 (ix) implies that $\alpha_1 = \alpha_*$ is the smallest fixed point of ϕ_d and that $\alpha_2 = \alpha^* > \alpha_*$ is the largest fixed point. Additionally, Lemma 2.1 and Claim 3.1 (ix) imply that α_*, α^* are the only local maximisers of Φ_d.

It remains to prove that $\Phi_d(\alpha_*) = \Phi_d(\alpha^*)$. Claim 3.1 (xii) implies that

$$\hat{\alpha}_* = 1 - \exp(-d(1-\alpha_*)) \qquad \text{and} \qquad \hat{\alpha}^* = 1 - \exp(-d(1-\alpha^*))$$

are fixed points of ϕ_d. Because $\alpha_0 \neq \alpha_*, \alpha^*$ is the unique root of $1 - \alpha - \exp(-d(1-\alpha))$, we conclude that $\hat{\alpha}_* = \alpha^*$ and $\hat{\alpha}^* = \alpha_*$. Hence,

$$1 - \alpha^* = \exp(-d(1-\alpha_*)), \quad 1 - \alpha_* = \exp(-d(1-\alpha^*)). \tag{3.9}$$

Consequently,

$$(1-\alpha_*)\exp(-d(1-\alpha_*)) = (1-\alpha^*)\exp(-d(1-\alpha^*)) \qquad \text{and} \tag{3.10}$$

$$1 - \alpha_* + \exp(-d(1-\alpha_*)) = 1 - \alpha^* + \exp(-d(1-\alpha^*)) \tag{3.11}$$

Finally, combining (3.10)–(3.11) with the fixed point equations $\phi_d(\alpha_*) = \alpha_*$, $\phi_d(\alpha^*) = \alpha^*$, we obtain

$$\begin{aligned}\Phi_d(\alpha^*) - \Phi_d(\alpha_*) &= \exp(-d\exp(-d(1-\alpha^*))) + \exp(-d(1-\alpha^*)) - \left[\exp(-d\exp(-d(1-\alpha_*))) + \exp(-d(1-\alpha_*))\right] \\ &\quad + d\left[(1-\alpha^*)\exp(-d(1-\alpha^*)) - (1-\alpha_*)\exp(-d(1-\alpha_*))\right] \\ &= 1 - \alpha^* + \exp(-d(1-\alpha^*)) - \left(1 - \alpha_* + \exp(-d(1-\alpha_*))\right) = 0,\end{aligned}$$

thereby completing the proof. □

Proof of Proposition 2.3. The first part follows immediately from Lemma 2.1 and Claim 3.1 (xi). The second assertion follows from Lemma 2.1, Lemma 3.2 and Corollary 3.3. □

3.4. **Proof of Lemma 2.2.** By a straightforward computation, we get that $\phi_d(0) > 0$ and $\phi_d(1) < 1$ for all $d > 0$. Moreover, $\phi_d(\alpha)$ is a continuously differentiable function. For $d < \mathrm{e}$, by Claim 3.1 (vi) and (xi) (or Proposition 2.3 (i)) there is one fixed point $\alpha_* = \alpha_0 = \alpha^*$. This implies $\phi_d(\alpha) > \alpha$ for $\alpha \in [0, \alpha_*)$ and $\phi_d(\alpha) < \alpha$ for $\alpha \in (\alpha_*, 1]$. By Equation (3.4), $\phi_d(\alpha)$ is strictly increasing so $\phi_d(\phi_d(\alpha)) > \phi_d(\alpha)$ for $\alpha \in [0, \alpha_*)$ and $\phi_d(\phi_d(\alpha)) < \phi_d(\alpha)$ for $\alpha \in (\alpha_*, 1]$. By induction, for all $t > 0$, $\phi_d^{\circ t}(\alpha) > \phi_d^{\circ t-1}(\alpha)$ for $\alpha \in [0, \alpha_*)$ and $\phi_d^{\circ t}(\alpha) < \phi_d^{\circ t-1}(\alpha)$ for $\alpha \in (\alpha_*, 1]$. In addition, the fact that α_* is a fixed point of ϕ implies that $\alpha_* = \phi_d(\alpha_*) > \phi_d^{\circ t}(\alpha)$ for $\alpha \in [0, \alpha_*)$ and $\alpha_* = \phi_d(\alpha_*) < \phi_d^{\circ t}(\alpha)$ for $\alpha \in (\alpha_*, 1]$. Hence, for $\alpha \in [0, \alpha_*)$, the sequence $\left(\phi_d^t(\alpha)\right)_{t \geq 0}$ is monotonically increasing and bounded above by $\phi_d(\alpha_*) = \alpha_*$, and therefore $\lim_{t\to\infty} \phi_d^{\circ t}(\alpha)$ exists. Furthermore, since ϕ_d is continuous, this limit must be a fixed point of ϕ_d. Since α_* is the smallest fixed point, we must have $\lim_{t\to\infty} \phi_d^{\circ t}(\alpha) = \alpha_*$, as required. Similarly, for $\alpha \in (\alpha_*, 1]$, the sequence $\left(\phi_d^t(\alpha)\right)_{t \geq 0}$ is monotonically decreasing and bounded below thus $\lim_{t\to\infty} \phi_d^{\circ t}(\alpha) = \alpha^*$.

For $d > \mathrm{e}$, by Proposition 2.3 (ii), there are three fixed points, $\alpha_* < \alpha_0 < \alpha^*$ where α_*, α^* are stable fixed points and α_0 is unstable. For the intervals $[0, \alpha_*), (\alpha^*, 1]$, the proof is exactly the same as in the case $d < \mathrm{e}$. Similarly, (α_*, α_0) comes down to the case of a monotonically decreasing sequence converging to α_* while (α_0, α^*) comes down to the case of a monotonically increasing sequence converging to α^*.

4. Tracing Warning Propagation

In this section we will analyse the local structure of $G(\boldsymbol{A})$ together with WP messages, and show that locally the graph has a rather simple structure. For this argument we will make use of the results of [11, 21].[2] The study of WP messages will enable us to prove Propositions 2.4, 2.5 and 2.6.

[2] The article [11] deals with the standard binomial random graph $G(n, d/n)$, whereas in our situation we have the *bipartite* graph $G(n, n, d/n)$ – however, the proofs in that paper generalise in an obvious way to this setting. The generalised version of the proof is in the article [21]

4.1. **Message distributions and the local structure.** To investigate the link between the local graph structure and the WP messages we need a few definitions. Let us first define a *message distribution* to be a vector

$$\boldsymbol{q} = \left(\boldsymbol{q}^{(v)}, \boldsymbol{q}^{(c)}\right) \quad \text{with} \quad \boldsymbol{q}^{(v)} = \left(q^{(v)}_{\mathtt{f}}, q^{(v)}_{\mathtt{s}}, q^{(v)}_{\mathtt{u}}\right),\ \boldsymbol{q}^{(c)} = \left(q^{(c)}_{\mathtt{f}}, q^{(c)}_{\mathtt{s}}, q^{(c)}_{\mathtt{u}}\right) \in [0,1]^3 \quad \text{s.t.} \quad \sum_{s\in\{\mathtt{f},\mathtt{s},\mathtt{u}\}} q^{(v)}_s = \sum_{s\in\{\mathtt{f},\mathtt{s},\mathtt{u}\}} q^{(c)}_s = 1.$$

Intuitively, $q^{(v)}, q^{(c)}$ model the probability distribution of an incoming message at a check/variable node, so for example $q^{(v)}_{\mathtt{f}}$ is the probability that an incoming message at a variable node is $\mathtt{f}$.

Given a message distribution $\boldsymbol{q}$, we define $\mathrm{Po}(d\boldsymbol{q})$ to be a distribution of half-edges with incoming messages. Specifically, at a variable node, this generates $\mathrm{Po}\left(dq^{(v)}_{\mathtt{f}}\right)$ half-edges whose in-message is $\mathtt{f}$ and similarly (and independently) generates half-edges whose in-message is $\mathtt{s}$ or $\mathtt{u}$. At a check node, the generation of half-edges with incoming messages is analogous. Let us define the message distribution

$$\begin{aligned}\boldsymbol{q}_* := \left(\boldsymbol{q}^{(v)}_*, \boldsymbol{q}^{(c)}_*\right) \quad \text{with} \quad \boldsymbol{q}^{(v)}_* &= \left(q^{(v)}_{*,\mathtt{f}}, q^{(v)}_{*,\mathtt{s}}, q^{(v)}_{*,\mathtt{u}}\right) := \left(1-\alpha^*, \alpha^*-\alpha_*, \alpha_*\right),\\ \boldsymbol{q}^{(c)}_* &= \left(q^{(c)}_{*,\mathtt{f}}, q^{(c)}_{*,\mathtt{s}}, q^{(c)}_{*,\mathtt{u}}\right) := \left(\alpha_*, \alpha^*-\alpha_*, 1-\alpha^*\right).\end{aligned}$$

which is our conjectured limiting distribution of a randomly chosen message after the completion of WP, which motivates the following definitions.

Definition 4.1. *We define branching processes $\mathscr{T}, \hat{\mathscr{T}}$ which will generate rooted trees decorated with messages along edges towards the root.*

(i) The root of the first process $\mathscr{T}$ is a variable node v_0. The root spawns $\mathrm{Po}(d)$ *children, which are check nodes. The edges from the children to the root independently carry an* $\mathtt{f}$*-message with probability* $1-\alpha^*$*, an* $\mathtt{s}$*-message with probability* $\alpha^*-\alpha_*$*, and a* $\mathtt{u}$*-message with probability* α_**. The process then proceeds such that each check node spawns variable nodes and each variable node spawns check nodes as its offspring such that the messages sent from the children to their parents abide by the rules from Figure 2. To be precise, a check node a that sends its parent message $z \in \{\mathtt{f},\mathtt{s},\mathtt{u}\}$ has offspring*

- *$z = \mathtt{f}$:* $\mathrm{Po}(\alpha_* d)$ *children that send an* $\mathtt{f}$*-message.*
- *$z = \mathtt{s}$:* $\mathrm{Po}(\alpha_* d)$ *children that send an* $\mathtt{f}$*-message and* $\mathrm{Po}_{\geq 1}(d(\alpha^*-\alpha_*))$ *children that each send an* $\mathtt{s}$*-message.*
- *$z = \mathtt{u}$:* $\mathrm{Po}(\alpha_* d)$ *children that send an* $\mathtt{f}$*-message,* $\mathrm{Po}(d(\alpha^*-\alpha_*))$ *children that send an* $\mathtt{s}$*-message and* $\mathrm{Po}_{\geq 1}(d(\alpha^*-\alpha_*))$ *children that send a* $\mathtt{u}$*-message.*

Analogously, a variable node v that sends its parent message $z \in \{\mathtt{f},\mathtt{s},\mathtt{u}\}$ has offspring

- *$z = \mathtt{f}$:* $\mathrm{Po}_{\geq 1}((1-\alpha_*)d)$ *children that send an* $\mathtt{f}$*-message,* $\mathrm{Po}(d(\alpha^*-\alpha_*))$ *children that send an* $\mathtt{s}$*-message, and* $\mathrm{Po}(d\alpha_*)$ *children that send a* $\mathtt{u}$*-message.*
- *$z = \mathtt{s}$:* $\mathrm{Po}(\alpha_* d)$ *children that each send a* $\mathtt{u}$*-message and* $\mathrm{Po}_{\geq 1}(d(\alpha^*-\alpha_*))$ *children that send an* $\mathtt{s}$*-message.*
- *$z = \mathtt{u}$:* $\mathrm{Po}(\alpha_* d)$ *children that send a* $\mathtt{u}$*-message.*

(ii) The root of the second process $\hat{\mathscr{T}}$ is a check node a_0. The root spawns $\mathrm{Po}(d)$ *children, which are variable nodes. They independently send messages* $\mathtt{f},\mathtt{s},\mathtt{u}$ *with probabilities* $\alpha_*, \alpha^*-\alpha_*, 1-\alpha^*$*. Apart from the root, the nodes have offspring as under (i).*

Let us note that the processes $\mathscr{T}, \hat{\mathscr{T}}$, when truncated at depth $t \in \mathbb{N}$, are equivalent to the following: generate a 2-type branching tree up to depth t from the appropriate type of root in which each variable node has $\mathrm{Po}(d)$ children which are check nodes and vice versa, generate messages from the leaves at depth t at random according to $\boldsymbol{q}_*$ and generate all other messages up the tree from these according to the WP update rule.

The following is the critical lemma describing the local structure. Given an integer t, let us define $\mathscr{S}_t$ to be the set of messaged trees rooted at a variable node and with depth at most t, and similarly $\hat{\mathscr{S}}_t$ for trees rooted at a check node. For any $T \in \mathscr{S}_t$ and matrix A, let us define

$$\xi_T(A) := \frac{1}{n}\sum_{v\in V(A)} \mathbf{1}\left\{\delta^t_{G(A)} v \cong T\right\}$$

to be the empirical fraction of variable nodes whose rooted depth t neighbourhood $G(A)$ with edges towards the root annotated by the WP messages $(w_{a\to y}(A), w_{y\to a}(A))_{a,y}$ is isomorphic to T. For $\hat{T} \in \hat{\mathscr{S}}_T$, the parameter $\xi_{\hat{T}}(A)$ is defined similarly. We also define $\zeta_T := \mathbb{P}[\mathscr{T}_t \cong T]$ and $\zeta_{\hat{T}} := \mathbb{P}\left[\hat{\mathscr{T}}_t \cong \hat{T}\right]$ to be the probabilities that the appropriate branching process is isomorphic to T or $\hat{T}$ respectively.

Lemma 4.2. *For any constant t and any trees $T \in \mathscr{S}_t$ and $\hat{T} \in \hat{\mathscr{S}}_t$ we have*

$$\lim_{n\to\infty} |\xi_T(\boldsymbol{A}) - \zeta_T| = 0 \qquad \textit{and} \qquad \lim_{n\to\infty} |\xi_{\hat{T}}(\boldsymbol{A}) - \zeta_{\hat{T}}| = 0 \qquad \textit{in probability.}$$

In other words, picking a random vertex and looking at its local neighbourhood gives asymptotically the same result as generating a $\mathrm{Po}(d)$ branching tree to the appropriate depth and initialising messages at the leaves according to $\boldsymbol{q}_*$.

Lemma 4.2 states that messages at the end of WP are roughly distributed according to $\boldsymbol{q}_*$, but of course, $\boldsymbol{q}_*$ does not reflect the messages at the start of the WP algorithm; our initialisation, in which all messages are $\mathtt{s}$, is represented by the message distribution $\boldsymbol{q}_0 = (\boldsymbol{q}_0^{(v)}, \boldsymbol{q}_0^{(c)}) := ((0,1,0),(0,1,0))$, but as the WP algorithm proceeds, the distribution will change, which motivates the following definition of an update function on message distributions.

Definition 4.3. *Given a message distribution $\boldsymbol{q} = \left(\left(q_{\mathtt{f}}^{(v)}, q_{\mathtt{s}}^{(v)}, q_{\mathtt{u}}^{(v)}\right), \left(q_{\mathtt{f}}^{(c)}, q_{\mathtt{s}}^{(c)}, q_{\mathtt{u}}^{(c)}\right)\right)$, let us define the message distribution $\varphi(\boldsymbol{q})$ by setting*

$$\varphi(\boldsymbol{q})_{\mathtt{f}}^{(v)} := \mathbb{P}\left[\mathrm{Po}\left(d\left(q_{\mathtt{u}}^{(c)} + q_{\mathtt{s}}^{(c)}\right)\right) = 0\right], \qquad \varphi(\boldsymbol{q})_{\mathtt{f}}^{(c)} := \mathbb{P}\left[\mathrm{Po}\left(d\, q_{\mathtt{f}}^{(v)}\right) \geq 1\right],$$

$$\varphi(\boldsymbol{q})_{\mathtt{s}}^{(v)} := \mathbb{P}\left[\mathrm{Po}\left(d\, q_{\mathtt{u}}^{(c)}\right) = 0\right] \cdot \mathbb{P}\left[\mathrm{Po}\left(d\, q_{\mathtt{s}}^{(c)}\right) \geq 1\right], \qquad \varphi(\boldsymbol{q})_{\mathtt{s}}^{(c)} := \mathbb{P}\left[\mathrm{Po}\left(d\, q_{\mathtt{f}}^{(v)}\right) = 0\right] \cdot \mathbb{P}\left[\mathrm{Po}\left(d\, q_{\mathtt{s}}^{(v)}\right) \geq 1\right],$$

$$\varphi(\boldsymbol{q})_{\mathtt{u}}^{(v)} := \mathbb{P}\left[\mathrm{Po}\left(d\, q_{\mathtt{u}}^{(c)}\right) \geq 1\right], \qquad \varphi(\boldsymbol{q})_{\mathtt{u}}^{(c)} := \mathbb{P}\left[\mathrm{Po}\left(d\left(q_{\mathtt{f}}^{(v)} + q_{\mathtt{s}}^{(v)}\right)\right) = 0\right].$$

We further recursively define $\varphi^{\circ t}(\boldsymbol{q}) := \varphi\left(\varphi^{\circ(t-1)}(\boldsymbol{q})\right)$ for $t \geq 2$, and define $\varphi^*(\boldsymbol{q}) := \lim_{t\to\infty} \varphi^{\circ t}(\boldsymbol{q})$ if this limit exists.

The function φ represents an update function of the WP message distributions in an idealised scenario, but it turns out that this idealised scenario is close to the truth. The following lemma is critical in order to be able to apply the results of [11, 21]. Let us define the total variation distance between message distributions $\boldsymbol{q}_1, \boldsymbol{q}_2$ by

$$d_{TV}\left(\boldsymbol{q}_1, \boldsymbol{q}_2\right) := d_{TV}\left(\boldsymbol{q}_1^{(v)}, \boldsymbol{q}_2^{(v)}\right) + d_{TV}\left(\boldsymbol{q}_1^{(c)}, \boldsymbol{q}_2^{(c)}\right).$$

Lemma 4.4. *We have $\varphi^*\left(\boldsymbol{q}_0\right) = \boldsymbol{q}_*$. Furthermore, there exist $\varepsilon, \delta > 0$ such that for any message distribution $\boldsymbol{q}$ which satisfies $d_{TV}\left(\boldsymbol{q}, \boldsymbol{q}_*\right) \leq \varepsilon$, we have $d_{TV}\left(\varphi\left(\boldsymbol{q}\right), \boldsymbol{q}_*\right) \leq (1-\delta) d_{TV}\left(\boldsymbol{q}, \boldsymbol{q}_*\right)$.*

In the language of [11, 21], this lemma states that $\boldsymbol{q}_*$ is the *stable limit* of $\boldsymbol{q}_0$. Before proving this lemma, we first show how to use it to prove Lemma 4.2. We begin with the critical application of the main result of [11, 21]. Recall that $w(A, t)$ denote the messages after t iterations of WP on the Tanner graph $G(A)$ with all initial messages set as $\mathtt{s}$, and $w(A) = \lim_{t\to\infty} w(A, t)$.

Lemma 4.5. *For any $d, \delta > 0$ there exists $t_0 \in \mathbb{N}$ such that w.h.p. $w(\boldsymbol{A})$ and $w(\boldsymbol{A}, t_0)$ are identical except on a set of at most δn edges.*

Proof. Since $\boldsymbol{q}_*$ is the stable limit of $\boldsymbol{q}_0$, this follows directly from [11, Theorem 1.5], [21, Theorem 1.3]. □

Using Lemma 4.5, we can determine the local limit of the graph with final WP messages.

Proof of Lemma 4.2. Fix t_0 sufficiently large, and in particular large enough that Lemma 4.5 can be applied. Since the local structure of the graph $G(\boldsymbol{A})$ is that of a $\mathrm{Po}(d)$ branching tree, after t_0 iterations of WP for some sufficiently large t_0, the local structure with incoming messages is approximately as $\mathscr{T}_{t_0}$ and $\hat{\mathscr{T}}_{t_0}$. Subsequently, Lemma 4.5 implies that almost all messages at time t_0 are the final ones, and in particular there are very few vertices whose depth t_0 neighbourhood will change. □

Proof of Lemma 4.4. For convenience, we will actually prove that $\boldsymbol{q}_*$ is the stable limit of $\boldsymbol{q}_0$ under the operator $\varphi^{\circ 2}$ rather than φ – the advantage is that this 2-step operator acts on the coordinates (corresponding to variable and check nodes) independently of each other. The analogous statement for φ follows from that for $\varphi^{\circ 2}$ due to continuity.

Furthermore, by symmetry we may prove the appropriate statements just for the first coordinate, i.e. for $\boldsymbol{q}_*^{(v)}$ – the corresponding proof for $\boldsymbol{q}_*^{(c)}$ is essentially identical.

As a final reduction, let us observe that since for any message distribution we have $q_{\mathtt{f}}^{(v)} + q_{\mathtt{s}}^{(v)} + q_{\mathtt{u}}^{(v)} = 1$, it is sufficient to consider just two of the three coordinates. In this case it will be most convenient to consider $q_{\mathtt{f}}^{(v)}$ and $q_{\mathtt{u}}^{(v)}$, so let us restate what we are aiming to prove.

Consider the operator $\tilde{\varphi}:[0,1]^2\to[0,1]^2$ defined by $\tilde{\varphi}(x_1,x_2):=\big(\tilde{\varphi}_1(x_1),\tilde{\varphi}_2(x_2)\big)$, where

$$\tilde{\varphi}_1(x_1):=\exp\big(-d\exp(-dx_1)\big),\qquad \tilde{\varphi}_2(x_2):=1-\exp\big(-d\exp(-d(1-x_2))\big).$$

This corresponds precisely to the action of $\varphi^{\circ 2}$ on $\Big(q_{\mathtt{f}}^{(v)},q_{\mathtt{u}}^{(v)}\Big)$. Thus our goal is to prove that $(1-\alpha^*,\alpha_*)$ is the stable limit of $(0,0)$ under $\tilde{\varphi}$.

Now observe that $\tilde{\varphi}_1(x_1)=1-\phi_d(1-x_1)$ and recall that ϕ_d was defined in (1.1). By Lemma 2.2 and Proposition 2.3, ϕ_d is a contraction on $[\alpha^*,1]$ with unique fixed point α^*, and so correspondingly $\tilde{\varphi}_1$ is a contraction on $[0,1-\alpha^*]$ with unique fixed point $1-\alpha^*$.

On the other hand, $\tilde{\varphi}_2$ is exactly the function ϕ_d. Therefore, similarly, by Lemma 2.2 and Proposition 2.3, $\tilde{\varphi}_2$ is a contraction on $[0,\alpha_*]$ with unique fixed point α_*. It follows that $(1-\alpha_*,\alpha_*)$ is the limit $\tilde{\varphi}^*(0,0)$.

To show that it is the *stable* limit, we simply observe that $\tilde{\varphi}_1'(1-\alpha^*)=\phi_d'(\alpha^*)<1$ by Proposition 2.3, and similarly $\tilde{\varphi}_2'(\alpha_*)=\phi_d'(\alpha_*)<1$. This implies that each coordinate function is a contraction in the neighbourhood of the corresponding limit point, and therefore so is $\tilde{\varphi}$. □

4.2. **Proof of Proposition 2.5.** To determine the asymptotic proportion of vertices in $V_{\mathtt{f}}(\boldsymbol{A})$, by Lemma 4.2 it suffices to determine the probability that in $\mathscr{T}$ the root receives at least one `f`-message. This event has probability

$$\mathbb{P}\Big[\mathrm{Po}(d(q_{*,\mathtt{f}}^{(v)}))\geq 1\Big]=1-\exp(-d(1-\alpha^*))=\alpha_*$$

since $q_{*,\mathtt{f}}^{(v)}=1-\alpha^*$ and by (3.9).

An analogous argument yields the statement for $V_{\mathtt{u}}(\boldsymbol{A})$. □

4.3. **Proof of Proposition 2.6.** To determine the asymptotic proportion of vertices in $V_{\mathtt{s}}(\boldsymbol{A})$, by Lemma 4.2 it suffices to determine the probability that in $\mathscr{T}$ the root receives at least two `s`-messages and no `f`-messages. This occurs with probability

$$\begin{aligned}\mathbb{P}\big[\mathrm{Po}(d(\alpha^*-\alpha_*))\geq 2\big]\cdot\mathbb{P}\left[\mathrm{Po}(d\alpha_*)=0\right]&=\big(1-\exp(-d(\alpha^*-\alpha_*))-d(\alpha^*-\alpha_*)\exp(-d(\alpha^*-\alpha_*))\big)\cdot\exp(-d\alpha_*)\\&=\exp(-d\alpha_*)-\exp(-d\alpha^*)(1+d(\alpha^*-\alpha_*)),\end{aligned}$$

as claimed. The analogous statement for $C_{\mathtt{s}}(\boldsymbol{A})$ can be proved similarly, or follows from the statement for $V_{\mathtt{s}}(\boldsymbol{A})$ by symmetry.

The statement on degree distributions follows directly from the approximation using $\mathscr{T}$ or $\hat{\mathscr{T}}$: conditioned on a node lying in $V_{\mathtt{s}}$ or $C_{\mathtt{s}}$, it must certainly receive at least two `s`-messages from its neighbours. Furthermore, a neighbour is in $C_{\mathtt{s}}$ or $V_{\mathtt{s}}$ respectively if and only if it sends an `s`-message to this vertex. The distribution of neighbours sending `s` is $\mathrm{Po}(\lambda)$ without the conditioning (where recall that $\lambda=d(\alpha^*-\alpha_*)$), therefore with the conditioning it is $\mathrm{Po}_{\geq 2}(\lambda)$, as required. □

4.4. **Proof of Proposition 2.4.** For a matrix A we let

$$V_{\mathtt{f}}(A,t)=\{v\in V(A):\exists a\in\partial v: w_{a\to v}(A,t)=\mathtt{f}\},\qquad V_{\mathtt{u}}(A,t)=\{v\in V(A):\forall a\in\partial v: w_{a\to v}(A,t)=\mathtt{u}\},\tag{4.1}$$

$$C_{\mathtt{f}}(A,t)=\{a\in C(A):\forall v\in\partial a: w_{v\to a}(A,t)=\mathtt{f}\},\qquad C_{\mathtt{u}}(A,t)=\{a\in C(A):\exists v\in\partial a: w_{v\to a}(A,t)=\mathtt{u}\}\tag{4.2}$$

be the sets of nodes of $G(A)$ classified as frozen or unfrozen after t iterations of WP. Furthermore, let $B(v,t)$ denote the nodes that are within distance t of v. Let $\mathscr{B}_t$ be the set of variable nodes v such that $B(v,t)$ contains at least one cycle.

Claim 4.6. *Let $t_0\geq 1$. If $v_0\in V_{\mathtt{u}}(A,t_0)$ and $v_0\notin\mathscr{B}_{t_0}$, then $v_0\notin\mathscr{F}(A)$.*

Proof. Let $v_0\in V_{\mathtt{u}}(A,t_0)$. We will consider a subtree T of $G(A)$ rooted at v_0 which we produce in the following way. All of the neighbours of v_0 are added to T as children of v_0. Furthermore, since each such neighbour a is a check node which sends v_0 a `u`-message at time t_0, the check node a has at least one further neighbour (apart from v_0) from which it receives a `u`-message at time t_0-1 – we choose one such neighbour arbitrarily and add it to T as a child of a. We continue recursively, for each variable node adding all neighbours (apart from the parent) if there are any, and for each check node at depth i adding one neighbour (distinct from the parent) from which it receives message `u` at time t_0-i.

Since the leaves at depth t_0 send out `u`-messages at time 1, they must be unary variables (if they exist at all which is not the case if, for example, t_0 is odd). Therefore T has the property that for any of its variable nodes, all its neighbours are also in T, while all checks have precisely two neighbours in T.

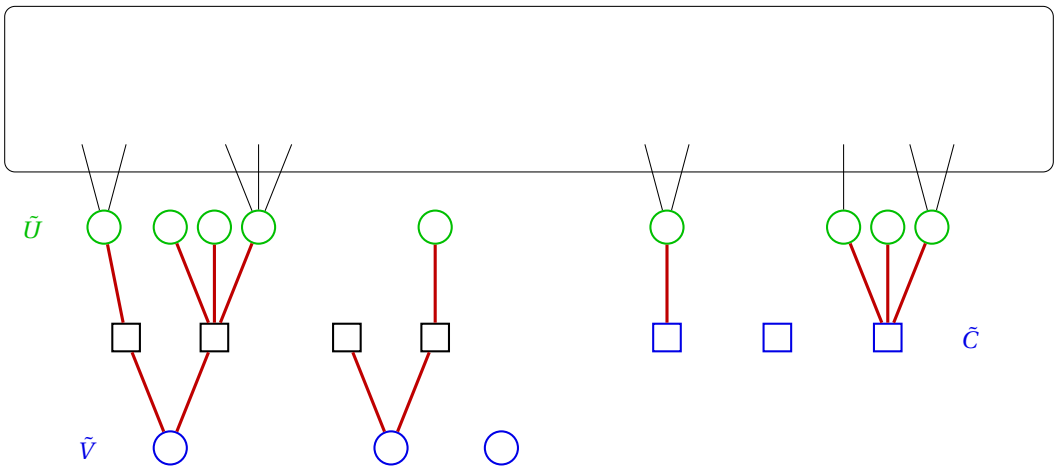

FIGURE 3. An instance of the randomly generated trees added to $G(\boldsymbol{A})$ to produce $G'(\boldsymbol{A})$ in Definition 5.1: the variable and check root sets $\tilde{V}, \tilde{C}$ are shown in blue; the attachment nodes $\tilde{U}$ in green; the thick red edges are those in the trees, which are added to $G(\boldsymbol{A})$; the thin black edges were already present in $G(\boldsymbol{A})$; all explicitly drawn nodes were already present but, apart from possibly the attachment nodes (i.e. those in $\tilde{U}$), were previously isolated in $G(\boldsymbol{A})$.

Therefore we can obtain a vector in the kernel of A that sets x_{v_0} to 1 by simply setting all the variable nodes in T to 1 and all other variables to zero. This shows that $v_0 \notin \mathscr{F}(A)$.

□

Proof of Proposition 2.4. First observe that Claim 4.6 implies $V_{\mathrm{u}}(A, t_0) \bigcap \mathscr{F}(A) \subseteq \mathscr{B}_{t_0}$. Calculating the expectation of the number of vertices lying on cycles of length up to $2t_0$ and applying Markov inequality gives us that indeed $|\mathscr{B}_{t_0}| = o(n)$. By choosing t_0 sufficiently large according to Lemma 4.5 we have $|V_{\mathrm{u}}(A, t_0)| = |V_{\mathrm{u}}(A)| + o(n)$ w.h.p. which concludes the proof. □

5. THE STANDARD MESSAGES

In this section we prove Proposition 2.7, which states that the proportion of frozen variables is likely close to one of the fixed points of ϕ_d. Along the way we will establish auxiliary statements that will pave the way for the proof of Proposition 2.8 (which rules out the unstable fixed point) in Section 6 as well.

5.1. **Perturbing the Tanner graph.** A key observation toward Proposition 2.7 is that if we make some minor alterations to $G(\boldsymbol{A})$, the resulting graph $G'(\boldsymbol{A})$ is essentially indistinguishable from $G(\boldsymbol{A})$. Let $\mathbb{T} = \mathbb{T}(d)$ be the tree generated by a Galton-Watson process with the two types 'variable node' and 'check node'. The root is a variable node v_0. Each variable node spawns $\mathrm{Po}(d)$ check nodes as offspring. Similarly, the offspring of a check node consists of $\mathrm{Po}(d)$ variable nodes. In addition, let $\hat{\mathbb{T}} = \hat{\mathbb{T}}(d)$ be the tree generated by a Galton-Watson process with the same offspring distribution whose root is a check node a_0. Given an integer t, we obtain $\mathbb{T}_t$ and $\hat{\mathbb{T}}_t$ from $\mathbb{T}$ and $\hat{\mathbb{T}}$, respectively, by deleting all nodes whose distance from the root exceeds t, so these are trees of depth (at most) t. (Unlike the branching processes from Definition 4.1, the trees $\mathbb{T}, \hat{\mathbb{T}}$ do not incorporate messages.)

Definition 5.1. *Let $0 \le \omega_1 = \omega_1(n) = o(\sqrt{n})$, $0 \le \omega_2 = \omega_2(n) = n^{1/2-\Omega(1)}$ and obtain $G'(\boldsymbol{A})$ from $G(\boldsymbol{A})$ as follows.*

(i) Generate ω_1 many $\mathbb{T}_2$ trees and ω_2 many $\hat{\mathbb{T}}_1$ trees independently.
(ii) For each node v in the final layer of these trees (which is a variable node), embed v onto a variable node of $G(\boldsymbol{A})$ chosen uniformly at random and independently.
(iii) Embed the remaining nodes of the trees randomly onto nodes which were previously isolated such that variable nodes are embedded onto variable nodes and checks onto checks.

Let $G'(\boldsymbol{A})$ denote the resulting graph and let $\boldsymbol{A}'$ be its adjacency matrix. (Thus $G'(\boldsymbol{A}) = G(\boldsymbol{A}')$ is the Tanner graph of $\boldsymbol{A}'$.)

Let $\tilde{V}, \tilde{C}$ denote the set of variable and check nodes of $G'(\boldsymbol{A})$ respectively onto which the roots of the $\mathbb{T}_2$ and $\hat{\mathbb{T}}_1$ branching trees from Definition 5.1 (i) are embedded. Similarly, let $\tilde{U} = (\partial\tilde{C} \cup \partial^2\tilde{V}) \setminus \tilde{V}$ be the set of variable nodes of $G(\boldsymbol{A})$ where the checks from Definition 5.1 attach to the bulk of the Tanner graph in Step (ii). An example is shown in Figure 3.

Note that it is possible that this process fails, for example if there are not enough isolated nodes available, in which case we simply set $G'(\boldsymbol{A}) := G(\boldsymbol{A})$. However, since w.h.p. the total size of all trees is $O(\omega_1 + \omega_2)$, and w.h.p. there are $\Omega(n)$ isolated variable and check nodes available, the failure probability is $\exp(-\Omega(n))$ and thus negligible for our purposes. For the same reason w.h.p. no two nodes from the trees are embedded onto the same node of $G(\boldsymbol{A})$.

Fact 5.2. *If $\omega_1 + \omega_2 = n^{1/2-\Omega(1)}$, then $d_{\mathrm{TV}}(G(\boldsymbol{A}), G'(\boldsymbol{A})) = n^{-\Omega(1)}$.*

This routine observation simply follows from the fact that w.h.p. we only added $n^{1/2-\Omega(1)}$ edges attached to isolated nodes in such a way that the expected degrees are bounded, and the attachment variables were chosen uniformly at random. In particular the number of changes is of lower order than the standard deviation in the number of nodes of each type which has changed.

We point out that $\tilde{V}, \tilde{C}$ are representative of $G'(\boldsymbol{A})$ as a whole.

Fact 5.3. *Let $\Lambda : (G, u) \mapsto \Lambda(G, u) \in [0, 1]$ be any function that maps a pair consisting of a graph and a node to a number. If $1 \ll \omega_1, \omega_2 = n^{1/2-\Omega(1)}$, then*

$$\mathbb{E}\left|\frac{1}{n}\sum_{v \in V(G'(\boldsymbol{A}))} \Lambda(G'(\boldsymbol{A}), v) - \frac{1}{|\tilde{V}|}\sum_{v \in \tilde{V}} \Lambda(G'(\boldsymbol{A}), v)\right| = o(1), \quad \mathbb{E}\left|\frac{1}{n}\sum_{a \in C(G'(\boldsymbol{A}))} \Lambda(G'(\boldsymbol{A}), a) - \frac{1}{|\tilde{C}|}\sum_{a \in \tilde{C}} \Lambda(G'(\boldsymbol{A}), a)\right| = o(1).$$

Proof. The statement for $\tilde{V}$ follows since the local structure of $G(\boldsymbol{A})$, and therefore also of $G'(\boldsymbol{A})$ by Fact 5.2, is that of a $\mathrm{Po}(d)$ branching tree, and this is clearly also the case at the variables of $\tilde{V}$. Formally, if $\boldsymbol{v}$ is a variable node chosen uniformly at random from $V(G'(\boldsymbol{A}))$ and $\tilde{\boldsymbol{v}}$ is a random element of $\tilde{V}$, then Fact 5.2 implies that $(G'(\boldsymbol{A}), \boldsymbol{v})$ and $(G'(\boldsymbol{A}), \tilde{\boldsymbol{v}})$ have total variation distance $o(1)$ given $G'(\boldsymbol{A})$ w.h.p. Therefore, the empirical average of Λ on the entire set $V(G'(\boldsymbol{A}))$ is well approximated by the average on $\tilde{V}$ w.h.p. The second statement concerning $\tilde{C}$ follows similarly. □

5.2. **Construction of the standard messages.** In Section 2.2 we defined Warning Propagation messages via an explicit combinatorial construction that captured our intuition as to the causes of freezing. In the following we pursue a converse path. We define a set of messages implicitly, purely in terms of algebraic reality. We call these $\{\mathtt{f},\mathtt{u}\}$-valued messages the *standard messages*. The battle plan is to ultimately match this implicit definition with the explicit construction from Section 2.2.

The standard messages can be defined for any $m \times n$-matrix A. Given a subset U of nodes of a graph G, we denote by $G - U$ the graph obtained from G by deleting U and all incident edges. For a node x, we write $G - x$ instead of $G - \{x\}$. For each adjacent variable/check pair (v, a) of $G(A)$ we define

$$\mathfrak{m}_{v\to a}(A) = \begin{cases} \mathtt{f} & \text{if } v \text{ is frozen in } G(A) - a, \\ \mathtt{u} & \text{otherwise,} \end{cases} \qquad \mathfrak{m}_{a\to v}(A) = \begin{cases} \mathtt{f} & \text{if } v \text{ is frozen in } G(A) - (\partial v \setminus \{a\}), \\ \mathtt{u} & \text{otherwise.} \end{cases} \tag{5.1}$$

Hence, $\mathfrak{m}_{v\to a}(A) = \mathtt{f}$ iff v is frozen in the matrix obtained from A by deleting the a-row. Moreover, $\mathfrak{m}_{a\to v}(A) = \mathtt{f}$ iff v is frozen in the matrix obtained by removing the rows of all $b \in \partial v$ except a. Let $\mathfrak{m}(A) = (\mathfrak{m}_{v\to a}(A), \mathfrak{m}_{a\to v}(A))_{v\in\partial a}$.

Further, we define $\{\mathtt{f}, \star, \mathtt{u}\}$-valued marks for the variables and checks by letting

$$\mathfrak{m}_v(A) = \begin{cases} \mathtt{f} & \text{if } \mathfrak{m}_{a\to v}(A) = \mathtt{f} \text{ for at least two } a \in \partial v, \\ \star & \text{if } \mathfrak{m}_{a\to v}(A) = \mathtt{f} \text{ for precisely one } a \in \partial v, \\ \mathtt{u} & \text{otherwise,} \end{cases} \tag{5.2}$$

$$\mathfrak{m}_a(A) = \begin{cases} \mathtt{f} & \text{if } \mathfrak{m}_{v\to a}(A) = \mathtt{f} \text{ for all } v \in \partial a, \\ \star & \text{if } \mathfrak{m}_{v\to a}(A) = \mathtt{f} \text{ for all but precisely one } v \in \partial a, \\ \mathtt{u} & \text{otherwise.} \end{cases} \tag{5.3}$$

The intended semantics is that $\mathtt{f}$ and $\star$ both represent frozen variables/checks, meaning that a variable v is frozen if $\mathfrak{m}_v(A) \neq \mathtt{u}$ while for any check a we have $\mathfrak{m}_a(A) \neq \mathtt{u}$ if all variables $v \in \partial a$ are frozen. But for checks or variables with mark $\star$, freezing hangs by a thread since, for instance, a variable v with $\mathfrak{m}_v(A) = \star$ receives just a single 'freeze'

message. We will see in Corollary 5.6 below how this manifests itself in the messages sent out by $\star$-variables or checks.

We consider a dumbed-down version of the Warning Propagation operator WP_A from Section 2.2 that "updates" the messages from (5.1) to messages $\hat{\mathfrak{m}}_{v\to a}(A)$ as follows:

$$\hat{\mathfrak{m}}_{v\to a}(A) = \begin{cases} \mathtt{f} & \text{if } \mathfrak{m}_{b\to v}(A) = \mathtt{f} \text{ for some } b \in \partial v \setminus \{a\}, \\ \mathtt{u} & \text{otherwise,} \end{cases} \tag{5.4}$$

$$\hat{\mathfrak{m}}_{a\to v}(A) = \begin{cases} \mathtt{f} & \text{if } \mathfrak{m}_{y\to a}(A) = \mathtt{f} \text{ for all } y \in \partial a \setminus \{v\}, \\ \mathtt{u} & \text{otherwise.} \end{cases} \tag{5.5}$$

We next show that the standard messages constitute an approximate fixed point of the $\mathrm{WP}_{\boldsymbol{A}}$ operator and that the marks mostly match their intended semantics w.h.p.

Lemma 5.4. *For all $d > 0$ we have*

$$\mathbb{E} \sum_{\substack{v \in V(\boldsymbol{A}) \\ a \in \partial v}} \mathbf{1}\{\mathfrak{m}_{v\to a}(\boldsymbol{A}) \neq \hat{\mathfrak{m}}_{v\to a}(\boldsymbol{A})\} + \mathbf{1}\{\mathfrak{m}_{a\to v}(\boldsymbol{A}) \neq \hat{\mathfrak{m}}_{a\to v}(\boldsymbol{A})\} = o(n), \tag{5.6}$$

$$\mathbb{E}|\{v \in V(\boldsymbol{A}) : \mathfrak{m}_v(\boldsymbol{A}) \neq \mathtt{u}\} \triangle \mathscr{F}(\boldsymbol{A})| = o(n), \qquad \mathbb{E}\left|\{a \in C(\boldsymbol{A}) : \mathfrak{m}_a(\boldsymbol{A}) \neq \mathtt{u}\} \triangle \hat{\mathscr{F}}(\boldsymbol{A})\right| = o(n). \tag{5.7}$$

We prove Lemma 5.4 by way of the perturbation from Section 5.1. Specifically, in light of Fact 5.3 it suffices to consider $G'(\boldsymbol{A})$ and the sets of variables/checks $\tilde{V}, \tilde{C}$ onto which the roots of the $\mathbb{T}_2$ and $\hat{\mathbb{T}}_1$ branching trees from Definition 5.1 are embedded. The following lemma summarises the main step of the argument. Recall that $\tilde{U}$ is the set of variable nodes where the trees from Definition 5.1 attach to the bulk of the Tanner graph in Step (ii) (see Figure 3).

Claim 5.5. *There exists $1 \ll \omega^* = \omega^*(n) \leq n^{1/2-\Omega(1)}$ such that for all $\omega_1, \omega_2 \leq \omega^*$ and every $d > 0$ w.h.p. we have*

$$\mathfrak{m}_{y\to a}(\boldsymbol{A}') = \mathtt{f} \;\Leftrightarrow\; y \in \mathscr{F}(\boldsymbol{A}) \qquad \text{for all } a \in \tilde{C} \cup \partial\tilde{V},\ y \in \tilde{U} \cap \partial a. \tag{5.8}$$

Furthermore, w.h.p. a random vector $\boldsymbol{x} \in \ker \boldsymbol{A}$ satisfies

$$\mathbb{P}\left[\forall y \in \tilde{U} \setminus \mathscr{F}(\boldsymbol{A}) : \boldsymbol{x}_y = \sigma_y \mid G(\boldsymbol{A}), G'(\boldsymbol{A})\right] = 2^{-|\tilde{U}\setminus\mathscr{F}(\boldsymbol{A})|} \qquad \text{for all } \sigma \in \mathbb{F}_2^{\tilde{U}\setminus\mathscr{F}(\boldsymbol{A})}. \tag{5.9}$$

Finally, $\mathscr{F}(\boldsymbol{A}) \subseteq \mathscr{F}(\boldsymbol{A}')$ and w.h.p. we have $f(\boldsymbol{A}') = f(\boldsymbol{A}) + o(1)$.

Proof. Let us begin with the last statement. The inclusion $\mathscr{F}(\boldsymbol{A}) \subseteq \mathscr{F}(\boldsymbol{A}')$ is deterministically true because $\boldsymbol{A}'$ is obtained from $\boldsymbol{A}$ by effectively adding checks (viz. "activating" formerly dormant isolated checks). Moreover, Proposition 2.11 shows that the distribution of a random $\boldsymbol{x} \in \ker \boldsymbol{A}$ is $n^{-\Omega(1)}$-symmetric w.h.p. Since $\boldsymbol{A}'$ is obtained from $\boldsymbol{A}$ by adding no more than $O(\omega^*)$ checks w.h.p. and since any additional check reduces the nullity by at most one, the distributions of a uniformly random $\boldsymbol{x}' \in \ker \boldsymbol{A}'$ and of $\boldsymbol{x}$ are mutually $2^{O(\omega_*)}$-contiguous w.h.p. Therefore, Proposition 2.16 implies that w.h.p.

$$\Delta_\square(\boldsymbol{x}, \boldsymbol{x}') = o(1), \tag{5.10}$$

provided that $\omega_*(n)$ grows sufficiently slowly. Finally, since the marginals of the individual entries $\boldsymbol{x}_i, \boldsymbol{x}'_i$ are either uniform or place all mass on zero by Fact 2.17, (2.14) and (5.10) yield

$$f(\boldsymbol{A}') - f(\boldsymbol{A}) = \frac{1}{n}\sum_{i=1}^n \mathbf{1}\{v_i \in \mathscr{F}(\boldsymbol{A}')\} - \mathbf{1}\{v_i \in \mathscr{F}(\boldsymbol{A})\} \leq \frac{2}{n}\sum_{i=1}^n d_{\mathrm{TV}}(\boldsymbol{x}_i, \boldsymbol{x}'_i) \leq 4\Delta_\square(\boldsymbol{x}, \boldsymbol{x}') = o(1). \tag{5.11}$$

The other two assertions (5.8) and (5.9) follow from similar deliberations. Indeed, to prove (5.9) we observe that given $G(\boldsymbol{A})$ the set $\tilde{U}$ of variable nodes where the bottom layers of the trees from Definition 5.1 attach in Step (ii) is just a uniformly random set of $O(\omega^*)$ variable nodes of $G(\boldsymbol{A})$. Therefore, providing $\omega^* \to \infty$ sufficiently slowly, Proposition 2.11 shows that w.h.p.

$$\mathbb{P}\left[\forall y \in \tilde{U} \setminus \mathscr{F}(\boldsymbol{A}) : \boldsymbol{x}_y = \sigma_y \mid G(\boldsymbol{A}), G'(\boldsymbol{A})\right] - 2^{-|\tilde{U}\setminus\mathscr{F}(\boldsymbol{A})|} = O(n^{-\Omega(1)}) \qquad \text{for any } \sigma \in \mathbb{F}_2^{\tilde{U}\setminus\mathscr{F}(\boldsymbol{A})}. \tag{5.12}$$

Now, the projections of the vectors $x \in \ker \boldsymbol{A}$ onto the coordinates in $\tilde{U}\setminus\mathscr{F}(\boldsymbol{A})$ form a subspace of $\mathbb{F}_2^{\tilde{U}\setminus\mathscr{F}(\boldsymbol{A})}$. Assuming that $|\tilde{U}| = O(\omega^*)$ and that $\omega^* \to \infty$ sufficiently slowly, (5.12) implies that the dimension of this subspace equals $|\tilde{U} \setminus \mathscr{F}(\boldsymbol{A})|$. Hence we obtain (5.9).

Regarding (5.8), fix some check $a \in \tilde{C} \cup \partial\tilde{V}$ and think of $G'(\boldsymbol{A})$, and therefore also its adjacency matrix $\boldsymbol{A}'$, as being constructed in two steps. In the first step we embed all the other new checks $b \in (\tilde{C} \cup \partial\tilde{V}) \setminus \{a\}$ and insert the edges that join them to the variable nodes of $G(\boldsymbol{A})$. Let $G''(\boldsymbol{A})$ be the outcome of this first step and let $\boldsymbol{A}''$ be its adjacency matrix. Subsequently we independently choose the set of neighbours $\partial a \setminus \tilde{V}$ among the variable nodes of $G(\boldsymbol{A})$ to obtain $G'(\boldsymbol{A})$. Let $\boldsymbol{x}''$ be a random element of $\ker \boldsymbol{A}''$. Repeating the argument towards (5.10) we see that $\Delta_\square(\boldsymbol{x}, \boldsymbol{x}'') = o(1)$ w.h.p. Hence, repeating the steps of (5.11) we conclude that $|\mathscr{F}(\boldsymbol{A}) \triangle \mathscr{F}(\boldsymbol{A}'')| = o(n)$ w.h.p. Since in our two-round exposure $\partial a \setminus \tilde{V}$ is independent of $\boldsymbol{A}''$, we thus conclude that $\partial a \cap \mathscr{F}(\boldsymbol{A}'') \setminus \tilde{V} = \partial a \cap \mathscr{F}(\boldsymbol{A}) \setminus \tilde{V}$ w.h.p. Hence, the definition (5.1) of the standard messages implies (5.8). □

Proof of Lemma 5.4. By Fact 5.3 it suffices to prove the fixed point conditions for the variables and checks $\tilde{V}, \tilde{C}$ of $G'(\boldsymbol{A})$ which are the roots of the $\mathbb{T}_2$ and $\hat{\mathbb{T}}_1$ branching processes added in Definition 5.1. Hence, with ω^* from in Claim 5.5 let $\omega_1 = \omega_*$ and $\omega_2 = 0$ and assume that (5.8)–(5.9) are satisfied. We may also assume that the subgraph of $G'(\boldsymbol{A})$ induced on $\mathscr{X} = \tilde{V} \cup \tilde{U} \cup \partial\tilde{V}$ is acyclic. Pick a variable $v \in \tilde{V}$ and an adjacent check $a \in \partial v$. We will show that under the assumptions the fixed point property is satisfied deterministically.

The definition (5.1) of the standard messages provides that $\mathtt{m}_{a\to v}(\boldsymbol{A}') = \mathtt{f}$ iff v is frozen in $G' - (\partial v \setminus \{a\})$. A sufficient condition is that $\partial a \setminus \{v\} \subseteq \mathscr{F}(\boldsymbol{A})$. Conversely, if $\partial a \setminus (\{v\} \cup \mathscr{F}(\boldsymbol{A})) \neq \emptyset$, then (5.9) shows that v is unfrozen in $G'(\boldsymbol{A}) - (\partial v \setminus \{a\})$. For there exists $\sigma \in \ker \boldsymbol{A}$ such that $\sum_{y \in \partial a \setminus \{v\}} \sigma_y = 1$, and because the subgraph induced on $\mathscr{X}$ is acyclic this vector σ extends to a vector $\sigma' \in \ker \boldsymbol{A}'$ with $\sigma'_v = 1$. Hence, $v \notin \mathscr{F}(\boldsymbol{A}')$. Furthermore, (5.8) ensures that $\partial a \setminus \{v\} \subseteq \mathscr{F}(\boldsymbol{A})$ iff $\mathtt{m}_{y\to a}(\boldsymbol{A}') = \mathtt{f}$ for all $y \in \partial a \setminus \{v\}$. Hence, $\mathtt{m}_{a\to v}(\boldsymbol{A}') = \mathtt{f}$ iff $\mathtt{m}_{y\to a}(\boldsymbol{A}') = \mathtt{f}$ for all $y \in \partial a \setminus \{v\}$. In other words, we obtain

$$\mathtt{m}_{a\to v}(\boldsymbol{A}') = \hat{\mathtt{m}}_{a\to v}(\boldsymbol{A}') \qquad \text{for all } v \in \tilde{V},\ a \in \partial v. \tag{5.13}$$

A similar argument shows that

$$\mathtt{m}_{v\to a}(\boldsymbol{A}') = \hat{\mathtt{m}}_{v\to a}(\boldsymbol{A}') \qquad \text{for all } v \in \tilde{V},\ a \in \partial v. \tag{5.14}$$

Indeed, (5.1) guarantees that $\mathtt{m}_{v\to a}(\boldsymbol{A}') = \mathtt{f}$ if there is a check $b \in \partial v \setminus \{a\}$ such that $\partial b \setminus \{v\} \subseteq \mathscr{F}(\boldsymbol{A})$. Such a check satisfies $\mathtt{m}_{b\to v}(\boldsymbol{A}') = \mathtt{f}$, and thus (5.4) shows that $\hat{\mathtt{m}}_{v\to a}(\boldsymbol{A}') = \mathtt{f}$. Conversely, suppose that $\mathtt{m}_{v\to a}(\boldsymbol{A}') = \mathtt{u}$. Then (5.1) shows that v is unfrozen in $G'(\boldsymbol{A}) - a$. Hence, the kernel of the matrix obtained from $\boldsymbol{A}'$ by deleting the a-row contains a vector σ'' with $\sigma''_v = 1$. Therefore, any check $b \in \partial v \setminus a$ features a variable $y \in \partial b \setminus (\{v\} \cup \mathscr{F}(\boldsymbol{A}))$. Consequently, because the subgraph induced on $\mathscr{X}$ is acyclic, (5.9) implies that v is unfrozen in the subraph $G'(\boldsymbol{A}) - (\partial v \setminus \{b\})$ where the only check adjacent to v is b. Thus, $\mathtt{m}_{b\to v}(\boldsymbol{A}') = \mathtt{u}$. Finally, (5.4) shows that $\hat{\mathtt{m}}_{v\to a}(\boldsymbol{A}') = \mathtt{u}$.

The proof of (5.7) proceeds along similar lines. Indeed, $v \in \tilde{V}$ is frozen in $\boldsymbol{A}'$ if there exists a check $a \in \partial v$ such that $\partial a \setminus \{v\} \subseteq \mathscr{F}(\boldsymbol{A})$. Hence, (5.8) shows that the existence of a check $a \in \partial v$ with $\mathtt{m}_{a\to v}(\boldsymbol{A}') = \mathtt{f}$ is a sufficient condition for $v \in \mathscr{F}(\boldsymbol{A}')$. Conversely, (5.9) shows that the absence of such a check is a sufficient condition for $v \notin \mathscr{F}(\boldsymbol{A}')$. Thus, recalling the definition (5.2), we obtain the first part of (5.7).

To prove the second part we combine (5.6)–(5.7) with (5.14) to see that $a \in \hat{\mathscr{F}}(\boldsymbol{A}')$ iff there is at most one $y \in \partial a$ with $\mathtt{m}_{y\to a}(\boldsymbol{A}') = \mathtt{u}$. For clearly $a \in \hat{\mathscr{F}}(\boldsymbol{A}')$ if no such y exists, while if there is precisely one such y the presence of the check a will freeze this variable. Conversely, if at least two $y, y' \in \partial a$ satisfy $\mathtt{m}_{y\to a}(\boldsymbol{A}'), \mathtt{m}_{y'\to a}(\boldsymbol{A}') \neq \mathtt{f}$, then $a \notin \mathscr{F}(\boldsymbol{A}')$ due to (5.9). Thus, a glance at the definition (5.3) of $\mathtt{m}_a(\boldsymbol{A}')$ completes the proof of (5.7). □

Proposition 2.7 is a statement about the proportion of variables identified as frozen by WP; in order to prove this result, we will need to analyse the distribution of the numbers of incoming and outgoing messages of each type at a node. This motivates the following definitions.

Given a vector $L = (\ell_{\mathtt{uu}}, \ell_{\mathtt{uf}}, \ell_{\mathtt{fu}}, \ell_{\mathtt{ff}}) \in \mathbb{N}_0^4$ and $z \in \{\mathtt{f}, \star, \mathtt{u}\}$, let

$$\boldsymbol{\Delta}_A(z, L) = \sum_{v \in V(A)} \mathbf{1}\{\mathtt{m}_v(A) = z\} \prod_{x,y \in \{\mathtt{u},\mathtt{f}\}} \mathbf{1}\left\{\left|\left\{a \in \partial v : \mathtt{m}_{a\to v}(A) = x \text{ and } \mathtt{m}_{v\to a}(A) = y\right\}\right| = \ell_{xy}\right\},$$

$$\boldsymbol{\Gamma}_A(z, L) = \sum_{a \in C(A)} \mathbf{1}\{\mathtt{m}_a(A) = z\} \prod_{x,y \in \{\mathtt{u},\mathtt{f}\}} \mathbf{1}\left\{\left|\left\{v \in \partial a : \mathtt{m}_{v\to a}(A) = x \text{ and } \mathtt{m}_{a\to v}(A) = y\right\}\right| = \ell_{xy}\right\}.$$

These random variables count variables/checks with certain marks and given numbers of edges with specific incoming/outgoing messages. For instance, $\ell_{\mathtt{uf}}$ provides the number of edges with an incoming $\mathtt{u}$-message and an outgoing $\mathtt{f}$-message. Of course, for some choices of z and L the variables $\boldsymbol{\Delta}_A(z, L)$ and $\boldsymbol{\Gamma}_A(z, L)$ may equal zero deterministically. We can think of $\boldsymbol{\Delta}$ and $\boldsymbol{\Gamma}$ as generalised degrees, giving information not just about the number

of edges, but the number of edges with each type of message. The following corollary pinpoints the generalised degree distribution. For $\alpha, \hat{\alpha} \in [0,1]$ and $L = (\ell_{\mathtt{uu}}, \ell_{\mathtt{uf}}, \ell_{\mathtt{fu}}, \ell_{\mathtt{ff}}) \in \mathbb{N}_0^4$, we define

$$\mathfrak{d}(\hat{\alpha}, \mathtt{u}, L) = \mathbf{1}\{\ell_{\mathtt{fu}} = \ell_{\mathtt{uf}} = \ell_{\mathtt{ff}} = 0\} \cdot \mathbb{P}[\mathrm{Po}(d\hat{\alpha}) = 0] \cdot \mathbb{P}[\mathrm{Po}(d(1-\hat{\alpha})) = \ell_{\mathtt{uu}}], \tag{5.15}$$

$$\mathfrak{d}(\hat{\alpha}, \star, L) = \mathbf{1}\{\ell_{\mathtt{fu}} = 1, \ell_{\mathtt{uu}} = \ell_{\mathtt{ff}} = 0\} \cdot \mathbb{P}[\mathrm{Po}(d\hat{\alpha}) = 1] \cdot \mathbb{P}[\mathrm{Po}(d(1-\hat{\alpha})) = \ell_{\mathtt{uf}}], \tag{5.16}$$

$$\mathfrak{d}(\hat{\alpha}, \mathtt{f}, L) = \mathbf{1}\{\ell_{\mathtt{fu}} = \ell_{\mathtt{uu}} = 0, \ell_{\mathtt{ff}} \geq 2\} \cdot \mathbb{P}[\mathrm{Po}(d\hat{\alpha}) = \ell_{\mathtt{ff}}] \cdot \mathbb{P}[\mathrm{Po}(d(1-\hat{\alpha})) = \ell_{\mathtt{uf}}], \tag{5.17}$$

$$\mathfrak{g}(\alpha, \mathtt{u}, L) = \mathbf{1}\{\ell_{\mathtt{uf}} = \ell_{\mathtt{ff}} = 0, \ell_{\mathtt{uu}} \geq 2\} \cdot \mathbb{P}[\mathrm{Po}(d(1-\alpha)) = \ell_{\mathtt{uu}}] \cdot \mathbb{P}[\mathrm{Po}(d\alpha) = \ell_{\mathtt{fu}}], \tag{5.18}$$

$$\mathfrak{g}(\alpha, \star, L) = \mathbf{1}\{\ell_{\mathtt{uf}} = 1, \ell_{\mathtt{uu}} = \ell_{\mathtt{ff}} = 0\} \cdot \mathbb{P}[\mathrm{Po}(d(1-\alpha) = 1] \cdot \mathbb{P}[\mathrm{Po}(d\alpha) = \ell_{\mathtt{fu}}], \tag{5.19}$$

$$\mathfrak{g}(\alpha, \mathtt{f}, L) = \mathbf{1}\{\ell_{\mathtt{fu}} = \ell_{\mathtt{uf}} = \ell_{\mathtt{uu}} = 0\} \cdot \mathbb{P}[\mathrm{Po}(d(1-\alpha)) = 0] \cdot \mathbb{P}[\mathrm{Po}(d\alpha) = \ell_{\mathtt{ff}}]. \tag{5.20}$$

Corollary 5.6. *Let $d > 0$. For any $z \in \{\mathtt{f}, \star, \mathtt{u}\}$ and $L = (\ell_{\mathtt{uu}}, \ell_{\mathtt{uf}}, \ell_{\mathtt{fu}}, \ell_{\mathtt{ff}}) \in \mathbb{N}_0^4$ we have*

$$\lim_{n\to\infty} \frac{1}{n} \mathbb{E}\big[\big|\boldsymbol{\Delta}_{\boldsymbol{A}}(z, L) - \mathfrak{d}(\hat{f}(\boldsymbol{A}), z, L)\big| + \big|\boldsymbol{\Gamma}_{\boldsymbol{A}}(z, L) - \mathfrak{g}(f(\boldsymbol{A}), z, L)\big|\big] = 0, \tag{5.21}$$

$$\lim_{n\to\infty} \mathbb{E}\big[\big|f(\boldsymbol{A}) - \phi_d(f(\boldsymbol{A}))\big| + \big|\hat{f}(\boldsymbol{A}) - (1 + d(1-f(\boldsymbol{A})))\exp\big(-d(1-f(\boldsymbol{A}))\big)\big|\big] = 0.$$

Proof. In light of Fact 5.3 it once again suffices to prove the various estimates for the variables/checks from $\tilde{V}, \tilde{C}$. Hence, with ω^* from Claim 5.5 let $1 \ll \omega_1, \omega_2 \ll \omega^*$.

To prove the second part of (5.21) we consider a check $a \in \tilde{C}$. The construction in Definition 5.1 ensures that a randomly selected $\boldsymbol{k}(a) \sim \mathrm{Po}(d)$ random variable nodes of G as neighbours. Each of them belongs to $\mathscr{F}(\boldsymbol{A})$ with probability $f(\boldsymbol{A})$. Thus, $\boldsymbol{k}(a)$ decomposes into two independent Poisson variables $\boldsymbol{k}_{\mathtt{f}}(a)$ and $\boldsymbol{k}_{\mathtt{u}}(a)$ with means $f(\boldsymbol{A})d$ and $(1-f(\boldsymbol{A}))d$. Furthermore, the definition (5.3) of the marks ensures that the mark of a depends only on the incoming messages. Moreover, (5.3) implies together with (5.8) that w.h.p. over the choice of $\boldsymbol{A}$ for any fixed integers $\ell_{\mathtt{u}}, \ell_{\mathtt{f}} \geq 0$ we have

$$\mathbb{P}\big[\mathtt{m}_a(\boldsymbol{A}') = \mathtt{u},\, \boldsymbol{k}_{\mathtt{f}}(a) = \ell_{\mathtt{f}},\, \boldsymbol{k}_{\mathtt{u}}(a) = \ell_{\mathtt{u}} \mid \boldsymbol{A}\big] = \mathbf{1}\{\ell_{\mathtt{u}} \geq 2\}\mathbb{P}\big[\mathrm{Po}(d(1-f(\boldsymbol{A}))) = \ell_{\mathtt{u}}\big]\mathbb{P}\big[\mathrm{Po}(df(\boldsymbol{A})) = \ell_{\mathtt{f}}\big] + o(1). \tag{5.22}$$

Indeed, (5.3) ensures that $\mathtt{m}_a(\boldsymbol{A}') = \mathtt{u}$ only if a receives at least two $\mathtt{u}$-messages. Furthermore, as Fact 5.5 shows that $f(\boldsymbol{A}') = f(\boldsymbol{A}) + o(1)$ w.h.p., we can rewrite (5.22) as

$$\mathbb{P}\big[\mathtt{m}_a(\boldsymbol{A}') = \mathtt{u},\, \boldsymbol{k}_{\mathtt{f}}(a) = \ell_{\mathtt{f}},\, \boldsymbol{k}_{\mathtt{u}}(a) = \ell_{\mathtt{u}} \mid \boldsymbol{A}\big] = \mathbf{1}\{\ell_{\mathtt{u}} \geq 2\}\mathbb{P}\big[\mathrm{Po}(d(1-f(\boldsymbol{A}))) = \ell_{\mathtt{u}}\big]\mathbb{P}\big[\mathrm{Po}(df(\boldsymbol{A})) = \ell_{\mathtt{f}}\big] + o(1). \tag{5.23}$$

Since by the fixed point property from Lemma 5.4 the reverse messages sent out by a are determined by the incoming ones via (5.5) w.h.p., all messages returned by a check with mark $\mathtt{u}$ are $\mathtt{u}$ w.h.p. Therefore, (5.23) implies the second part of (5.21). Finally, we observe that the identity $\lim_{n\to\infty}\mathbb{E}\big|\hat{f}(\boldsymbol{A}) - (1+d(1-f(\boldsymbol{A})))\exp\big(-d(1-f(\boldsymbol{A}))\big)\big| = 0$ is equivalent to the statement that w.h.p. $\hat{f}(\boldsymbol{A}) = (1+d(1-f(\boldsymbol{A})))\exp\big(-d(1-f(\boldsymbol{A}))\big) + o(1)$, which actually follows from (5.7), (5.18) and (5.21) by summing over $L \in \mathbb{N}_0^4$. More precisely, (5.7) implies that w.h.p. $\hat{f}(\boldsymbol{A}) = n^{-1}|\{a : \mathtt{m}_a(\boldsymbol{A}) \neq \mathtt{u}\}| + o(1)$. Furthermore, by (5.21), w.h.p. for all but $o(n)$ check nodes a we have $\mathtt{m}_a(\boldsymbol{A}) \neq \mathtt{u}$ if and only if a is adjacent to no edge along which both messages are $\mathtt{u}$. A glance at (5.18) shows that the sum over all $L \in \mathbb{N}_0^4$ of $\mathfrak{g}(\alpha, \mathtt{u}, L)$ is simply $\mathbb{P}[\mathrm{Po}(d(1-\alpha)) \geq 2] = 1 - (1+d(1-\alpha))\exp(-d(1-\alpha))$. Considering the complement and substituting $\alpha = f(\boldsymbol{A})$, the result follows.

The first part of (5.21) also follows from similar deliberations. For example, for $x \in \tilde{V}$ we have $\mathtt{m}_x(\boldsymbol{A}') = \mathtt{u}$ iff $\mathtt{m}_{a\to x}(\boldsymbol{A}') = \mathtt{u}$ for all $a \in \partial x$. Furthermore, the fixed point property from Lemma 5.6 shows that w.h.p. $\mathtt{m}_{a\to x}(\boldsymbol{A}') = \mathtt{f}$ iff $y \in \mathscr{F}(\boldsymbol{A})$ for all $y \in \partial a \setminus \tilde{V}$. Since the variables y are chosen randomly and independently, we see that $\mathbb{P}[\mathtt{m}_{a\to x}(\boldsymbol{A}') = \mathtt{f} \mid \boldsymbol{A}] = \mathbb{P}\big[\mathrm{Po}(d(1-f(\boldsymbol{A}))) = 0\big] + o(1) = \exp(-d(1-f(\boldsymbol{A}))) + o(1) = \hat{f}(\boldsymbol{A}) + o(1)$ w.h.p. Because x has a total of $\mathrm{Po}(d)$ independent adjacent checks, we obtain (5.21) for $z = \mathtt{u}$; the cases $z = \mathtt{f}$ and $z = \star$ are analogous. Finally, the identity $f(\boldsymbol{A}) = \phi_d(f(\boldsymbol{A})) + o(1)$ w.h.p. follows from Fact 5.3, (5.7) and (5.21) by summing on $\ell_{\mathtt{uu}}$. □

Proof of Proposition 2.7. Fix a small $\varepsilon > 0$ and let $U(\varepsilon) = \{\alpha \in [0,1] : |\alpha - \alpha_*| \wedge |\alpha - \alpha_0| \wedge |\alpha - \alpha^*| > \varepsilon\}$. Then Lemma 2.2 shows that there exists an integer $t > 0$ such that $\big|\phi_d^{\circ t}(\alpha) - \alpha_*\big| \wedge \big|\phi_d^{\circ t}(\alpha) - \alpha^*\big| < \varepsilon/2$ for all $\alpha \in U(\varepsilon)$. Hence,

$$\big|\alpha - \phi_d^{\circ t}(\alpha)\big| > \varepsilon/2 \qquad \text{for all } \alpha \in U(\varepsilon). \tag{5.24}$$

By contrast, Corollary 5.6 shows that $\big|f(\boldsymbol{A}) - \phi_d(f(\boldsymbol{A}))\big| = o(1)$ w.h.p. Since $\phi_d(\cdot)$ is uniformly continuous on $[0,1]$, this implies that $\big|f(\boldsymbol{A}) - \phi_d^{\circ t}(f(\boldsymbol{A}))\big| = o(1)$ w.h.p. Hence, (5.24) shows that $\mathbb{P}\big[f(\boldsymbol{A}) \in U(\varepsilon)\big] = o(1)$. Because this holds for arbitrarily small $\varepsilon > 0$, the assertion follows. □

6. The unstable fixed point

Proposition 2.7 shows that $f(\boldsymbol{A})$ is close to one of the fixed points of the function ϕ_d w.h.p. The aim in this section is to prove Proposition 2.8 by using the "hammer and anvil" strategy described in Section 1.4.2 to rule out the unstable fixed point α_0. The proof is subtle and requires three steps. First we show that a random $\boldsymbol{x} \in \ker \boldsymbol{A}$ sets about half the unfrozen variables to one. Indeed, even if we weight the variable nodes by their degrees the overall weight of the one-entries comes to about half w.h.p. Therefore, (1.2) implies that $\ker \boldsymbol{A}$ contains $2^{\Phi_d(\alpha_*)n+o(n)}$ such balanced vectors w.h.p. This is the "anvil" part of the argument.

The "hammer" part consists of the next two steps showing that the existence of that many balanced solutions is actually unlikely if $f(\boldsymbol{A}) \sim \alpha_0$. We proceed by way of a sophisticated moment computation. Specifically, we estimate the number of fixed points of the operator from (5.4)–(5.5) that mark about $\alpha_0 n$ variable nodes unfrozen as per (5.2). This expectation turns out to be of order $\exp(o(n))$. Subsequently we compute the expected number of actual balanced solutions compatible with such a WP fixed point. The answer turns out to be $2^{\Phi_d(\alpha_0)n+o(n)}$. Since $\Phi_d(\alpha_0) < \Phi_d(\alpha_*) = \max_\alpha \Phi_d(\alpha)$, we conclude that a random matrix with $f(\boldsymbol{A}) \sim \alpha_0$ would have far fewer "balanced" vectors in its kernel than the anvil part of the argument demands. Consequently, the event $f(\boldsymbol{A}) \sim \alpha_0$ is unlikely.

6.1. **Degree-weighted solutions.** Let us now carry this strategy out in detail. A vector $x \in \ker \boldsymbol{A}$ is called δ*-balanced* if

$$\left|\sum_{v \notin \mathscr{F}(\boldsymbol{A})} d_{\boldsymbol{A}}(v)\left(\mathbf{1}\{x_v = 1\} - 1/2\right)\right| < \delta n.$$

The following observation is a simple consequence of Proposition 2.11.

Lemma 6.1. *W.h.p. the random matrix $\boldsymbol{A}$ has $2^{\Phi_d(\alpha_*)n+o(n)}$ many $o(1)$-balanced solutions.*

Proof. Since (1.2) and Proposition 2.3 show that $\operatorname{nul} \boldsymbol{A} \sim \Phi_d(\alpha_*)n$ w.h.p., it suffices to prove that a random $\boldsymbol{x} \in \ker \boldsymbol{A}$ is $o(1)$-balanced w.h.p. To see this, fix any integer $\ell > 0$. Proposition 2.11 implies together with Proposition 2.15 that the distribution of a random $\boldsymbol{x} \in \ker \boldsymbol{A}$ is $o(1)$-extremal w.h.p. Moreover, Fact 2.17 shows that the event $\{\boldsymbol{x}_v = 1\}$ has probability $1/2$ for all $v \notin \mathscr{F}(\boldsymbol{A})$. Therefore, the definition (2.12) of the cut metric implies that for any $\ell \in \mathbb{N}$, w.h.p. over the choice of $\boldsymbol{A}$ we have

$$\mathbb{E}\left[\left|\sum_{v \notin \mathscr{F}(\boldsymbol{A})} \mathbf{1}\{d_{\boldsymbol{A}}(v) = \ell\}\left(\mathbf{1}\{\boldsymbol{x}_v = 1\} - \frac{1}{2}\right)\right| \mid \boldsymbol{A}\right] = o(n). \tag{6.1}$$

As this is true for every fixed ℓ and the Poisson degree distribution of $G(\boldsymbol{A})$ has sub-exponential tails, the assertion follows from (6.1) by summing on ℓ. □

6.2. **Counting WP fixed points.** Proceeding to the next step of our strategy, we now estimate the expected number of approximate WP fixed points that leave about $\alpha_0 n$ variables unfrozen. We call such fixed points α_0-covers. The precise definition, in which we condition on the degree sequence $d_{\boldsymbol{A}}$ of $G(\boldsymbol{A})$, reads as follows.

Definition 6.2. *Given $d_{\boldsymbol{A}}$ let*

$$\mathfrak{V} = \bigcup_{i=1}^{n} \{v_i\} \times [d_{\boldsymbol{A}}(v_i)] \qquad \text{and} \qquad \mathfrak{C} = \bigcup_{i=1}^{n} \{a_i\} \times [d_{\boldsymbol{A}}(a_i)]$$

*be sets of variable/check clones. An α-*cover *is a pair $(\mathfrak{m}, \pi)$ consisting of a map $\mathfrak{m} : \mathfrak{V} \cup \mathfrak{C} \to \{\mathtt{f}, \mathtt{u}\}^2$, $(u, j) \mapsto (\mathfrak{m}_1(u, j), \mathfrak{m}_2(u, j))$ and a bijection $\pi : \mathfrak{V} \to \mathfrak{C}$ such that the following conditions are satisfied.*

COV1: *For all $i \in [n]$ and $j \in [d_{\boldsymbol{A}}(v_i)]$ we have $\big(\mathfrak{m}_1(\pi(v_i, j)), \mathfrak{m}_2(\pi(v_i, j))\big) = \big(\mathfrak{m}_2(v_i, j), \mathfrak{m}_1(v_i, j)\big)$.*

COV2: *For all but $o(n)$ pairs (i, j) with $i \in [n]$ and $j \in [d_{\boldsymbol{A}}(v_i)]$ we have*

$$\mathfrak{m}_2\big(v_i, j\big) = \begin{cases} \mathtt{f} & \text{if } \mathfrak{m}_1(v_i, h) = \mathtt{f} \text{ for some } h \in [d_{\boldsymbol{A}}(v_i)] \setminus \{j\}, \\ \mathtt{u} & \text{otherwise.} \end{cases}$$

COV3: *For all but $o(n)$ pairs (v_i, j) with $i \in [n]$ and $j \in [d_{\boldsymbol{A}}(a_i)]$ we have*

$$\mathfrak{m}_2\big(a_i, j\big) = \begin{cases} \mathtt{f} & \text{if } \mathfrak{m}_1(a_i, h) = \mathtt{f} \text{ for all } h \in [d_{\boldsymbol{A}}(a_i)] \setminus \{j\}, \\ \mathtt{u} & \text{otherwise.} \end{cases}$$

COV4: *For any $z \in \{\mathtt{f},\star,\mathtt{u}\}$ and $L = (\ell_{\mathtt{uu}},\ell_{\mathtt{uf}},\ell_{\mathtt{fu}},\ell_{\mathtt{ff}}) \in \mathbb{N}_0^4$ let*

$$\mathfrak{m}(v_i) = \begin{cases} \mathtt{f} & \text{if } \mathfrak{m}_1(v_i,j) = \mathtt{f} \text{ for at least two } j \in [d_{\boldsymbol{A}}(v_i)], \\ \star & \text{if } \mathfrak{m}_1(v_i,j) = \mathtt{f} \text{ for precisely one } j \in [d_{\boldsymbol{A}}(v_i)], \\ \mathtt{u} & \text{otherwise,} \end{cases} \tag{6.2}$$

$$\mathfrak{m}(a_i) = \begin{cases} \mathtt{f} & \text{if } \mathfrak{m}_1(a_i,j) = \mathtt{f} \text{ for all } j \in [d_{\boldsymbol{A}}(a_i)], \\ \star & \text{if } \mathfrak{m}_1(a_i,j) = \mathtt{f} \text{ for all but precisely one } j \in [d_{\boldsymbol{A}}(a_i)], \\ \mathtt{u} & \text{otherwise,} \end{cases} \tag{6.3}$$

$$\boldsymbol{\Delta}(z,L) = \sum_{i=1}^{n} \mathbf{1}\{\mathfrak{m}(v_i) = z\} \prod_{x,y\in\{\mathtt{u},\mathtt{f}\}} \mathbf{1}\left\{\left|\left\{j \in [d_{\boldsymbol{A}}(v_i)] : \mathfrak{m}_1(v_i,j) = x,\ \mathfrak{m}_2(v_i,j) = y\right\}\right| = \ell_{xy}\right\}, \tag{6.4}$$

$$\boldsymbol{\Gamma}(z,L) = \sum_{i=1}^{n} \mathbf{1}\{\mathfrak{m}(a_i) = z\} \prod_{x,y\in\{\mathtt{u},\mathtt{f}\}} \mathbf{1}\left\{\left|\left\{j \in [d_{\boldsymbol{A}}(a_i)] : \mathfrak{m}_1(a_i,j) = x,\ \mathfrak{m}_2(a_i,j) = y\right\}\right| = \ell_{xy}\right\}. \tag{6.5}$$

Then with $\mathfrak{d}(\cdot),\mathfrak{g}(\cdot)$ from (5.15)–(5.20) we have

$$\boldsymbol{\Delta}(z,L) = n\mathfrak{d}(1-\alpha_0,z,L) + o(n), \qquad \boldsymbol{\Gamma}(z,L) = n\mathfrak{g}(\alpha_0,z,L) + o(n). \tag{6.6}$$

Let $\mathfrak{Z}(\alpha)$ be the number of α-covers. The main result in this section is the proof of the following bound.

Proposition 6.3. *For any $d >$ e w.h.p. over the choice of the degree sequence $d_{\boldsymbol{A}}$ we have*

$$\frac{\mathfrak{Z}(\alpha_0)}{(dn)!\prod_{i=1}^{n} d_{\boldsymbol{A}}(v_i)!d_{\boldsymbol{A}}(a_i)!} = \exp(o(n)) \ .$$

The rest of this section is devoted to the proof of Proposition 6.3. The following lemma decomposes $\mathfrak{Z}(\alpha_0)$ into a few factors that we will subsequently calculate separately.

Lemma 6.4. *W.h.p. over the choice of $d_{\boldsymbol{A}}$ we have $\mathfrak{Z}(\alpha_0) = \exp(o(n))\mathfrak{H}^2\mathfrak{L}^2\mathfrak{E}$ where*

$$\mathfrak{H} = \binom{n}{n((\mathfrak{d}(1-\alpha_0,z,L))_{z\in\{\mathtt{f},\star,\mathtt{u}\},L\in\mathbb{N}_0^4})}, \qquad \mathfrak{L} = \prod_{\substack{z\in\{\mathtt{f},\star,\mathtt{u}\}\\ L=(\ell_{\mathtt{uu}},\ell_{\mathtt{uf}},\ell_{\mathtt{fu}},\ell_{\mathtt{ff}})\in\mathbb{N}_0^4}} \binom{\ell_{\mathtt{uu}}+\cdots+\ell_{\mathtt{ff}}}{\ell_{\mathtt{uu}},\ldots,\ell_{\mathtt{ff}}}^{n\mathfrak{d}(1-\alpha_0,z,L)}$$

$$\mathfrak{E} = \left(dn\alpha_0^2\right)!\left((dn\alpha_0(1-\alpha_0))!\right)^2\left(dn(1-\alpha_0)^2\right)!.$$

Proof. The first factor $\mathfrak{H}$ simply accounts for the number of ways of partitioning the n variable nodes and the n check nodes into the various types as designated by (6.4)–(6.5). Since we need to select a type for each variable and check node, the number of possible designations actually reads

$$\binom{n}{n((\mathfrak{d}(1-\alpha_0,z,L))_{z\in\{\mathtt{f},\star,\mathtt{u}\},L\in\mathbb{N}_0^4}}\binom{n}{n((\mathfrak{g}(\alpha_0,z,L))_{z\in\{\mathtt{f},\star,\mathtt{u}\},L\in\mathbb{N}_0^4}}\exp(o(n)); \tag{6.7}$$

the $\exp(o(n))$ error term accounts for the $o(n)$ error terms in (6.6). But a glimpse at (5.15)–(5.20) reveals that these two multinomial coefficients coincide. Hence, (6.7) is equal to $\mathfrak{H}^2\exp(o(n))$. Furthermore, the factor $\mathfrak{L}$ accounts for the number of ways of selecting, for each variable/check node, the clones along which messages of the four types $\{\mathtt{f},\mathtt{u}\}^2$ travel. Finally, $\mathfrak{E}$ counts the number of ways of matching up these clones so that **COV2–COV3** are satisfied. To be precise, since **COV2–COV3** only provide asymptotic estimates rather than precise equalities, we incur an $\exp(o(n))$ error term; hence $\mathfrak{Z}(\alpha_0) = \exp(o(n))\mathfrak{H}^2\mathfrak{L}^2\mathfrak{E}$. □

Lemma 6.5. *We have $\frac{1}{n}\log\mathfrak{L} = \mathfrak{l}' + \mathfrak{l}'' + o(1)$, where*

$$\mathfrak{l}' = \exp(-d)\sum_{\ell=0}^{\infty}\frac{d^\ell}{\ell!}\log(\ell!), \qquad \mathfrak{l}'' = -\sum_{\substack{z\in\{\mathtt{f},\star,\mathtt{u}\}\\ L=(\ell_{\mathtt{uu}},\ell_{\mathtt{uf}},\ell_{\mathtt{fu}},\ell_{\mathtt{ff}})\in\mathbb{N}_0^4}} \mathfrak{d}(1-\alpha_0,z,L)\log(\ell_{\mathtt{uu}}!\ell_{\mathtt{uf}}!\ell_{\mathtt{fu}}!\ell_{\mathtt{ff}}!).$$

Proof. Choose $\boldsymbol{z} \in \{\mathtt{f},\star,\mathtt{u}\}$ along with non-negative vector $\boldsymbol{L} \in \mathbb{N}_0^4$ from the distribution

$$\mathbb{P}[\boldsymbol{z} = z, \boldsymbol{L} = L] = \mathfrak{d}(1-\alpha_0,z,L) \qquad (z \in \{\mathtt{f},\star,\mathtt{u}\},\ L \in \mathbb{N}_0^4).$$

Then due to **COV4** we have

$$\frac{1}{n}\log\mathfrak{L} = \mathbb{E}\left[\log(\boldsymbol{\ell}_{\mathtt{uu}}+\cdots+\boldsymbol{\ell}_{\mathtt{ff}})!\right] - \mathbb{E}\left[\log(\boldsymbol{\ell}_{\mathtt{uu}}!\cdots\boldsymbol{\ell}_{\mathtt{ff}}!)\right] + o(1) = \mathbb{E}\left[\log(\boldsymbol{\ell}_{\mathtt{uu}}+\cdots+\boldsymbol{\ell}_{\mathtt{ff}})!\right] - \mathfrak{l}'' + o(1). \tag{6.8}$$

Moreover, (5.15)–(5.17) show that $\boldsymbol{\ell}_{\mathtt{uu}}+\cdots+\boldsymbol{\ell}_{\mathtt{ff}}$ has distribution $\mathrm{Po}(d)$. Therefore, $\mathbb{E}\left[\log(\boldsymbol{\ell}_{\mathtt{uu}}+\cdots+\boldsymbol{\ell}_{\mathtt{ff}})!\right] = \mathfrak{l}'$. Hence, the assertion follows from (6.8). □

Lemma 6.6. *We have* $\frac{1}{n}\log\mathfrak{H} = d\Big(1-\log(d)-\alpha_0\log\alpha_0-(1-\alpha_0)\log(1-\alpha_0)\Big)-\mathfrak{l}''$.

Proof. This is a straightforward computation. For the sake of brevity we introduce $q(\lambda,i)=\mathbb{P}[\mathrm{Po}(\lambda)=i]$. Using Stirling's formula, we approximate $\mathfrak{H}$ in terms of entropy as

$$\frac{1}{n}\log\mathfrak{H} = H((\mathfrak{d}(1-\alpha_0,z,L))_{z\in\{\mathtt{f},\star,\mathtt{u}\},L\in\mathbb{N}_0^4}) + o(1). \tag{6.9}$$

Depending on the choice of $z\in\{\mathtt{f},\star,\mathtt{u}\}$, the definitions (5.15)–(5.17) of the $\mathfrak{d}(1-\alpha_0,z,L)$ constrain some of the values $\ell_{\mathtt{uu}},\ldots,\ell_{\mathtt{ff}}$ to be zero. Hence, using the identity (2.1), we can spell the right hand side of (6.9) out as

$$\begin{aligned}
H((\mathfrak{d}(1-\alpha_0,z,L))_{z\in\{\mathtt{f},\star,\mathtt{u}\},L\in\mathbb{N}_0^4}) &= -\sum_{z,L}\mathfrak{d}(1-\alpha_0,z,L)\log\mathfrak{d}(1-\alpha_0,z,L)\\
&= -\sum_{\ell_{\mathtt{uu}}\geq 0} q(d(1-\alpha_0),0)q(d\alpha_0,\ell_{\mathtt{uu}})\log(q(d(1-\alpha_0),0)q(d\alpha_0,\ell_{\mathtt{uu}}))\\
&\quad -\sum_{\ell_{\mathtt{uf}}\geq 0} q(d(1-\alpha_0),1)q(d\alpha_0,\ell_{\mathtt{uf}})\log(q(d(1-\alpha_0),1)q(d\alpha_0,\ell_{\mathtt{uf}}))\\
&\quad -\sum_{\ell_{\mathtt{uf}}\geq 0,\ell_{\mathtt{ff}}\geq 2} q(d(1-\alpha_0),\ell_{\mathtt{ff}})q(d\alpha_0,\ell_{\mathtt{uf}})\log(q(d(1-\alpha_0),\ell_{\mathtt{ff}})q(d\alpha_0,\ell_{\mathtt{uf}}))\\
&= d(1-\alpha_0)^2-(1-\alpha_0)\sum_{\ell_{\mathtt{uu}}\geq 0} q(d\alpha_0,\ell_{\mathtt{uu}})\left[\ell_{\mathtt{uu}}\log(d\alpha_0)-d\alpha_0\right]\\
&\quad -d(1-\alpha_0)^2\log(d(1-\alpha_0)^2)-d(1-\alpha_0)^2\sum_{\ell_{\mathtt{uf}}\geq 0} q(d\alpha_0,\ell_{\mathtt{uf}})\left[\ell_{\mathtt{uf}}\log(d\alpha_0)-d\alpha_0\right]\\
&\quad -\left(\alpha_0-d(1-\alpha_0)^2\right)\sum_{\ell_{\mathtt{uf}}\geq 0} q(d\alpha_0,\ell_{\mathtt{uf}})\left[\ell_{\mathtt{uf}}\log(d\alpha_0)-d\alpha_0\right]\\
&\quad -\sum_{\ell_{\mathtt{ff}}\geq 2} q(d(1-\alpha_0),\ell_{\mathtt{ff}})\left[\ell_{\mathtt{ff}}\log(d(1-\alpha_0))-d(1-\alpha_0)\right]-\mathfrak{l}''\\
&= -\mathfrak{l}''+d(1-\alpha_0)^2+d\alpha_0(1-\alpha_0)-d\alpha_0(1-\alpha_0)\log(d\alpha_0)\\
&\quad -d(1-\alpha_0)^2\log(d(1-\alpha_0)^2)+d^2\alpha_0(1-\alpha_0)^2-d^2\alpha_0(1-\alpha_0)^2\log(d\alpha_0)\\
&\quad +d(1-\alpha_0)-d(1-\alpha_0)\log(d(1-\alpha_0))+(1-\alpha_0)\log(1-\alpha_0)+d(1-\alpha_0)^2\log(d(1-\alpha_0)^2)\\
&\quad +d\alpha_0(\alpha_0-d(1-\alpha_0)^2)-d\alpha_0(\alpha_0-d(1-\alpha_0)^2)\log(d\alpha_0)\\
&= -\mathfrak{l}''-d\log d-d\alpha_0\log\alpha_0-d(1-\alpha_0)\log(1-\alpha_0)+d+(1-\alpha_0)\log(1-\alpha_0)+d(1-\alpha_0)^2.
\end{aligned} \tag{6.10}$$

Since $1-\alpha_0=\exp(-d(1-\alpha_0))$, the assertion is immediate from (6.10). □

Lemma 6.7. *W.h.p. over the choice of* $d_{\boldsymbol{A}}$ *we have* $\frac{1}{n}\log\frac{\mathfrak{E}}{(dn)!} = 2d\alpha_0\log\alpha_0+2d(1-\alpha_0)\log(1-\alpha_0)$.

Proof. This follows immediately from Stirling's formula. □

Proof of Proposition 6.3. The proposition is an immediate consequence of Lemmas 6.4–6.7. □

6.3. **Extending covers.** While in the previous section we just estimated the number of covers, here we also count actual solutions to the random linear system encoded by a cover. The following definition captures assignments σ that, up to $o(n)$ errors, comply with the frozen/unfrozen designations of a cover $(\mathfrak{m},\pi)$ and also satisfy the checks, again up to $o(n)$ errors. We extend $\sigma:\{v_1,\ldots,v_n\}\to\mathbb{F}_2$ to the set $\mathfrak{V}$ of clones by letting $\sigma(v_i,j)=\sigma(v_i)$.

Definition 6.8. *An α-extension consists of an α-cover $(\mathfrak{m},\pi)$ together with an assignment $\sigma:\{v_1,\ldots,v_n\}\to\mathbb{F}_2$ such that the following conditions are satisfied.*

EXT1: *We have* $\sum_{i=1}^n(1+d_{\boldsymbol{A}}(v_i))\mathbf{1}\{\sigma(v_i)=1,\ \mathfrak{m}(v_i)\neq\mathtt{u}\}=o(n)$.
EXT2: *We have* $\sum_{i=1}^n d_{\boldsymbol{A}}(v_i)\mathbf{1}\{\sigma(v_i)=1,\ \mathfrak{m}(v_i)=\mathtt{u}\}=o(n)+\frac{1}{2}\sum_{i=1}^n d_{\boldsymbol{A}}(v_i)\mathbf{1}\{\mathfrak{m}(v_i)=\mathtt{u}\}$.
EXT3: *We have* $\sum_{i=1}^n\mathbf{1}\left\{\sum_{j\in[d_{\boldsymbol{A}}(a_i)]}\sigma(\pi(a_i,j))\neq 0\right\}=o(n)$.

The first condition **EXT1** posits that, when weighted according to their degrees, all but $o(n)$ variables that are deemed frozen under $\mathfrak{m}$ are set to zero under σ. **EXT2** provides that about half the variables that ought to be unfrozen according to $\mathfrak{m}$ are set to one, if we weight variables by their degrees. Finally, **EXT3** ensures that all but $o(n)$ checks are satisfied.

Let $\mathfrak{X}(\alpha)$ be the total number of α-extensions. The main result of this section reads as follows.

Proposition 6.9. *Let $d >$ e. W.h.p. over the choice of the degree sequence $d_{\boldsymbol{A}}$ we have*

$$\frac{\mathfrak{X}(\alpha_0)}{(dn)!\prod_{i=1}^n d_{\boldsymbol{A}}(v_i)!d_{\boldsymbol{A}}(a_i)!} = \exp(n\Phi_d(\alpha_0)+o(n)).$$

The following lemma summarises the key step toward the proof of Proposition 6.9. For a fixed $\mathfrak{m}$ let $\boldsymbol{\pi}$ be a random matching of the clones $\mathfrak{V},\mathfrak{C}$ such that $(\mathfrak{m},\boldsymbol{\pi})$ is an α_0-cover.

Lemma 6.10. *For a $o(1)$-balanced σ let $\mathfrak{p}(\mathfrak{m},\sigma)$ be the probability that σ satisfies all but $o(n)$ checks. Then w.h.p. over the choice of $d_{\boldsymbol{A}}$ we have*

$$\mathfrak{p}(\mathfrak{m},\sigma) \le 2^{-|\{i\in[n]:\mathfrak{m}(a_i)=\mathtt{u}\}|+o(n)}.$$

Proof. Given $\mathfrak{m}$ the precise matching $\boldsymbol{\pi}$ of the frozen/unfrozen clones remains random subject to conditions **COV1–COV3**. We will expose this matching in two steps. First we expose the degree-weighted fraction of occurrences of frozen/unfrozen variables set to one. Specifically, let $\boldsymbol{r}_{\mathtt{u}} \sim 1/2$ be the precise degree-weighted fraction of occurrences of unfrozen variables that are set to zero under σ; in formulae,

$$\boldsymbol{r}_{\mathtt{u}} = \frac{\sum_{i=1}^n \left|\left\{j\in[d_{\boldsymbol{A}}(a_i)] : \mathfrak{m}_1(a_i,j)=\mathtt{u}, \sigma(\pi(a_i,j))=0\right\}\right|}{\sum_{i=1}^n \left|\left\{j\in[d_{\boldsymbol{A}}(a_i)] : \mathfrak{m}_1(a_i,j)=\mathtt{u}\right\}\right|}. \tag{6.11}$$

Similarly, let $\boldsymbol{r}_{\mathtt{f}} \sim 1$ be the degree-weighted fraction of frozen clones set to zero:

$$\boldsymbol{r}_{\mathtt{f}} = \frac{\sum_{i=1}^n \left|\left\{j\in[d_{\boldsymbol{A}}(a_i)] : \mathfrak{m}_1(a_i,j)=\mathtt{f}, \sigma(\pi(a_i,j))=0\right\}\right|}{\sum_{i=1}^n \left|\left\{j\in[d_{\boldsymbol{A}}(a_i)] : \mathfrak{m}_1(a_i,j)=\mathtt{f}\right\}\right|}. \tag{6.12}$$

Once we condition on $\boldsymbol{r}_{\mathtt{u}},\boldsymbol{r}_{\mathtt{f}}$, the precise matching of the various clones remains random. To study the conditional probability that σ satisfies all but $o(n)$ checks, we set up an auxiliary probability space. To be precise, let $\boldsymbol{\chi} = \left(\boldsymbol{\chi}_{ij}\right)_{i\in[n],j\in[d_A(a_i)]}$ be a random sequence of mutually independent field elements $\boldsymbol{\chi}_{ij}\in\mathbb{F}_2$ such that

$$\mathbb{P}\left[\boldsymbol{\chi}_{ij}=0\right] = \begin{cases} \boldsymbol{r}_{\mathtt{u}} & \text{if } \mathfrak{m}_1(a_i,j)=\mathtt{u},\\ \boldsymbol{r}_{\mathtt{f}} & \text{if } \mathfrak{m}_1(a_i,j)=\mathtt{f}. \end{cases} \tag{6.13}$$

Further, consider the events

$$\mathscr{R} = \left\{\sum_{i=1}^n\sum_{j=1}^{d_{\boldsymbol{A}}(a_i)} \mathbf{1}\left\{\boldsymbol{\chi}_{ij}=0, \mathfrak{m}_1(a_i,j)=z\right\} = \boldsymbol{r}_z\sum_{i=1}^n\sum_{j=1}^{d_{\boldsymbol{A}}(a_i)}\mathbf{1}\left\{\mathfrak{m}_1(a_i,j)=z\right\} \text{ for } z\in\{\mathtt{f},\mathtt{u}\}\right\},$$
$$\mathscr{S} = \left\{\sum_{i=1}^n \mathbf{1}\left\{\sum_{j=1}^{d_{\boldsymbol{A}}(a_i)}\boldsymbol{\chi}_{ij}\neq 0\right\} = o(n)\right\}.$$

Then because the matching $\boldsymbol{\pi}$ of the clones is random subject to **COV1–COV3** we obtain

$$\mathfrak{p}(\mathfrak{m},\sigma) = \mathbb{E}[\mathbb{P}[\mathscr{S}\mid\mathscr{R},\boldsymbol{r}_{\mathtt{f}},\boldsymbol{r}_{\mathtt{u}}]]. \tag{6.14}$$

Hence, we are left to calculate $\mathbb{P}[\mathscr{S}\mid\mathscr{R},\boldsymbol{r}_{\mathtt{f}},\boldsymbol{r}_{\mathtt{u}}]$. Calculating the unconditional probabilities is easy. Indeed, the choice (6.11)–(6.12) of $\boldsymbol{r}_{\mathtt{u}},\boldsymbol{r}_{\mathtt{f}}$ and the definition (6.13) of $\boldsymbol{\chi}$ and the local limit theorem for the binomial distribution ensure that

$$\mathbb{P}[\mathscr{R}] = \Omega(1/n). \tag{6.15}$$

Furthermore, we claim that

$$\mathbb{P}[\mathscr{S}] = 2^{-|\{i\in[n]:\mathfrak{m}(a_i)=\mathtt{u}\}|+o(n)}. \tag{6.16}$$

Indeed, consider a check a_i such that $\mathfrak{m}(a_i)=\mathtt{u}$. Then there exists $j\in[d_{\boldsymbol{A}}(a_i)]$ such that $\mathfrak{m}_1(a_i,j)=\mathtt{u}$. Therefore, the choice (6.11) of $\boldsymbol{r}_{\mathtt{u}}$ ensures that the event $\boldsymbol{\chi}_{ij}\neq 0$ occurs with probability $1/2+o(1)$. Similarly, if $\mathfrak{m}(a_i)\neq\mathtt{u}$, then by the choice of $\boldsymbol{r}_{\mathtt{f}}$ the event $\boldsymbol{\chi}_{ij}\neq 0$ has probability at most $o(d_{\boldsymbol{A}}(a_i))$. Since the definition (6.13) of the

$\boldsymbol{\chi}_{ij}$ ensures that these events are independent for the different checks a_i, we obtain (6.16). Finally, combining (6.14)–(6.16) with Bayes' rule, we obtain

$$\mathfrak{p}(\mathfrak{m},\sigma) = \mathbb{E}\Big[\mathbb{P}\left[\mathscr{S} \mid \mathscr{R}, \boldsymbol{r}_{\mathtt{f}}, \boldsymbol{r}_{\mathtt{u}}\right]\Big] = \mathbb{E}\Big[\mathbb{P}\left[\mathscr{S} \mid \boldsymbol{r}_{\mathtt{f}}, \boldsymbol{r}_{\mathtt{u}}\right] \cdot \mathbb{P}\left[\mathscr{R} \mid \mathscr{S}, \boldsymbol{r}_{\mathtt{f}}, \boldsymbol{r}_{\mathtt{u}}\right] / \mathbb{P}\left[\mathscr{R} \mid \boldsymbol{r}_{\mathtt{f}}, \boldsymbol{r}_{\mathtt{u}}\right]\Big] \le 2^{-|\{i\in[n]:\mathfrak{m}(a_i)=\mathtt{u}\}|+o(n)},$$

as desired. □

To complete the proof of Proposition 6.9 we combine Lemma 6.10 with the following statement about the numbers of variables/checks of the various types. Given $z \in \{\mathtt{f},\mathtt{u}\}$, let us define $\epsilon_z := \mathbf{1}\{z = \mathtt{u}\}$.

Lemma 6.11. *Let $(\mathfrak{m},\pi)$ be an α_0-cover. Then w.h.p. over the choice of $d_{\boldsymbol{A}}$,*

$$\frac{1}{dn}\sum_{i=1}^{n}\sum_{j=1}^{d_{\boldsymbol{A}}(v_i)} \mathbf{1}\left\{\mathfrak{m}(v_i,j) = (x,y)\right\} \sim \alpha_0^{1+\epsilon_x-\epsilon_y}(1-\alpha_0)^{1-\epsilon_x+\epsilon_y} \qquad (x,y\in\{\mathtt{f},\mathtt{u}\}), \tag{6.17}$$

$$\frac{1}{dn}\sum_{i=1}^{n}\sum_{j=1}^{d_{\boldsymbol{A}}(a_i)} \mathbf{1}\left\{\mathfrak{m}(a_i,j) = (x,y)\right\} \sim \alpha_0^{1-\epsilon_x+\epsilon_y}(1-\alpha_0)^{1+\epsilon_x-\epsilon_y} \qquad (x,y\in\{\mathtt{f},\mathtt{u}\}), \tag{6.18}$$

$$\frac{1}{n}\sum_{i=1}^{n}\mathbf{1}\left\{\mathfrak{m}(v_i)=\mathtt{f}\right\} \sim \alpha_0 - d(1-\alpha_0)^2, \quad \frac{1}{n}\sum_{i=1}^{n}\mathbf{1}\left\{\mathfrak{m}(v_i)=\mathtt{u}\right\} \sim 1-\alpha_0, \quad \frac{1}{n}\sum_{i=1}^{n}\mathbf{1}\left\{\mathfrak{m}(v_i)=\star\right\} \sim d(1-\alpha_0)^2, \tag{6.19}$$

$$\frac{1}{n}\sum_{i=1}^{n}\mathbf{1}\left\{\mathfrak{m}(a_i)=\mathtt{u}\right\} \sim \alpha_0 - d(1-\alpha_0)^2, \quad \frac{1}{n}\sum_{i=1}^{n}\mathbf{1}\left\{\mathfrak{m}(a_i)=\mathtt{f}\right\} \sim 1-\alpha_0, \quad \frac{1}{n}\sum_{i=1}^{n}\mathbf{1}\left\{\mathfrak{m}(a_i)=\star\right\} \sim d(1-\alpha_0)^2. \tag{6.20}$$

Proof. We observe that **COV4** implies the estimate

$$\frac{1}{n}\sum_{i=1}^{n}\sum_{j=1}^{d_{\boldsymbol{A}}(v_i)} \mathbf{1}\left\{\mathfrak{m}(v_i,j) = (x,y)\right\} \sim d\alpha_0^{\epsilon_x}(1-\alpha_0)^{1-\epsilon_x}\exp(-d\epsilon_y(1-\alpha_0))(1-\exp(-d(1-\alpha_0)))^{1-\epsilon_y}.$$

Using the identity (2.1), we obtain (6.17). The second identity (6.18) follows from (6.17) and **COV1**. Equations (6.19)–(6.20) follow from the identity $\alpha_0 = 1-\exp(-d(1-\alpha_0))$ and **COV2** by summing on L. □

Proof of Proposition 6.9. Lemmas 6.10 and 6.11 imply that w.h.p. over the choice of $d_{\boldsymbol{A}}$,

$$p(\mathfrak{m},\sigma) \le 2^{|\{i\in[n]:\mathfrak{m}(v_i)=\mathtt{u}\}|-|\{i\in[n]:\mathfrak{m}(a_i)=\mathtt{u}\}|+o(n)} \le 2^{n(1-2\alpha_0+d(1-\alpha_0)^2+o(1))}. \tag{6.21}$$

Further, using the identity (2.1), we verify that $1-2\alpha_0+d(1-\alpha_0)^2 = \Phi_d(\alpha_0)$. Thus, the assertion follows from (6.21) and Proposition 6.3. □

Proof of Proposition 2.8. We can generate a random Tanner graph $G(\boldsymbol{A})$ with a given degree sequence $d_{\boldsymbol{A}}$ by way of the pairing model. Specifically, we generate a random pairing $\boldsymbol{\pi}$ of the sets $\mathfrak{V},\mathfrak{C}$ of clones and condition on the event $\mathfrak{S}$ that the resulting graph $G(\boldsymbol{\pi})$ is simple. W.h.p. over the choice of the degree sequence $d_{\boldsymbol{A}}$ we have $\mathbb{P}[\mathfrak{S} \mid d_{\boldsymbol{A}}] = \Omega(1)$; but in fact, for the purposes of the present proof the trivial estimate

$$\mathbb{P}[\mathfrak{S} \mid d_{\boldsymbol{A}}] = \exp(o(n)) \qquad \text{w.h.p.} \tag{6.22}$$

suffices. Now, let $\mathscr{E}$ be the event that $G(\boldsymbol{\pi})$ has at least $2^{\Phi_d(\alpha^*)n+o(n)}$ many α_0-extensions. Recall that w.h.p. over the choice of $d_{\boldsymbol{A}}$ there are $\left(\sum_{i=1}^n d_{\boldsymbol{A}}(v_i)\right)! = (dn)!\exp(o(n))$ possible matchings of the $2\left(\sum_{i=1}^n d_{\boldsymbol{A}}(v_i)\right)$ clones in total, and that each Tanner graph extends to $\prod_{i=1}^n d_{\boldsymbol{A}}(v_i)!d_{\boldsymbol{A}}(a_i)!$ pairings. Therefore, Propositions 2.3 and 6.9, (6.22) and Markov's inequality show that w.h.p. over the choice of $d_{\boldsymbol{A}}$,

$$\mathbb{P}\Big[\mathscr{E} \mid \mathfrak{S}, d_{\boldsymbol{A}}\Big] \le 2^{-\Phi_d(\alpha^*)n+o(n)}\frac{\mathfrak{X}(\alpha_0)}{(dn)!\prod_{i=1}^n d_{\boldsymbol{A}}(v_i)!d_{\boldsymbol{A}}(a_i)!} \le 2^{n(\Phi_d(\alpha_0)-\Phi_d(\alpha^*))+o(n)} = \exp(-\Omega(n)) \qquad \text{w.h.p.} \tag{6.23}$$

To complete the proof, assume that $\mathbb{P}\left[f(\boldsymbol{A}) = \alpha_0 + o(1)\right] > \varepsilon$ for some $\varepsilon > 0$. Then (1.2), Lemma 5.4, Corollary 5.6 and Lemma 6.1 show that $\mathbb{P}\left[\boldsymbol{A}\in\mathscr{E} \mid f(\boldsymbol{A}) = \alpha_0 + o(1)\right] = 1-o(1)$. Hence, $\mathbb{P}\left[\boldsymbol{A}\in\mathscr{E} \mid d_{\boldsymbol{A}}\right] > \varepsilon/2$ with probability at least $\varepsilon/2$, in contradiction to (6.23). □

7. Symmetry and correlation

The aim in this section is to prove Proposition 2.9, which states that w.h.p. the numbers of variables and checks in the slush are not almost equal. Thus, we study the subgraph $G_{\mathtt{s}}(\boldsymbol{A})$ induced on $V_{\mathtt{s}}(\boldsymbol{A}) \cup C_{\mathtt{s}}(\boldsymbol{A})$. We use the notation $n_{\mathtt{s}} := |V_{\mathtt{s}}(\boldsymbol{A})|$ and $m_{\mathtt{s}} := |C_{\mathtt{s}}(\boldsymbol{A})|$. We exploit the symmetry of the distribution of $\boldsymbol{A}$ by considering the transpose of the matrix. While symmetry automatically implies that events are equally likely for $\boldsymbol{A}$ and $\boldsymbol{A}^\top$, we would like to be able to deduce that the event $|V_{\mathtt{s}}(\boldsymbol{A})| - |C_{\mathtt{s}}(\boldsymbol{A})| \geq \omega$ occurs with probability asymptotically $1/2$ for some $\omega = \omega(n) \gg 1$. The main step is to prove the following.

Lemma 7.1. *There exists some $\omega_0 \xrightarrow{n\to\infty} \infty$ such that w.h.p. $|n_{\mathtt{s}} - m_{\mathtt{s}}| \geq \omega_0$.*

As indicated above, Proposition 2.9 follows from this Lemma and symmetry considerations. We first describe the symmetry property more explicitly.

Lemma 7.2. *For any matrix A we have $V_{\mathtt{s}}\left(A^\top\right) = C_{\mathtt{s}}(A)$ and $C_{\mathtt{s}}\left(A^\top\right) = V_{\mathtt{s}}(A)$.*

Proof. We can show by induction on $t \in \mathbb{N}$ that the messages at time t in the Tanner graphs of $A, A^\top$ are symmetric. More precisely, the Tanner graphs are identical except that variable nodes become check nodes and vice versa. At time 0 all messages are $\mathtt{s}$ in both graphs, while it can be easily checked that the update rules remain identical if we switch checks and variables and also switch the symbols $\mathtt{f}$ and $\mathtt{u}$. Therefore, introducing

$$V_{\mathtt{s}}(A,t) = \left\{v \in V(A) : \left(\forall a \in \partial v : w_{a\to v}(A,t) \neq \mathtt{f}\right) \text{ and } |\{a \in \partial v : w_{a\to v}(A,t) = \mathtt{s}\}| \geq 2\right\},$$
$$C_{\mathtt{s}}(A,t) = \left\{a \in C(A) : \left(\forall v \in \partial a : w_{v\to a}(A,t) \neq \mathtt{u}\right) \text{ and } |\{v \in \partial a : w_{v\to a}(A,t) = \mathtt{s}\}| \geq 2\right\}.$$

we conclude that $V_{\mathtt{s}}(A,t) = C_{\mathtt{s}}(A^\top, t)$ and $C_{\mathtt{s}}(A,t) = V_{\mathtt{s}}(A^\top, t)$ for all t. Recalling (2.5)–(2.6), we see that $V_{\mathtt{s}}(A) = \bigcap_{t\geq 0} V_{\mathtt{s}}(A,t)$ and $C_{\mathtt{s}}(A) = \bigcap_{t\geq 0} C_{\mathtt{s}}(A,t)$, whence the assertion follows. □

Proof of Proposition 2.9. We apply Lemma 7.2 to deduce that

$$\mathbb{P}\left[|V_{\mathtt{s}}(\boldsymbol{A})| - |C_{\mathtt{s}}(\boldsymbol{A})| \geq \omega_0\right] = \mathbb{P}\left[\left|C_{\mathtt{s}}\left(\boldsymbol{A}^\top\right)\right| - \left|V_{\mathtt{s}}\left(\boldsymbol{A}^\top\right)\right| \geq \omega_0\right] = \mathbb{P}\left[|C_{\mathtt{s}}(\boldsymbol{A})| - |V_{\mathtt{s}}(\boldsymbol{A})| \geq \omega_0\right],$$

where for the second equality we used the fact that $\boldsymbol{A}, \boldsymbol{A}^\top$ have identical distributions. Furthermore Lemma 7.1 implies that $\mathbb{P}\left[|V_{\mathtt{s}}(\boldsymbol{A})| - |C_{\mathtt{s}}(\boldsymbol{A})| \geq \omega_0\right] + \mathbb{P}\left[|C_{\mathtt{s}}(\boldsymbol{A})| - |V_{\mathtt{s}}(\boldsymbol{A})| \geq \omega_0\right] = 1 - o(1)$, and the desired statement follows. □

The proof strategy for Lemma 7.1 is similar to (but rather simpler than) the standard approach to proving a local limit theorem: we will show that $n_{\mathtt{s}} - m_{\mathtt{s}}$ is almost equally likely to hit any value in a range much larger than ω_0, and therefore the probability of hitting the much smaller interval $[-\omega_0, \omega_0]$ is negligible. We begin by estimating the sizes of some special sets of vertices. Recall λ from (2.8).

Definition 7.3. *(i) Let $R = R(\boldsymbol{A})$ be the set of check nodes a of degree two such that $w_{v\to a}(\boldsymbol{A}) = \mathtt{s}$ for all $v \in \partial a$.*
(ii) Let $S = S(\boldsymbol{A})$ be the set of isolated variable nodes.
(iii) Let $T = T(\boldsymbol{A})$ be the set of check nodes a of degree three such that $w_{v\to a}(\boldsymbol{A}) = \mathtt{s}$ for all $v \in \partial a$.
(iv) Let $U = U(\boldsymbol{A})$ be the set of variable nodes which have precisely two neighbours, both in T.
(v) Let

$$r = r(\boldsymbol{A}) := |R|/n, \qquad s = s(\boldsymbol{A}) := |S|/n, \qquad u = u(\boldsymbol{A}) := |U|/n,$$
$$\bar{r} := \frac{\exp(-d)\lambda^2}{2}, \qquad \bar{s} := \exp(-d), \qquad \bar{u} := \left(\frac{\exp(-d)\lambda^2}{2}\right)\cdot\left(\frac{\exp(-d\alpha^*)\lambda^2/2}{1-\exp(-\lambda)}\right)^2.$$

Lemma 7.4. *W.h.p.*

$$r = (1+o(1))\bar{r}, \qquad s = (1+o(1))\bar{s}, \qquad u = (1+o(1))\bar{u}.$$

In particular, there exists some $\omega_1 \to \infty$ such that

$$r = \left(1+o\left(\frac{1}{\omega_1}\right)\right)\bar{r}, \qquad s = \left(1+o\left(\frac{1}{\omega_1}\right)\right)\bar{s}, \qquad u = \left(1+o\left(\frac{1}{\omega_1}\right)\right)\bar{u}.$$

Proof. Since whether a node lies in each of these sets is a fact about its depth (at most) 2 neighbourhood (with messages), by Lemma 4.2, it is enough to look at the probabilities that $\mathscr{T}_2$ (for S, U) and $\hat{\mathscr{T}}_2$ (for R) have the appropriate structure. (Indeed, the statement for S could be proved directly using a Chernoff bound and without appealing to Lemma 4.2.) An elementary check verifies that these probabilities are $\bar{r}, \bar{s}, \bar{u}$, as appropriate. □

Let $1 \ll \omega_1 \ll n^{1/2}$ be a function such that Lemma 7.4 holds. For the remainder of this section, we will fix further functions ω_0, ω_2 such that

$$1 \ll \omega_0 \ll \omega_1 \ll n^{1/2} \tag{7.1}$$

and such that ω_2 is chosen uniformly at random from the interval $[\omega_1/2, \omega_1]$ independently of $\boldsymbol{A}$. In particular, we will prove Lemma 7.1 with this ω_0.

Claim 7.5. *If $|U| = \Theta(n)$, then for all but $o\left(\binom{|U|}{\omega_1}\right)$ subsets $U' \subseteq U$ of size ω_1, no node has more than one neighbour in U'.*

Proof. It is a simple exercise to check that if a subset $U' \subseteq U$ of size ω_1 is chosen uniformly at random, then the expected number of nodes of T for which two of their three neighbours are chosen to be in U' is $O\left(|T|\omega_1^2/n^2\right) = o(1)$. Therefore by Markov's inequality, w.h.p. this does not occur for any check node. □

We will use the following notation for the remainder of the section. Given a Tanner graph G and a set of variable nodes W, let $G\langle W\rangle$ denote the graph obtained from G by deleting the set of edges incident to W. Note that this amounts to replacing the columns of the matrix corresponding to nodes of W with 0 columns.

Claim 7.6. *Let G be any Tanner graph and $U' \subseteq U(G)$ be any subset whose nodes lie at distance greater than 2. Let $U'' \subseteq U'$ be any subset of U'. Then $V_{\mathtt{s}}\left(G\left\langle U''\right\rangle\right) = V_{\mathtt{s}}(G) \setminus U''$.*

In other words, removing U'' from G does not have any knock-on effects on the slush.

Proof. Let $G' := G\left\langle U''\right\rangle$, and let us run WP on both G' and G simultaneously, initialising with all messages being $\mathtt{s}$. We verify by induction on t that the messages on the common edge set (those in G') are identical in both processes, since a discrepancy can only enter at edges incident to a deleted edge (i.e. in $G \setminus G'$), but our choice of $U'' \subseteq U$ is such that the messages emanating from the vertices of T incident to U'' remain $\mathtt{s}$. □

For any r, s, u, let $\mathscr{G}_{r,s,u}$ denote the class of graphs with the appropriate parameters, i.e. with $r(G) = r$, with $s(G) = s$ and with $u(G) = u$, and let

$$\mathscr{G}'_{r,s,u} = \mathscr{G}'_{r,s,u;\omega_2} := \mathscr{G}_{r',s',u'}, \qquad \text{where } r' := r + \frac{2\omega_2}{n}, \qquad s' := s + \frac{\omega_2}{n}, \qquad u' := u - \frac{\omega_2}{n}.$$

The intuition behind this definition is that if we delete a set $U'' \subseteq U'$ of size ω_2 to obtain G', then by Claim 7.5 no remaining messages are changed, and therefore

- $|R(G')| = |R(G)| + 2\omega_2$ (for each vertex of U'', its two neighbours are moved into R);
- $|S(G')| = |S(G)| + \omega_2$ (the vertices of U'' are moved into S);
- $|U(G')| = |U(G)| - \omega_2$.

Furthermore, for any integer $\ell \in \mathbb{Z}$, let $\mathscr{G}_{r,s,u}(\ell) \subseteq \mathscr{G}_{r,s,u}$ be the subset consisting of graphs such that $n_{\mathtt{s}} - m_{\mathtt{s}} = \ell$, and similarly define $\mathscr{G}'_{r,s,u}(\ell) \subseteq \mathscr{G}'_{r,s,u}$ to be the subset consisting of graphs such that $n_{\mathtt{s}} - m_{\mathtt{s}} = \ell' := \ell - \omega_2$.

Proposition 7.7. *Suppose that we have parameters r, s, u satisfying*

$$r = \left(1 + o\left(\frac{1}{\omega_1}\right)\right)\bar{r}, \qquad s = \left(1 + o\left(\frac{1}{\omega_1}\right)\right)\bar{s}, \qquad u = \left(1 + o\left(\frac{1}{\omega_1}\right)\right)\bar{u}.$$

Then for any integer $\ell \in \mathbb{Z}$ we have $\mathbb{P}\left[G(\boldsymbol{A}) \in \mathscr{G}_{r,s,u}(\ell)\right] = (1 + o(1))\mathbb{P}\left[G(\boldsymbol{A}) \in \mathscr{G}'_{r,s,u}(\ell)\right]$.

Proof. We construct an auxiliary bipartite graph H with classes $\mathscr{G}_{r,s,u}(\ell), \mathscr{G}'_{r,s,u}(\ell)$, and with an edge between $G \in \mathscr{G}_{r,s,u}(\ell)$ and $G' \in \mathscr{G}'_{r,s,u}(\ell)$ if G' can be obtained from G by deleting the edges incident to a set $U'' \subseteq U(G)$ of size ω_2. (Note that by Claim 7.6, G' satisfies $n'_{\mathtt{s}} = n_{\mathtt{s}} - \omega_2$ and $m'_{\mathtt{s}} = m_{\mathtt{s}}$, so $n'_{\mathtt{s}} - m'_{\mathtt{s}} = (n_{\mathtt{s}} - m_{\mathtt{s}}) - \omega_2 = \ell - \omega_2 = \ell'$, so such an edge is plausible.)

By Claim 7.5 (and the fact that $\omega_2 \le \omega_1$), every graph $G \in \mathscr{G}_{r,s,u}(\ell)$ is incident to $(1 + o(1))\binom{un}{\omega_2}$ edges of H, since almost every choice of ω_2 nodes from U will result in a graph from $\mathscr{G}'_{r,s,u}(\ell)$.

On the other hand, given a graph $G' \in \mathscr{G}'_{r,s,u}(\ell)$, we may construct a graph $G \in \mathscr{G}_{r,s,u}(\ell)$ by picking any set of ω_2 nodes within $S(G')$, any set of $2\omega_2$ nodes within $R(G')$ and adding $2\omega_2$ edges between them in the appropriate way. Thus we may double-count the edges of H and obtain

$$\left|\mathscr{G}_{r,s,u}(\ell)\right|\binom{un}{\omega_2} = (1 + o(1))\left|\mathscr{G}'_{r,s,u}(\ell)\right|\binom{sn}{\omega_2}\binom{rn}{2\omega_2}\frac{(2\omega_2)!}{2^{\omega_2}}.$$

Since r, s, u are very close to their idealised values $\bar{r}, \bar{s}, \bar{u}$, some standard approximations lead to

$$\frac{\left|\mathscr{G}_{r,s,u}(\ell)\right|}{\left|\mathscr{G}'_{r,s,u}(\ell)\right|} = (1+o(1))\left(\frac{\bar{s}\bar{r}^2 n^2}{2\bar{u}}\right)^{\omega_2}. \tag{7.2}$$

Substituting in the definitions of $\bar{r}, \bar{s}, \bar{u}$, some elementary calculations and (3.9) show that $\frac{\bar{s}\bar{r}^2}{2\bar{u}} = \frac{1}{d^2} = \frac{1}{p^2 n^2}$. Substituting this into (7.2), we obtain

$$\left|\mathscr{G}_{r,s,u}(\ell)\right| = (1+o(1))\left|\mathscr{G}'_{r,s,u}(\ell)\right| p^{-2\omega_2}. \tag{7.3}$$

On the other hand, let us observe that for any graph $G \in \mathscr{G}_{r,s,u}(\ell)$ and any graph G' constructed from G as above, G' has precisely $2\omega_2$ edges fewer than G, and therefore

$$\mathbb{P}\left[G(\boldsymbol{A}) = G'\right] = \mathbb{P}\left[G(\boldsymbol{A}) = G\right] p^{-2\omega_2}(1-p)^{2\omega_2} = (1+o(1))\mathbb{P}\left[G(\boldsymbol{A}) = G\right] p^{-2\omega_2}. \tag{7.4}$$

Combining (7.3) and (7.4), we deduce the statement of the proposition. □

Proof of Lemma 7.1. For any $(r,s,u) = (1+o(\omega_1^{-1}))(\bar{r},\bar{s},\bar{u})$ and for any $G \in \mathscr{G}_{r,s,u}$, pick an arbitrary subset $U'' \subseteq U'$ of size ω_2, where U' is as in Claim 7.5 and let $G' := G\langle U''\rangle$.

Let us define the set $\mathscr{S} = \left\{(r,s,u) : \frac{r}{\bar{r}} = \frac{s}{\bar{s}} = \frac{u}{\bar{u}} = 1+o(1)\right\}$. Observe that since $\omega_2 \le \omega_1 = o(n)$ we have

$$(r,s,u) \in \mathscr{S} \Leftrightarrow \left(r + \frac{2\omega_2}{n}, s + \frac{\omega_2}{n}, u - \frac{\omega_2}{n}\right) \in \mathscr{S}.$$

Using this fact, we obtain

$$\begin{aligned}\mathbb{P}\left[|n_{\mathtt{s}} - m_{\mathtt{s}}| \le \omega_0\right] &= \left(\sum_{(r,s,u)\in\mathscr{S}} \sum_{|\ell|\le\omega_0} \mathbb{P}\left[G(\boldsymbol{A}) \in \mathscr{G}_{r,s,u}(\ell)\right]\right) + o(1) \\ &\overset{\text{P.7.7}}{=} \left(\sum_{(r,s,u)\in\mathscr{S}} \sum_{|\ell|\le\omega_0} \mathbb{P}\left[G(\boldsymbol{A}) \in \mathscr{G}'_{r,s,u}(\ell)\right]\right) + o(1) = \mathbb{P}\left[|n_{\mathtt{s}} - m_{\mathtt{s}} + \omega_2| \le \omega_0\right] + o(1).\end{aligned}$$

However, since ω_2 is chosen uniformly at random from the interval $[\omega_1/2, \omega_1]$, and in particular independently of $\boldsymbol{A}$, we may change our point of view and say that

$$\mathbb{P}\left[|n_{\mathtt{s}} - m_{\mathtt{s}} + \omega_2| \le \omega_0\right] = \mathbb{P}\left[\omega_2 = |m_{\mathtt{s}} - n_{\mathtt{s}}| \pm \omega_0\right] \le \frac{2\omega_0 + 1}{\omega_1/2} = o(1),$$

as required. □

8. Moments and expansion

8.1. **Overview.** In this section we prove Proposition 2.10. The proofs of the two statements of the proposition proceed via two rather different arguments. First we show that it is unlikely that $|V_{\mathtt{s}}(\boldsymbol{A})| - |C_{\mathtt{s}}(\boldsymbol{A})|$ is large and at the same time $f(\boldsymbol{A}) \sim \alpha^*$, which would imply that the slush is almost entirely frozen. The proof relies on the fact that $G(\boldsymbol{A})$ is unlikely to contain a moderately large, relatively densely connected subgraph. Specifically, let A be a matrix. A *flipper* of A is a set of variable nodes $U \subseteq V(A)$ such that for all $a \in \partial U$ we have $|\partial a \cap U| \ge 2$. Let $\mathfrak{F}_\varepsilon(A)$ be the set of all flippers U of A of size $|U| \le \varepsilon n$. Moreover, let $F_\varepsilon(A) = \sum_{U\in\mathfrak{F}_\varepsilon(A)} |U|$ be the total size of all flippers of A which individually each have size at most εn.

Lemma 8.1. *For any $d > 0$ there exists $\varepsilon > 0$ such that for any function $\omega = \omega(n) \gg 1$ we have $F_\varepsilon(\boldsymbol{A}_{\mathtt{s}}) \le \omega$ w.h.p.*

The proof of Lemma 8.1 can be found in Section 8.2. We will combine Lemma 8.1 with the following statement to bound the size of $V_{\mathtt{s}}(\boldsymbol{A}) \setminus \mathscr{F}(\boldsymbol{A}_{\mathtt{s}})$.

Lemma 8.2. *The set $U = V_{\mathtt{s}}(\boldsymbol{A}) \setminus \mathscr{F}(\boldsymbol{A}_{\mathtt{s}})$ is a flipper of $\boldsymbol{A}_{\mathtt{s}}$ of size $|U| \ge |V_{\mathtt{s}}(\boldsymbol{A})| - |C_{\mathtt{s}}(\boldsymbol{A})|$ and $U \cap \mathscr{F}(\boldsymbol{A}) = \emptyset$.*

Proof. Clearly, $\operatorname{nul} \boldsymbol{A}_{\mathtt{s}} \ge |V_{\mathtt{s}}(\boldsymbol{A})| - |C_{\mathtt{s}}(\boldsymbol{A})|$ and thus

$$2^{|V_{\mathtt{s}}(\boldsymbol{A})| - |C_{\mathtt{s}}(\boldsymbol{A})|} \le 2^{\operatorname{nul} \boldsymbol{A}_{\mathtt{s}}} = |\ker \boldsymbol{A}_{\mathtt{s}}| \le \left|\left\{\xi \in \mathbb{F}_2^{|V_{\mathtt{s}}(\boldsymbol{A})|} : \forall v \in \mathscr{F}(\boldsymbol{A}_{\mathtt{s}}) : \xi_v = 0\right\}\right| = 2^{|U|}.$$

Hence, $|U| \ge |V_{\mathtt{s}}(\boldsymbol{A})| - |C_{\mathtt{s}}(\boldsymbol{A})|$.

To show that U is a flipper of A we consider a variable node $v \in U$ and an adjacent check node $a \in C_{\mathtt{s}}(\boldsymbol{A})$. Assume for a contradiction that $\partial a \cap U = \{v\}$. Then for all other variable nodes $u \in \partial a \cap V_{\mathtt{s}}(\boldsymbol{A})$ we have $u \in \mathscr{F}(\boldsymbol{A}_{\mathtt{s}})$. Hence, the only way to satisfy check a is by setting v to zero, too. Thus, $v \in \mathscr{F}(\boldsymbol{A}_{\mathtt{s}})$, which contradicts $v \in U$.

Finally, to show that $U \cap \mathscr{F}(\boldsymbol{A}) = \emptyset$ it suffices to prove that any vector $\xi_{\mathtt{s}} \in \ker \boldsymbol{A}_{\mathtt{s}}$ extends to a vector $\xi \in \ker \boldsymbol{A}$. To see this we recall the peeling process (2.7) that yields $V_{\mathtt{s}}(\boldsymbol{A})$. Let us actually run this peeling process in two stages. In the first stage we repeatedly remove check nodes of degree one or less from $G(\boldsymbol{A})$:

while there is a check node of degree one or less, remove it along with its adjacent variable (if any).

The set of variable nodes that this process removes is precisely $V_{\mathtt{f}}(\boldsymbol{A})$ and we extend $\xi_{\mathtt{s}}$ by setting $\xi_v = 0$ for all $v \in V_{\mathtt{f}}(\boldsymbol{A})$. Next we repeatedly delete variable nodes of degree one or less:

while there is a variable node of degree one or less, remove it along with its adjacent check (if any).

Let $y_1, \ldots, y_\ell$ be the variable nodes that this process deletes, and suppose that they were deleted in this order. Then we inductively extend $\xi_{\mathtt{s}}$ by assigning the variables in the reverse order $y_\ell, \ldots, y_1$ as follows. At the time y_k was deleted, where $1 \le k \le \ell$, this variable node either had no adjacent check node at all, in which case we define $\xi_{y_k} = 0$, or there was precisely one adjacent check node b_k. In the latter case we set ξ_{y_k} to the (unique) value that satisfies b_k given the previously defined entries of ξ. The construction ensures that $\xi \in \ker \boldsymbol{A}$. □

Second, we bound the probability that $|C_{\mathtt{s}}(\boldsymbol{A})| - |V_{\mathtt{s}}(\boldsymbol{A})|$ is large and at the same time $f(\boldsymbol{A}) \sim \alpha_*$. The proof of the following lemma, which we postpone to Section 8.3, is based on a delicate moment calculation.

Lemma 8.3. *For any $d >$ e there exists $\varepsilon > 0$ such that for any $\omega = \omega(n) \gg 1$ we have*

$$\mathbb{P}\left[|C_{\mathtt{s}}(\boldsymbol{A})| - |V_{\mathtt{s}}(\boldsymbol{A})| \ge \omega \text{ and } |V_{\mathtt{s}}(\boldsymbol{A}) \cap \mathscr{F}(\boldsymbol{A})| < \varepsilon n\right] = o(1).$$

Proof of Proposition 2.10. Fix a small enough $\varepsilon > 0$ and suppose that $\omega \to \infty$. To prove the first statement let $\mathscr{E} = \{|V_{\mathtt{s}}(\boldsymbol{A})| - |C_{\mathtt{s}}(\boldsymbol{A})| \ge \omega\}$ and $\mathscr{E}' = \{F_\varepsilon(\boldsymbol{A}) < \omega\}$. Lemma 8.2 shows that if the event $\mathscr{E} \cap \mathscr{E}'$ occurs, then the set $U = V_{\mathtt{s}}(\boldsymbol{A}) \setminus \mathscr{F}(\boldsymbol{A}_{\mathtt{s}})$, being a flipper of size at least ω (by $\mathscr{E}$), cannot be included in $\mathscr{F}_\varepsilon(\boldsymbol{A})$ (because of $\mathscr{E}'$) and therefore has size at least εn. Additionally, we have $U \cap \mathscr{F}(\boldsymbol{A}) = \emptyset$ while $U \subseteq V_{\mathtt{s}}(\boldsymbol{A}) \subseteq V(\boldsymbol{A}) \setminus V_{\mathtt{u}}(\boldsymbol{A})$. Hence, Proposition 2.4 implies $f(\boldsymbol{A}) \le |V(\boldsymbol{A}) \setminus V_{\mathtt{u}}(\boldsymbol{A})|/n + o(1) - \varepsilon$. Consequently, Proposition 2.5 and Lemma 8.1 yield

$$\mathbb{P}\left[\mathscr{E} \cap \left\{f(\boldsymbol{A}) > \alpha^* - \varepsilon/2\right\}\right] \le \mathbb{P}\left[\{F_\varepsilon(\boldsymbol{A}) > \omega\} \cup \left\{|V(\boldsymbol{A}) \setminus V_{\mathtt{u}}(\boldsymbol{A})|/n > \alpha^* + \varepsilon/3\right\}\right] = o(1).$$

Thus, Propositions 2.7 and 2.8 show that $\mathbb{P}\left[\mathscr{E} \cap \left\{\left|f(\boldsymbol{A}) - \alpha_*\right| > \varepsilon\right\}\right] = o(1)$.

With respect to the second statement, let $\mathscr{A} = \{|C_{\mathtt{s}}(\boldsymbol{A})| - |V_{\mathtt{s}}(\boldsymbol{A})| \ge \omega\}$ and $\mathscr{A}' = \{|V_{\mathtt{s}}(\boldsymbol{A}) \cap \mathscr{F}(\boldsymbol{A})| < \varepsilon n\}$. Then Lemma 8.3 shows that

$$\mathbb{P}\left[\mathscr{A} \cap \mathscr{A}'\right] = o(1). \tag{8.1}$$

Moreover, Proposition 2.5 and (2.3) show that

$$\mathbb{P}\left[\left\{f(\boldsymbol{A}) \le \alpha_* + \varepsilon/2\right\} \setminus \mathscr{A}'\right] = o(1), \tag{8.2}$$

and the assertion is immediate from (8.1), (8.2) and Propositions 2.7 and 2.8. □

8.2. **Proof of Lemma 8.1.** A (u, c, m)*-flipper of* $\boldsymbol{A}_{\mathtt{s}}$ consists of a set $U \subseteq V_{\mathtt{s}}(\boldsymbol{A})$ of size $|U| = u$ whose neighbourhood $C = \partial U \cap C_{\mathtt{s}}(\boldsymbol{A})$ has size $|C| = c$ such that the number the number of U-C-edges in $G_{\mathtt{s}}(\boldsymbol{A})$ is equal to m. Let $\boldsymbol{Z}(u, c, m)$ be the number of (u, c, m)-flippers. As a first step we deal with flippers whose average variable degree exceeds two.

Claim 8.4. *For any $d > 0, \delta > 0$ there exists $\varepsilon > 0$ such that*

$$\mathbb{E}\left[\sum_{U \in \mathfrak{F}_\varepsilon(\boldsymbol{A})} |U| \mathbf{1}\left\{\sum_{x \in U} |\partial x \cap C_{\mathtt{s}}(\boldsymbol{A})| \ge (2+\delta)|U|\right\}\right] = o(1).$$

Proof. Recalling $p = d/n \wedge 1$, we write the simple-minded bound

$$\mathbb{E}[u\boldsymbol{Z}(u, c, m)] \le u\binom{n}{u}\binom{n}{c}\binom{uc}{m}p^m; \tag{8.3}$$

here $\binom{n}{u}$ counts the number of choices for U, $\binom{n}{c}$ accounts for the number of possible sets of c check nodes, $\binom{uc}{m}$ bounds the number of bipartite graphs on the chosen variable and check sets, and p^m bounds the probability that the chosen subgraph is actually contained in $G(\boldsymbol{A})$. We aim to bound the r.h.s. of (8.3) subject to the constraints

$$m \ge \max\{2c, (2+\delta)u\}, \qquad 1 \le u \le \varepsilon n \qquad \text{for a small enough } \varepsilon > 0. \tag{8.4}$$

We consider three separate cases.

Case 1: $c \le u$**:** we estimate

$$\binom{n}{u}\binom{n}{c}\binom{uc}{m}p^m \le \left(\frac{\mathrm{e}n}{u}\right)^{2u}\left(\frac{\mathrm{e}ucd}{mn}\right)^m \le \left(\frac{\mathrm{e}n}{u}\right)^{2u}\left(\frac{\mathrm{e}cd}{2n}\right)^{(2+\delta)u} \le \left(\mathrm{e}^{4+\delta}d^{2+\delta}\right)^u\left(\frac{u}{n}\right)^{\delta u}. \tag{8.5}$$

Combining (8.3)–(8.5), we obtain

$$\sum_{1\le c\le u\le \varepsilon n}\mathbb{E}[u\boldsymbol{Z}(u,c,m)] \le \sum_{1\le u\le \varepsilon n} u^2\left(\mathrm{e}^{4+\delta}d^{2+\delta}\right)^u\left(\frac{u}{n}\right)^{\delta u} = o(1). \tag{8.6}$$

Case 2: $u \le c \le 100u$**:** due to (8.4) we obtain

$$\binom{n}{u}\binom{n}{c}\binom{uc}{m}p^m \le \left(\frac{\mathrm{e}n}{u}\right)^u\left(\frac{\mathrm{e}n}{c}\right)^c\left(\frac{\mathrm{e}ud}{2n}\right)^c\left(\frac{\mathrm{e}ud}{2n}\right)^{m/2} \le \left(\frac{\mathrm{e}n}{u}\right)^u\left(\frac{\mathrm{e}^2d}{2}\right)^c\left(\frac{\mathrm{e}ud}{2n}\right)^{u(1+\delta/2)} \le \left(\frac{\mathrm{e}^2d}{2}\right)^{400u}\left(\frac{u}{n}\right)^{\delta u/2}. \tag{8.7}$$

Combining (8.3) and (8.8), we get

$$\sum_{\substack{1\le u\le \varepsilon n\\ u\le c\le 100u}}\mathbb{E}[u\boldsymbol{Z}(u,c,m)] \le \sum_{1\le u\le \varepsilon n} 100u^2\left(\frac{\mathrm{e}^2d}{2}\right)^{400u}\left(\frac{u}{n}\right)^{\delta/2} = o(1). \tag{8.8}$$

Case 3: $100u \le c \le n$**:** the condition (8.4) yields

$$\binom{n}{u}\binom{n}{c}\binom{uc}{m}p^m \le \left(\frac{100\mathrm{e}n}{c}\right)^{1.1c}\left(\frac{\mathrm{e}du}{n}\right)^{2c} \le \left(\frac{\mathrm{e}du}{n}\right)^{c/2}.$$

Hence,

$$\sum_{\substack{1\le u\le \varepsilon n\\ 100u\le c\le n}}\mathbb{E}[u\boldsymbol{Z}(u,c,m)] \le \sum_{1\le u\le \varepsilon n} u\sum_{100u\le c\le n}\left(\frac{\mathrm{e}du}{n}\right)^{c/2} \le \sum_{1\le u\le \varepsilon n} u\left(\frac{\mathrm{e}du}{n}\right)^u = o(1). \tag{8.9}$$

Finally, the assertion follows from (8.6), (8.8) and (8.9). □

Complementing Claim 8.4, we now estimate the sizes of flippers of average check degree greater than two.

Claim 8.5. *For any $d > 0, \delta > 0$ there exists $\varepsilon > 0$ such that*

$$\mathbb{E}\left[\sum_{U\in\mathfrak{F}_\varepsilon(\boldsymbol{A})}|U|\mathbf{1}\left\{\sum_{a\in\partial U\cap C_{\mathtt{s}}(\boldsymbol{A})}|\partial a\cap U| \ge (2+\delta)|C|\right\}\right] = o(1).$$

Proof. The proof is rather similar to the proof of the previous claim, except that we swap the roles of u and c. Once more we start from the naive bound (8.3), but this time m satisfies $m \ge \max\{2u, (2+\delta)c\}$ and $1 \le u \le \varepsilon n$.

Case 1: $u \le c$**:** we have

$$\binom{n}{u}\binom{n}{c}\binom{uc}{m}p^m \le \left(\frac{\mathrm{e}n}{c}\right)^{2c}\left(\frac{\mathrm{e}ud}{2n}\right)^{(2+\delta)c} \le (\mathrm{e}d)^{5c}\left(\frac{u}{n}\right)^{\delta c}. \tag{8.10}$$

Case 2: $c \le u \le 100c$**:** we estimate

$$\binom{n}{u}\binom{n}{c}\binom{uc}{m}p^m \le \left(\frac{\mathrm{e}n}{u}\right)^u\left(\frac{\mathrm{e}n}{c}\right)^c\left(\frac{\mathrm{e}cd}{2n}\right)^u\left(\frac{\mathrm{e}cd}{2n}\right)^{m/2} \le \left(\frac{\mathrm{e}n}{c}\right)^c\left(\frac{\mathrm{e}^2d}{2}\right)^u\left(\frac{\mathrm{e}cd}{2n}\right)^{c(1+\delta/2)} \le \left(\frac{100\mathrm{e}^2d}{2}\right)^u\left(\frac{u}{n}\right)^{\delta u/200}. \tag{8.11}$$

Case 3: $100c \le u$**:** we have

$$\binom{n}{u}\binom{n}{c}\binom{uc}{m}p^m \le \left(\frac{\mathrm{e}n}{u}\right)^{1.1u}\left(\frac{\mathrm{e}dc}{n}\right)^{2u} \le \left(\frac{\mathrm{e}du}{n}\right)^{c/2}. \tag{8.12}$$

Summing (8.10), (8.11) and (8.12) on u, c, m such that $m \ge (2+\delta)c$, we obtain $\sum_{u,c,m}\mathbb{E}[uZ(u,c,m)] = o(1)$. □

Finally, we need to deal with flippers of average variable and constraint degree about two.

Claim 8.6. *For any $d >$ e there exists $\varepsilon > 0$ such that for any $\omega = \omega(n) \gg 1$ we have*

$$\mathbb{P}\left[\sum_{U\in\mathfrak{F}_\varepsilon(\boldsymbol{A})}|U|\mathbf{1}\left\{\sum_{x\in U}|\partial x\cap C_{\mathtt{s}}(\boldsymbol{A})| \le (2+\varepsilon)|U|, \sum_{a\in\partial U\cap C_{\mathtt{s}}(\boldsymbol{A})}|\partial a\cap U| \le (2+\varepsilon)|C|\right\} > \omega\right] = o(1).$$

Proof. Choose $L = L(d) > 0$ sufficiently large and subsequently $\varepsilon > 0$ sufficiently small. Moreover, for a vertex u of $G_{\mathbf{s}}(\boldsymbol{A})$ let $d_{\mathbf{s}}(u)$ signify the degree of u in $G_{\mathbf{s}}(\boldsymbol{A})$. Further, with ν, λ from (2.8) let $\mathscr{D}$ be the event that the graph $G_{\mathbf{s}}(\boldsymbol{A})$ enjoys the following four properties.

D1: $|V_{\mathbf{s}}(\boldsymbol{A})| = (\nu + o(1))n$ and $|C_{\mathbf{s}}(\boldsymbol{A})| = (\nu + o(1))n$.
D2: For any $2 \le \ell \le L$ we have $\sum_{x \in V_{\mathbf{s}}(\boldsymbol{A})} \mathbf{1}\{d_{\mathbf{s}}(x) = \ell\} = \mathbb{P}[\mathrm{Po}_{\ge 2}(\lambda) = \ell]\,\nu n + o(n)$.
D3: For any $2 \le \ell \le L$ we have $\sum_{a \in C_{\mathbf{s}}(\boldsymbol{A})} \mathbf{1}\{d_{\mathbf{s}}(a) = \ell\} = \mathbb{P}[\mathrm{Po}_{\ge 2}(\lambda) = \ell]\,\nu n + o(n)$.
D4: The bounds from (2.11) hold for the degree sequence of $G(\boldsymbol{A})$.

Then Proposition 2.6 and Lemma 2.14 imply that

$$\mathbb{P}[\mathscr{D}] = 1 - o(1). \tag{8.13}$$

We aim to count (u,c,m)-flippers $U \subseteq V_{\mathbf{s}}(\boldsymbol{A})$ with neighbourhoods $C = \partial U \cap C_{\mathbf{s}}(\boldsymbol{A})$ of size $|C| = c$ such that

$$m = \sum_{x \in U} |\partial x \cap C| = \sum_{a \in C} |\partial a \cap U| \le (2+\varepsilon)(u \wedge c), \qquad \text{and, of course,} \qquad \min_{a \in C} |\partial a \cap U| \ge 2. \tag{8.14}$$

To estimate the number $\boldsymbol{Z}(u,c,m)$ we recall from Proposition 2.6 that the graph $G_{\mathbf{s}}(\boldsymbol{A})$ is uniformly random given the degrees. Therefore, according to Lemma 2.13 it suffices to bound the number of (u,c,m)-flippers of a random graph chosen from the pairing model with the same degree sequence. Thus, let $\boldsymbol{\Gamma}_{\mathbf{s}}$ be a random perfect matching of the complete bipartite graph on the vertex sets

$$\mathscr{V} = \bigcup_{v \in V_{\mathbf{s}}(\boldsymbol{A})} \{v\} \times [d_{\mathbf{s}}(v)], \qquad \mathscr{C} = \bigcup_{a \in C_{\mathbf{s}}(\boldsymbol{A})} \{a\} \times [d_{\mathbf{s}}(a)].$$

Further, let $\mathscr{G}_{\mathbf{s}}$ be the multigraph obtained from $\boldsymbol{\Gamma}_{\mathbf{s}}$ by contracting the clones $\{v\} \times [d_{\mathbf{s}}(v)]$ and $\{a\} \times [d_{\mathbf{s}}(a)]$ of the variable and constraint nodes into single vertices for all $v \in V_{\mathbf{s}}(\boldsymbol{A})$, $a \in C_{\mathbf{s}}(\boldsymbol{A})$. Due to (8.13) it suffices to establish the bound

$$\sum_{u,c,m : 1 \le u \le \varepsilon n} u\mathbb{E}[\boldsymbol{Z}(u,c,m) \mid \mathscr{D}] = O(1). \tag{8.15}$$

To prove (8.15) we first count viable choices of U. Since (8.14) implies that $2u \le m \le (2+\varepsilon)u$, no more than δu of the vertices in the set U have degree greater than two. Further, **D1** and **D2** show that there are no more than

$$\binom{(\nu+o(1))n}{u}\binom{u}{\varepsilon u}\left(\frac{\lambda^2+o(1)}{2(\exp(\lambda)-\lambda-1)}\right)^{(1-\varepsilon)u} \le \left(\frac{\mathrm{e}L}{\varepsilon}\right)^{\varepsilon u}\left(\frac{\mathrm{e}(\nu+o(1))n}{u}\right)^{u}\left(\frac{\lambda^2+o(1)}{2(\exp(\lambda)-\lambda-1)}\right)^{u} \tag{8.16}$$

such sets U.

By a similar token, most check nodes in C have precisely two neighbours in U. Thus, we estimate the number of choices of $C \subseteq C_{\mathbf{s}}(\boldsymbol{A})$ of size c along with a set $\mathfrak{C}$ of m clones of these checks as follows. Summing on all vectors $\boldsymbol{k} = (k_1, \ldots, k_c)$ of integers $k_i \ge 2$ with $\sum_i k_i = m$ and on all sequences $(b_1, \ldots, b_c) \in C_{\mathbf{s}}(\boldsymbol{A})^c$, we obtain the bound

$$\frac{1}{c!}\sum_{b_1,\ldots,b_c \in C_{\mathbf{s}}(\boldsymbol{A})}\sum_{\boldsymbol{k}}\prod_{i=1}^{c}\binom{d_{\mathbf{s}}(b_i)}{k_i} = \frac{1}{c!}\sum_{\boldsymbol{k}}\prod_{i=1}^{c}\sum_{b \in C_{\mathbf{s}}(\boldsymbol{A})}\binom{d_{\mathbf{s}}(b)}{k_i}. \tag{8.17}$$

Now, (8.14) implies that $\sum_{i \le c} \mathbf{1}\{k_i > 2\}\, k_i \le 3\varepsilon c$. Therefore, **D3** and **D4** ensure that for any $\boldsymbol{k}$,

$$\prod_{i=1}^{c}\sum_{b \in C_{\mathbf{s}}(\boldsymbol{A})}\binom{d_{\mathbf{s}}(b)}{k_i} \le L^{3\varepsilon c}\prod_{i=1}^{c}\sum_{b \in C_{\mathbf{s}}(\boldsymbol{A})}\binom{d_{\mathbf{s}}(b)}{2} \le L^{3\varepsilon c}((\nu+o(1))n)^c\left(\frac{\lambda^2\exp(\lambda)+o(1)}{2(\exp(\lambda)-\lambda-1)}\right)^{c}. \tag{8.18}$$

Furthermore, there are no more than $\binom{m-c-1}{c-1} = \binom{m-c-1}{m-2c}$ possible vectors $\boldsymbol{k}$ and thus (8.14) yields

$$\binom{m-c-1}{m-2c} \le \left(\frac{2\mathrm{e}}{\varepsilon}\right)^{\varepsilon c}. \tag{8.19}$$

Combining (8.17)–(8.19) with **D1**, we see that the number of possible $C, \mathfrak{C}$ is bounded by

$$\left(\frac{2\mathrm{e}L^3}{\varepsilon}\right)^{\varepsilon c}\left(\frac{\mathrm{e}(\nu+o(1))n}{c}\right)^{c}\left(\frac{\lambda^2\exp(\lambda)+o(1)}{2(\exp(\lambda)-\lambda-1)}\right)^{c}. \tag{8.20}$$

Finally, since **D2** and **D4** imply that

$$\sum_{x \in V_{\mathbf{s}}(\boldsymbol{A})} d_{\mathbf{s}}(x) = (1+o_\varepsilon(1))\nu n\mathbb{E}[\mathrm{Po}_{\ge 2}(\lambda)] = (1+o_\varepsilon(1))\frac{\nu n\lambda(\exp(\lambda)-1)}{\exp(\lambda)-\lambda-1},$$

the probability that $\mathbf{\Gamma}_\mathbf{s}$ matches the designated variable/check clones comes to

$$\frac{m!(\sum_{x\in V_\mathbf{s}(\boldsymbol{A})} d_\mathbf{s}(x)-m)!}{(\sum_{x\in V_\mathbf{s}(\boldsymbol{A})} d_\mathbf{s}(x))!}=\binom{\sum_{x\in V_\mathbf{s}(\boldsymbol{A})} d_\mathbf{s}(x)}{m}^{-1}=\left(\frac{\mathrm{e}(\lambda(\exp(\lambda)-1)\nu+o_\varepsilon(1))n}{m(\exp(\lambda)-\lambda-1)}\right)^{-m}. \tag{8.21}$$

Combining (8.16), (8.20) and (8.21) (and dragging all $o(1)$-error terms into the $o_\varepsilon(1)$), we obtain

$$\mathbb{E}[\boldsymbol{Z}(u,c,m)\mid\mathscr{D}]\le\left(\frac{\mathrm{e}\nu n}{u}\right)^u\left(\frac{\mathrm{e}\nu n}{c}\right)^c\left(\frac{\mathrm{e}(\lambda(\exp(\lambda)-1)\nu+o_\varepsilon(1))n}{m(\exp(\lambda)-\lambda-1)}\right)^{-m}\left(\frac{\lambda^2\exp(\lambda)}{2(\exp(\lambda)-\lambda-1)}\right)^c\left(\frac{\lambda^2}{2(\exp(\lambda)-\lambda-1)}\right)^u.$$

Hence, (8.14) yields

$$\mathbb{E}[\boldsymbol{Z}(u,c,m)\mid\mathscr{D}]\le\left(\frac{u}{n}\right)^{m-u-c}\left(\frac{\lambda^2\exp(\lambda)+o_\varepsilon(1)}{(\exp(\lambda)-1)^2}\right)^u. \tag{8.22}$$

Since $\lambda>0$ we have $\lambda^2\exp(\lambda)/((\exp(\lambda)-1)^2)<1$. Therefore, (8.22) implies (8.15) for small $\varepsilon>0$. □

Proof of Lemma 8.1. The lemma follows from Claims 8.4, 8.5 and 8.6. More precisely, let given $d>\mathrm{e}$, let ε_1 be the ε given by Claim 8.6, and subsequently set $\delta:=\varepsilon_1$ and let $\varepsilon_2,\varepsilon_3$ be the ε given by Claims 8.4 and 8.5 respectively. Then let us set $\varepsilon_0:=\varepsilon_1\wedge\varepsilon_2\wedge\varepsilon_3$.

Now Claims 8.4 and 8.5 imply that w.h.p. there is no $U\in\mathfrak{F}_{\varepsilon_0}(\boldsymbol{A})$ with $\sum_{x\in U}|\partial x\cap C_\mathbf{s}(\boldsymbol{A})|\ge(2+\delta)|U|$ or with $\sum_{a\in\partial U\cap C_\mathbf{s}(\boldsymbol{A})}|\partial a\cap U|\ge(2+\delta)|C|$. On the other hand, conditioning on this event, since $\varepsilon_0\le\varepsilon_1=\delta$ we have $\mathfrak{F}_{\varepsilon_0}(\boldsymbol{A})\subseteq\mathfrak{F}_\delta(\boldsymbol{A})$, and therefore Claim 8.6 implies that w.h.p. $F_{\varepsilon_0}(\boldsymbol{A})\le\omega$ for any function $\omega=\omega(n)\gg1$, as required. □

8.3. **Proof of Lemma 8.3.** The proof is based on a somewhat delicate moment calculation. Suppose that $|V_\mathbf{s}(\boldsymbol{A})\cap\mathscr{F}(\boldsymbol{A})|<\varepsilon n$, i.e., very few coordinates in the slush are frozen. Then Fact 2.17 implies that for most $v\in V_\mathbf{s}(\boldsymbol{A})$ the corresponding entry $\boldsymbol{x}_{\mathbf{s},v}$ of a random vector $\boldsymbol{x}_\mathbf{s}\in\ker\boldsymbol{A}_\mathbf{s}$ takes the value 0 with probability precisely 1/2. Furthermore, since $|V_\mathbf{s}(\boldsymbol{A})|=\Omega(n)$ w.h.p., Proposition 2.11 implies that for most pairs $u,v\in V_\mathbf{s}(\boldsymbol{A})$ the entries $\boldsymbol{x}_{\mathbf{s},u},\boldsymbol{x}_{\mathbf{s},v}$ are stochastically independent. Therefore, w.h.p. the random vector $\boldsymbol{x}_\mathbf{s}$ has Hamming weight $(1/2+o_\varepsilon(1))|V_\mathbf{s}(\boldsymbol{A})|$. Hence, a tempting first idea toward the proof of Lemma 8.3 might be to simply calculate the expected number of vectors of Hamming weight $(1/2+o_\varepsilon(1))|V_\mathbf{s}(\boldsymbol{A})|$ in the kernel of $\boldsymbol{A}_\mathbf{s}$.

This strategy would work if we could replace the $o_\varepsilon(1)$ error term above by $O(n^{-1/2})$. Indeed, there are $2^{|V_\mathbf{s}(\boldsymbol{A})|}$ candidate vectors of Hamming weight $|V_\mathbf{s}(\boldsymbol{A})|/2+O(\sqrt{n})$. Moreover, it is not very hard to verify that a given such vector satisfies all checks with probability $\Theta(2^{-|C_\mathbf{s}(\boldsymbol{A})|})$. As a consequence, the expected number of vectors in $\ker\boldsymbol{A}_\mathbf{s}$ of Hamming weight $|V_\mathbf{s}(\boldsymbol{A})|/2+O(\sqrt{n})$ tends to zero if $|C_\mathbf{s}(\boldsymbol{A})|-|V_\mathbf{s}(\boldsymbol{A})|\gg1$. But unfortunately this simple calculation does not extend to larger ε as required by Lemma 8.3. The reason is that for larger ε a second order term pop up, i.e., the probability that all checks are satisfied reads

$$2^{-|C_\mathbf{s}(\boldsymbol{A})|+O_\varepsilon(\varepsilon^2)|C_\mathbf{s}(\boldsymbol{A})|}.$$

This quadratic term is due to the presence of checks of degree two. We deal with this problem by observing that a check node of degree two simply imposes an equality constraint on its two adjacent variables. Thus, any two variable nodes that appear in a check node of degree two can be contracted into a single variable node and then the check node can be eliminated. A variant of the moment calculation, without the quadratic error term, can then be applied to the matrix that the multigraph resulting from the contraction procedure induces.

To carry out this programme we first investigate the subgraph $G'_\mathbf{s}(\boldsymbol{A})$ obtained from $G_\mathbf{s}(\boldsymbol{A})$ by deleting all checks of degree greater than two. More precisely, invoking Lemma 2.13, for the apparent technical reason we will instead analyse the random multigraph $\mathscr{G}'_\mathbf{s}$ that results by applying the contraction procedure to the random multigraph $\mathscr{G}_\mathbf{s}$ chosen from the pairing model with the same degrees as $\boldsymbol{G}_\mathbf{s}(\boldsymbol{A})$. The proof of the following lemma can be found in Section 8.4.

Lemma 8.7. *For any $d>\mathrm{e}$ there exists $b>0$ such that for any $\omega=\omega(n)\gg1$ the random graph $\mathscr{G}'_\mathbf{s}$ enjoys the following properties w.h.p.*

(i) The largest component of $\mathscr{G}'_\mathbf{s}$ has size at most $\omega\log n$.
(ii) $\mathscr{G}'_\mathbf{s}$ contains no more than ω cycles.
(iii) For any $t>0$ no more than $|V_\mathbf{s}(\boldsymbol{A})|\exp(-bt)$ variable nodes belong to components of size at least t.

Now obtain the multigraph $\mathscr{G}_{\mathtt{s}}''$ from $\mathscr{G}_{\mathtt{s}}$ by deleting all checks of degree two and contracting every connected component of $\mathscr{G}_{\mathtt{s}}'$ into a single variable node. Let us write $\mathscr{V}_{\mathtt{s}}''$ and $\mathscr{C}_{\mathtt{s}}''$ for the set of variable and check nodes of $\mathscr{G}_{\mathtt{s}}''$ and let $\mathscr{A}_{\mathtt{s}}''$ denote the matrix encoded by $\mathscr{G}_{\mathtt{s}}''$. Further, for $v \in \mathscr{V}_{\mathtt{s}}'' \cup \mathscr{C}_{\mathtt{s}}''$ let $d_{\mathtt{s}}''(v)$ be the degree of v in $\mathscr{G}_{\mathtt{s}}''$. Finally, let $\mathscr{K}_{\varepsilon}''$ be the set of all vectors $\xi \in \ker \mathscr{A}_{\mathtt{s}}''$ such that

$$\left| \frac{1}{2} - \frac{\sum_{x \in \mathscr{V}_{\mathtt{s}}''} d_{\mathtt{s}}''(x) \mathbf{1}\{\xi_x = 0\}}{\sum_{x \in \mathscr{V}_{\mathtt{s}}''} d_{\mathtt{s}}''(x)} \right| < \varepsilon.$$

In Section 8.5 we will prove the following statement.

Lemma 8.8. *For any $d >$ e there exists $\varepsilon > 0$ such that for any $\omega = \omega(n) \gg 1$ we have*

$$\mathbb{P}\left[|\mathscr{C}_{\mathtt{s}}''| \geq |\mathscr{V}_{\mathtt{s}}''| + \omega \text{ and } \mathscr{K}_{\varepsilon}'' \neq \emptyset\right] = o(1).$$

In addition, we observe the following.

Lemma 8.9. *For any $d >$ e, $\varepsilon > 0$ there exists $\delta > 0$ such that*

$$\mathbb{P}\left[|V_{\mathtt{s}}(\boldsymbol{A}) \setminus \mathscr{F}(\boldsymbol{A})| > (1-\delta)|V_{\mathtt{s}}(\boldsymbol{A})| \text{ and } \mathscr{K}_{\varepsilon}'' = \emptyset\right] = o(1).$$

The proof of Lemma 8.9 can be found in Section 8.6.

Proof of Lemma 8.3. The assertion is an immediate consequence of Lemmas 8.7, 8.8 and 8.9. □

8.4. **Proof of Lemma 8.7.** We apply a branching process argument to a random graph chosen from the pairing model, not unlikely the one from [38]. Specifically, let $(d_{\mathtt{s}}(v))_{v \in V_{\mathtt{s}}(\boldsymbol{A})}$ be the degree sequence of the graph $G_{\mathtt{s}}(\boldsymbol{A})$ and let $\boldsymbol{m}_{\mathtt{s}}'$ be the number of check of degree two in $G_{\mathtt{s}}(\boldsymbol{A})$. Let us write $b_1, \ldots, b_{\boldsymbol{m}_s'}$ for the check nodes of $\mathscr{G}_{\mathtt{s}}'$. Starting from an edge exiting b_1, we will explore the set of all nodes of $\mathscr{G}_{\mathtt{s}}'$ that can be reached via that edge. We will describe this exploration process as a branching process, which will turn out to be subcritical.

To be precise, let $\boldsymbol{\Delta} = \sum_{v \in V_{\mathtt{s}}(\boldsymbol{A})} d_{\mathtt{s}}(v)$ and let $\boldsymbol{\Gamma}_{\mathtt{s}}'$ be a random perfect matching of the complete bipartite graph with vertex sets

$$\mathscr{V} = \bigcup_{v \in V_{\mathtt{s}}(\boldsymbol{A})} \{v\} \times [d_{\mathtt{s}}(v)] \qquad \text{and} \qquad \mathscr{C} = \left(\{\alpha_1, \ldots, \alpha_{\boldsymbol{m}_{\mathtt{s}}'}\} \times [2]\right) \cup \{\beta_1, \ldots, \beta_{\boldsymbol{\Delta} - 2\boldsymbol{m}_{\mathtt{s}}'}\}.$$

As always, $\{v\} \times [d_{\mathtt{s}}(v)]$ and $\{\alpha_i\} \times [2]$ represent sets of clones of the variable node v and the check node α_i, respectively. The 'ballast' clones $\beta_1, \ldots, \beta_{\boldsymbol{\Delta} - 2\boldsymbol{m}_{\mathtt{s}}'}$ are included so that both sides of the bipartition have the same size. Further, deleting $\beta_1, \ldots, \beta_{\boldsymbol{\Delta} - 2\boldsymbol{m}_{\mathtt{s}}'}$ and contracting the other clones into single vertices, we obtain a random multigraph $\mathscr{G}(\boldsymbol{\Gamma})$ from the matching $\boldsymbol{\Gamma}$. This multigraph is identical in distribution to $\mathscr{G}_{\mathtt{s}}'$.

Claim 8.10. *W.h.p. all connected components of $\mathscr{G}(\boldsymbol{\Gamma})$ have size $O(\log n)$.*

Proof. To trace the set of nodes reachable from $(\alpha_1, 1)$, we classify each clone as either unexplored, active or inactive. At the start of the process only $(\alpha_1, 1)$ is active and all other clones are unexplored; thus,

$$\mathscr{A}_0 = \{(\alpha_1, 1)\}, \qquad \mathscr{U}_0 = \left\{(\alpha_1, 2), (\alpha_2, 1), (\alpha_2, 2), \ldots, (\alpha_{\boldsymbol{m}_{\mathtt{s}}'}, 1), (\alpha_{\boldsymbol{m}_{\mathtt{s}}'}, 2)\right\} \setminus \mathscr{A}_0, \qquad \mathscr{I}_0 = \emptyset.$$

The classification determines the order in which the edges of the matching $\boldsymbol{\Gamma}$ are exposed. Specifically, if at some time $t \geq 1$ no active check clone remains, the process stops and we let $T_0 = t - 1$. Otherwise, at time step $t \geq 1$ an active clone $(\alpha_{\boldsymbol{i}_t}, \boldsymbol{h}_t) \in \mathscr{A}_{t-1}$ is chosen uniformly at random and we let $\mathscr{I}_t = \mathscr{I}_{t-1} \cup \{(\alpha_{\boldsymbol{i}_t}, \boldsymbol{h}_t)\}$. If the second clone $(\alpha_{\boldsymbol{i}_t}, 3 - \boldsymbol{h}_t)$ of the same check is either active or inactive, we let $\mathscr{U}_t = \mathscr{U}_{t-1}$, $\mathscr{A}_t = \mathscr{A}_{t-1} \setminus \{(\alpha_{\boldsymbol{i}_t}, \boldsymbol{h}_t)\}$. Otherwise we expose the edge of $\boldsymbol{\Gamma}$ incident with the other clone $(\alpha_{\boldsymbol{i}_t}, 3 - \boldsymbol{h}_t)$ of check $\alpha_{\boldsymbol{i}_t}$. Let $\boldsymbol{y}_t$ be the variable node on the other end of this edge. We then declare all as yet inactive clones of checks α_i, $i \in [\boldsymbol{m}_{\mathtt{s}}']$, that are adjacent to clones of $\boldsymbol{y}_t$ active. Formally, we let

$$\mathscr{I}_t = \mathscr{I}_{t-1} \cup \{(\alpha_{\boldsymbol{i}_t}, 1), (\alpha_{\boldsymbol{i}_t}, 2)\}, \qquad \mathscr{A}_t = \left(\mathscr{A}_{t-1} \cup \left(\partial_{\boldsymbol{\Gamma}}(\boldsymbol{y}_t \times [d_{\mathtt{s}}(\boldsymbol{y}_t)]) \cap \{(\alpha_i, 1), (\alpha_i, 2) : i \in [\boldsymbol{m}_{\mathtt{s}}']\}\right)\right) \setminus \mathscr{I}_t$$

and $\mathscr{U}_t = \mathscr{U}_{t-1} \setminus (\mathscr{A}_t \cup \mathscr{I}_t)$. Let $\mathfrak{A}_t$ be the σ-algebra generated by the first t step of the process.

The aim is to investigate the stopping time T_0. We may condition on the event $d_{\mathtt{s}}(v) \leq \log^2 n$ for all v. Moreover, we claim that for $1 \leq t \leq T_0 \wedge \log^3 n$,

$$\mathbb{E}\left[|\mathscr{A}_t| - |\mathscr{A}_{t-1}| \,|\, \mathfrak{A}_{t-1}\right] < 0. \tag{8.23}$$

Indeed, $|\mathscr{A}_t| - |\mathscr{A}_{t-1}|$ is trivially negative if $(b_{\boldsymbol{i}_t}, 3 - \boldsymbol{h}_t) \notin \mathscr{U}_{t-1}$. Further, if $(\alpha_{\boldsymbol{i}_t}, 3 - \boldsymbol{h}_t) \in \mathscr{U}_{t-1}$, then $\boldsymbol{\Gamma}$ matches this clone to a random vacant variable clone. Because $t \leq \log^3 n$ and $\max_v d_{\mathtt{s}}(v) \leq \log^2 n$ while the slush has size

$|V_{\mathsf{s}}(\boldsymbol{A})| = \Omega(n)$, the distribution of $d_{\mathsf{s}}(\boldsymbol{y}_t)$ is within $O(n^{-0.99})$ in total variation of the distribution $(d_{\mathsf{s}}(v)/\boldsymbol{\Delta})_{v\in V_{\mathsf{s}}(\boldsymbol{A})}$ of the degree of the variable node of a random variable clone. We subsequently expose all edges of $\boldsymbol{\Gamma}$ incident with a clone of $\boldsymbol{y}_t$ that was unexplored at time $t-1$. Once more because $t \le \log^3 n$ and $\max_v d_{\mathsf{s}}(v) \le \log^2 n$, the conditional probability that a specific unexplored clone of $\boldsymbol{y}_t$ links to an unexplored clone from the set $\{(\alpha_i,1),(\alpha_i,2) : i \in [\boldsymbol{m}'_{\mathsf{s}}]\}$ is bounded by $2\boldsymbol{m}'_{\mathsf{s}}/\boldsymbol{\Delta} + O(n^{-0.99})$. Therefore, we obtain the bound

$$\mathbb{E}\left[|\mathscr{A}_t| - |\mathscr{A}_{t-1}| \mid \mathfrak{A}_{t-1}\right] \le o(1) - 1 + \mathbb{E}\left[\frac{2\boldsymbol{m}'_{\mathsf{s}}}{\boldsymbol{\Delta}^2}\sum_{v\in V_{\mathsf{s}}(\boldsymbol{A})} d_{\mathsf{s}}(v)(d_{\mathsf{s}}(v)-1)\right] \le \frac{\lambda^2\exp(\lambda)}{(\exp(\lambda)-1)^2} - 1 + o(1). \tag{8.24}$$

Moreover, it is easy to check that $\lambda > 0$ for all $d >$ e and that

$$\frac{z^2\exp(z)}{(\exp(z)-1)^2} < 1 \qquad \text{for any } z > 0. \tag{8.25}$$

Thus, (8.23) follows from (8.24) and (8.25). Finally, (8.23) implies that $(|\mathscr{A}_t|)_t$ is dominated by a random walk with a negative drift. Consequently, $\mathbb{P}\left[T_0 \ge c\log n\right] = o(n^{-1})$ for a suitable $c > 0$. The assertion follows from the union bound. □

Claim 8.11. *There exists $b = b(d) > 0$ such that w.h.p. for all $t > 0$ the number of variable nodes of $\mathscr{G}'_{\mathsf{s}}$ that belong to components of size at least t is bounded by $|V_{\mathsf{s}}(\boldsymbol{A})|\exp(-bt)$.*

Proof. Let $\boldsymbol{Z}_t$ be the number of variable nodes of $\mathscr{G}'_{\mathsf{s}}$ that belong to components of size at least t. Tracing the same exploration process as in the previous proof and using (8.24), we find $\zeta = \zeta(d) > 0$ such that

$$\mathbb{E}[\boldsymbol{Z}_t] \le |V_{\mathsf{s}}(\boldsymbol{A})|\exp(-2\zeta t). \tag{8.26}$$

If $t > \log\log n$, say, then the assertion simply follows from (8.26) and Markov's inequality. Thus, suppose that $t \le \log\log n$ and $|V_{\mathsf{s}}(\boldsymbol{A})| = \Omega(n)$ and that the largest component of $\mathscr{G}'_{\mathsf{s}}$ contains no more than $\log n\log\log n$ variable nodes. Then adding to or removing from $\mathscr{G}'_{\mathsf{s}}$ a single edge can alter $\boldsymbol{Z}_t$ by at most $2t$. Therefore, the assertion follows from (8.26) and Azuma's inequality. □

As a next step we need to estimate the number of short cycles.

Claim 8.12. *The expected number of nodes on cycles of $\mathscr{G}'_{\mathsf{s}}$ of size at most $\log^2 n$ is bounded.*

Proof. Let $\ell \le \log^2 n$, let $\boldsymbol{y} = (y_1,\ldots,y_\ell) \in V_{\mathsf{s}}(\boldsymbol{A})^\ell$ be a sequence of variables, let $\boldsymbol{i} = (i_1,i'_1,\ldots,i_\ell,i'_\ell)$ be a sequence that contains two clones of each variable $y_1,\ldots,y_\ell$ and let $\boldsymbol{\alpha} = (\alpha_1,\ldots,\alpha_\ell)$ be a sequence of ℓ distinct checks of degree two. Let $\mathscr{E}(\boldsymbol{y},\boldsymbol{i},\boldsymbol{\alpha})$ be the event that $\boldsymbol{\Gamma}$ connects the two clones of α_h with (y_h,i'_h) and (y_{h+1},i_{h+1}). Since Proposition 2.6 shows that $\boldsymbol{\Delta} = \Omega(n)$ and $\ell \le \log^2 n$, we obtain

$$\mathbb{P}\left[\mathscr{E}(\boldsymbol{y},\boldsymbol{i},\boldsymbol{\alpha}) \mid (d_x)_x, \boldsymbol{m}'_{\mathsf{s}}\right] \sim \left(2/\boldsymbol{\Delta}^2\right)^\ell.$$

Furthermore, we have

$$\mathbb{E}\left[\sum_{x\in V_{\mathsf{s}}(\boldsymbol{A})}\frac{d_{y_i}(d_{y_i}-1)}{|V_{\mathsf{s}}(\boldsymbol{A})|}\right] \sim \frac{\lambda^2\exp(\lambda)}{\exp(\lambda)-\lambda-1}, \quad \mathbb{E}\left[\frac{\boldsymbol{\Delta}}{|V_{\mathsf{s}}(\boldsymbol{A})|}\right] \sim \frac{\lambda(\exp(\lambda)-1)}{\exp(\lambda)-\lambda-1}, \quad \mathbb{E}\left[\frac{\boldsymbol{m}'_s}{|V_{\mathsf{s}}(\boldsymbol{A})|}\right] \sim \frac{\lambda^2}{2(\exp(\lambda)-\lambda-1)}.$$

Consequently, the expected number of nodes on cycles of length ℓ works out to be

$$\frac{1}{2\ell}\sum_{\boldsymbol{y},\boldsymbol{i},\boldsymbol{\alpha}} 2\ell\,\mathbb{P}\left[\mathscr{E}(\boldsymbol{y},\boldsymbol{i},\boldsymbol{\alpha}) \mid (d_x)_x, \boldsymbol{m}'_{\mathsf{s}}\right] \sim \left(\frac{\lambda^2\exp(\lambda)}{(\exp(\lambda)-1)^2}\right)^\ell = \exp(-\Omega(\ell)).$$

Summing on ℓ completes the proof. □

Proof of Lemma 8.7. The statement follows from Claims 8.10–8.12. □

8.5. **Proof of Lemma 8.8.** To simplify the notation we introduce $N = |\mathscr{V}_{\mathsf{s}}''|$, $M = |\mathscr{C}_{\mathsf{s}}''|$. Moreover, we write $d_1, \dots, d_N$ for the degrees of the variable nodes of $\mathscr{G}_{\mathsf{s}}''$ and $k_1, \dots, k_M \geq 3$ for the degrees of the constraints. We need the following facts about M, N and the degrees.

Claim 8.13. *W.h.p. we have*

$$M, N = \Omega(n), \qquad \max_{1 \leq i \leq N} d_i \leq \log^3 N, \qquad \max_{1 \leq i \leq M} k_i \leq \log^2 N, \qquad \sum_{i=1}^{M} k_i^2 = O(M), \qquad \sum_{i=1}^{N} d_i^2 = O(N). \tag{8.27}$$

Proof. The first estimate follows immediately from Proposition 2.6 and Lemma 8.7. The second statement follows from Lemma 8.7 (i) and the fact that the maximum degree of $G(\boldsymbol{A})$ is of order $\log n$ w.h.p., which also implies the third bound. Similarly, the sum of the squares of the check degrees of $G(\boldsymbol{A})$ is bounded w.h.p. due to routine bounds on the tails of the binomial distribution. This implies that $\sum_{i=1}^{M} k_i^2 = O(M)$ because $M = \Omega(n)$ w.h.p. by Proposition 2.6. To obtain the final bound we apply the Chernoff bound to conclude that for any $d > 0$ there exists $b > 0$ such that w.h.p.

$$\frac{1}{n} \sum_{i=1}^{n} \mathbf{1}\left\{|\partial_{G(\boldsymbol{A})} v_i| \geq t\right\} \leq \exp(-bt)/b. \tag{8.28}$$

In other words, the degree sequence of $G(\boldsymbol{A})$ has an exponentially decaying tail w.h.p. Assuming $N = \Omega(n)$, we see that (8.28) implies the bound

$$\frac{1}{N} \sum_{i=1}^{N} \mathbf{1}\{d_i \geq t\} \leq \exp(-b't)/b' \tag{8.29}$$

for some $b' > 0$. Furthermore, Lemma 8.7 (iii) implies an exponentially decaying tail for the component sizes of $\mathscr{G}_{\mathsf{s}}'$. Since $\mathscr{G}_{\mathsf{s}}''$ is obtained by contracting the components of $\mathscr{G}_{\mathsf{s}}'$, the desired bounds follow from (8.29) and Lemma 2.18. □

In the following we will condition on the event $\mathscr{D}$ that the conditions (8.27) are satisfied. Let $\boldsymbol{\sigma} \in \mathbb{F}_2^N$ be a uniformly random vector. We will prove Lemma 8.8 by estimating the probability that $\boldsymbol{\sigma} \in \mathscr{K}_\varepsilon''$. To this end, let

$$\boldsymbol{W} = \frac{\sum_{i=1}^{N} d_i \mathbf{1}\{\boldsymbol{\sigma}_i = 1\}}{\sum_{i=1}^{N} d_i}$$

count the degree-weighted one-entries of $\boldsymbol{\sigma}$. The following claim bounds the probability that $\boldsymbol{W}$ deviates significantly from 1/2.

Claim 8.14. *For any $d >$ e there is $s = s(d) > 0$ such that $\mathbb{P}[|\boldsymbol{W} - 1/2| \geq t \mid \mathscr{D}] \leq 2\exp(-st^2 N)$.*

Proof. This is an immediate consequence of (8.27) and Azuma's inequality. □

As a next step we calculate the probability that $\boldsymbol{\sigma} \in \ker \mathscr{A}_{\mathsf{s}}''$ given $\boldsymbol{W}$.

Claim 8.15. *For any $d >$ e there exist $\varepsilon > 0, \gamma > 0$ such that uniformly for every $w \in (1/2 - \varepsilon, 1/2 + \varepsilon)$ for which $w \sum_{i=1}^{M} k_i$ is an even integer we have*

$$\log \mathbb{P}\left[\mathscr{A}_{\mathsf{s}}'' \boldsymbol{\sigma} = 0 \mid \boldsymbol{W} = w, \mathscr{D}\right] \leq -M \log 2 - \gamma M (w - 1/2)^3 + O(1).$$

Proof. Consider a random vector $\boldsymbol{\xi} = (\boldsymbol{\xi}_{ij})_{i \in [M], j \in [k_i]}$ where we choose every entry $\boldsymbol{\xi}_{ij} \in \mathbb{F}_2$ to be a one with probability w independently. Let $\mathscr{S}$ be the event that $\sum_{j \in [k_i]} \boldsymbol{\xi}_{ij} = 0$ for all $i \in [M]$. Moreover, let

$$\mathscr{R} = \left\{ \sum_{i=1}^{M} \sum_{j=1}^{k_i} \left(\mathbf{1}\{\boldsymbol{\xi}_{i,j} = 1\} - w \right) = 0 \right\}.$$

Because $\mathscr{G}_{\mathsf{s}}''$ is drawn from the pairing model, we have

$$\mathbb{P}\left[\mathscr{A}_{\mathsf{s}}'' \boldsymbol{\sigma} = 0 \mid \boldsymbol{W} = w, \mathscr{D}\right] = \mathbb{P}\left[\mathscr{S} \mid \mathscr{R}\right]. \tag{8.30}$$

We will calculate the probability on the r.h.s. of (8.30) via Bayes' rule. The unconditional probabilities are computed easily. Indeed, for every $i \in [M]$ we have

$$\mathbb{P}\left[\sum_{j\in[k_i]} \boldsymbol{\xi}_{ij} = 0\right] = \sum_{j=0}^{k} \mathbf{1}\{j \text{ even}\}\binom{k}{j} w^j (1-w)^{k-j}$$
$$= \frac{1}{2}\left[\sum_{j=0}^{k}\binom{k}{j} w^j(1-w)^{k-j} + \sum_{j=0}^{k}\binom{k}{j}(-w)^j(1-w)^{k-j}\right] = \frac{1+(1-2w)^k}{2}.$$

Hence,

$$\mathbb{P}[\mathscr{S}] = \prod_{i=1}^{M} \frac{1+(1-2w)^{k_i}}{2}. \tag{8.31}$$

Furthermore, the local limit theorem for the binomial distribution shows that

$$\mathbb{P}[\mathscr{R}] = \Theta(M^{-1/2}). \tag{8.32}$$

In addition, (8.27) and the local limit theorem for sums of independent random variables yield

$$\mathbb{P}[\mathscr{R} \mid \mathscr{S}] = \Theta(M^{-1/2}). \tag{8.33}$$

Combining (8.31)–(8.33) and recalling that the $\boldsymbol{\xi}_{ij}$ are independent, we obtain

$$\log \mathbb{P}[\mathscr{S} \mid \mathscr{R}] = \sum_{i=1}^{M} \log \frac{1+(1-2w)^{k_i}}{2} + O(1) = -M\log 2 + \sum_{i=1}^{M} \log(1+(1-2w)^{k_i}) + O(1). \tag{8.34}$$

To complete the proof we compute the derivatives of the last expression, keeping in mind that $k_i \geq 3$ for all i:

$$\frac{\partial \log \mathbb{P}[\mathscr{S} \mid \mathscr{R}]}{\partial w} = \sum_{i=1}^{M} \frac{-2k_i(1-2w)^{k_i-1}}{1+(1-2w)^{k_i}},$$
$$\frac{\partial^2 \log \mathbb{P}[\mathscr{S} \mid \mathscr{R}]}{\partial w^2} = \sum_{i=1}^{M} \frac{4k_i(k_i-1)(1-2w)^{k_i-2}}{1+(1-2w)^{k_i}} - \frac{4k_i^2(1-2w)^{2k_i-2}}{\left(1+(1-2w)^{k_i}\right)^2},$$
$$\frac{\partial^3 \log \mathbb{P}[\mathscr{S} \mid \mathscr{R}]}{\partial w^3} = \sum_{i=1}^{M} \frac{-8k_i(k_i-1)(k_i-2)(1-2w)^{k_i-3}}{1+(1-2w)^{k_i}} + \frac{8k_i^2(k_i-1)(1-2w)^{k_i-2}(1-2w)^{k_i-1}}{\left(1+(1-2w)^{k_i}\right)^2}$$
$$+ \frac{16k_i^2(k_i-1)(1-2w)^{2k_i-3}}{\left(1+(1-2w)^{k_i}\right)^2} - \frac{16k_i^3(1-2w)^{3k_i-2}}{\left(1+(1-2w)^{k_i}\right)^3}.$$

Evaluating these derivatives at $w = 1/2$, we obtain

$$\frac{\partial \log \mathbb{P}[\mathscr{S} \mid \mathscr{R}]}{\partial w}\Big|_{w=1/2} = \frac{\partial^2 \log \mathbb{P}[\mathscr{S} \mid \mathscr{R}]}{\partial w^2}\Big|_{w=1/2} = 0, \qquad \frac{\partial^3 \log \mathbb{P}[\mathscr{S} \mid \mathscr{R}]}{\partial w^3} = -48\sum_{i=1}^{M} \mathbf{1}\{k_i = 3\}. \tag{8.35}$$

Finally, combining (8.30), (8.34) and (8.35) with Taylor's formula completes the proof. □

Proof of Lemma 8.8. Choose $\varepsilon = \varepsilon(d) > 0$ small enough. Summing over $w \in (1/2-\varepsilon, 1/2+\varepsilon)$ such that $w\sum_{i=1}^{N} d_i$ is an even integer, we obtain

$$\mathbb{P}\big[\mathscr{K}_\varepsilon \neq \emptyset \mid \mathscr{D}, M \geq N+\omega\big] \leq 2^N \mathbb{P}\left[\mathscr{A}_{\mathsf{s}}''\boldsymbol{\sigma} = 0, |\boldsymbol{W}-1/2| < \varepsilon \mid \mathscr{D}, M \geq N+\omega\right]$$
$$\leq 2^N \sum_{w} \mathbb{P}\big[\boldsymbol{W} = w \mid \mathscr{D}, M \geq N+\omega\big]\mathbb{P}\left[\mathscr{A}_{\mathsf{s}}''\boldsymbol{\sigma} = 0 \mid \boldsymbol{W} = w, \mathscr{D}, M \geq N+\omega\right].$$

Combining this bound with Claims 8.14 and 8.15, we obtain

$$\mathbb{P}\big[\mathscr{K}_\varepsilon \neq \emptyset \mid \mathscr{D}, M \geq N+\omega\big] \leq 2^N \sum_{h=1}^{\lceil \varepsilon\sqrt{N}\rceil} \sum_{w: h-1 \leq w\sqrt{N} \leq h} \mathbb{P}\big[\boldsymbol{W} = w \mid \mathscr{D}, M \geq N+\omega\big]\mathbb{P}\left[\mathscr{A}_{\mathsf{s}}''\boldsymbol{\sigma} = 0 \mid \boldsymbol{W} = w, \mathscr{D}, M \geq N+\omega\right]$$
$$\leq 2^{N-M} \sum_{1 \leq h \leq \varepsilon\sqrt{n}} \exp\Big(-\Omega\big(h^2\big) + O\big(h^3 M N^{-3/2}\big)\Big) = O\big(2^{N-M}\big) = o(1),$$

provided that $M \geq N+\omega$ and $\varepsilon > 0$ is small enough. □

8.6. **Proof of Lemma 8.9.** The following observation is an easy consequence of the construction of $\boldsymbol{A}_{\mathtt{s}}$.

Claim 8.16. *If $v, y \in V(\boldsymbol{A}_{\mathtt{s}})$ are variables such that $\xi_v = \xi_y$ for all $\xi \in \ker \boldsymbol{A}_{\mathtt{s}}$, then $\xi_v = \xi_y$ for all $\xi \in \ker \boldsymbol{A}$.*

Proof. By construction the matrix $\boldsymbol{A}_{\mathtt{s}}$ is the minor of $\boldsymbol{A}$ induced on $V_{\mathtt{s}}(\boldsymbol{A}) \times C_{\mathtt{s}}(\boldsymbol{A})$. Although some of the checks $a \in C_{\mathtt{s}}(\boldsymbol{A})$ may contain variables $v \notin V_{\mathtt{s}}(\boldsymbol{A})$, all such v are frozen in $\boldsymbol{A}$. Therefore, any $\xi \in \ker \boldsymbol{A}$ induces a vector $\xi_{\mathtt{s}} \in \ker \boldsymbol{A}_{\mathtt{s}}$. □

We now combine Claim 8.16 with Proposition 2.11 to prove the lemma. Hence, let $\mathscr{U}$ be the event that $|V_{\mathtt{s}}(\boldsymbol{A}) \setminus \mathscr{F}(\boldsymbol{A})| > (1-\delta)|V_{\mathtt{s}}(\boldsymbol{A})|$. Provided that $\delta = \delta(d,\varepsilon) > 0$ is chosen small enough, routine tail bounds for the binomial distribution imply that the event

$$\mathscr{E} = \left\{ \sum_{v \in V_{\mathtt{s}}(\boldsymbol{A}) \cap \mathscr{F}(\boldsymbol{A})} d_{\mathtt{s}}(v) < \frac{\varepsilon}{4} \sum_{v \in V_{\mathtt{s}}(\boldsymbol{A})} d_{\mathtt{s}}(v) \right\} \quad \text{satisfies} \quad \mathbb{P}[\mathscr{U} \setminus \mathscr{E}] = o(1). \tag{8.36}$$

Further, with $\boldsymbol{x}_{\mathtt{s}} = (\boldsymbol{x}_{\mathtt{s},y})_{y \in V_{\mathtt{s}}(\boldsymbol{A})} \in \ker \boldsymbol{A}_{\mathtt{s}}$ chosen randomly, Proposition 2.11 and Claim 8.16 ensure that the event

$$\left\{ \sum_{y,y' \in V_{\mathtt{s}}(\boldsymbol{A}) \setminus \mathscr{F}(\boldsymbol{A})} \left| \mathbb{P}\left[\boldsymbol{x}_{\mathtt{s},y} = \boldsymbol{x}_{\mathtt{s},y'} = 0 \mid \boldsymbol{A}\right] - \frac{1}{4} \right| < |V_{\mathtt{s}}(\boldsymbol{A})| \log^{-9} n \right\}$$

has probability $1 - o(1)$. As a consequence, since all degrees of $G_{\mathtt{s}}(\boldsymbol{A})$ are bounded by $\log n$ w.h.p., the event

$$\mathscr{R} = \left\{ \sum_{y,y' \in V_{\mathtt{s}}(\boldsymbol{A}) \setminus \mathscr{F}(\boldsymbol{A})} d_{\mathtt{s}}(y) d_{\mathtt{s}}(y') \left| \mathbb{P}\left[\boldsymbol{x}_{\mathtt{s},y} = \boldsymbol{x}_{\mathtt{s},y'} = 0 \mid \boldsymbol{A}\right] - \frac{1}{4} \right| < \left(\sum_{y \in V_{\mathtt{s}}(\boldsymbol{A})} d_{\mathtt{s}}(y) \right)^2 \log^{-4} n \right\}$$

satisfies $\mathbb{P}[\mathscr{R}] = 1 - o(1)$. Hence, (8.36) yields $\mathbb{P}[\mathscr{U} \setminus (\mathscr{E} \cap \mathscr{R})] = o(1)$. In effect, it suffices to prove that on the event $\mathscr{U} \cap \mathscr{E} \cap \mathscr{R}$ we have $\mathscr{K}_\varepsilon \neq \emptyset$.

To verify this we recall that any variables y, y' that get contracted in the course of the construction of $G''_{\mathtt{s}}(\boldsymbol{A})$ deterministically satisfy $\boldsymbol{x}_{\mathtt{s},y} = \boldsymbol{x}_{\mathtt{s},y'}$. As a consequence, for a random $\boldsymbol{x}''_{\mathtt{s}} \in \ker \boldsymbol{A}''_{\mathtt{s}}$ we have

$$\sum_{y,y' \in V''_{\mathtt{s}}(\boldsymbol{A}) \setminus \mathscr{F}(\boldsymbol{A}''_{\mathtt{s}})} d''_{\mathtt{s}}(y) d''_{\mathtt{s}}(y') \left| \mathbb{P}\left[\boldsymbol{x}''_{\mathtt{s},y} = \boldsymbol{x}''_{\mathtt{s},y'} = 0 \mid \boldsymbol{A}\right] - \frac{1}{4} \right| = \sum_{y,y' \in V_{\mathtt{s}}(\boldsymbol{A}) \setminus \mathscr{F}(\boldsymbol{A})} d_{\mathtt{s}}(y) d_{\mathtt{s}}(y') \left| \mathbb{P}\left[\boldsymbol{x}_{\mathtt{s},y} = \boldsymbol{x}_{\mathtt{s},y'} = 0 \mid \boldsymbol{A}\right] - \frac{1}{4} \right|.$$

Therefore, if $\mathscr{U} \cap \mathscr{E} \cap \mathscr{R}$ occurs, then so does the event

$$\mathscr{S} = \left\{ \sum_{y,y' \in V''_{\mathtt{s}}(\boldsymbol{A}) \setminus \mathscr{F}(\boldsymbol{A}''_{\mathtt{s}})} d''_{\mathtt{s}}(y) d''_{\mathtt{s}}(y') \left| \mathbb{P}\left[\boldsymbol{x}''_{\mathtt{s},y} = \boldsymbol{x}''_{\mathtt{s},y'} = 0 \mid \boldsymbol{A}\right] - \frac{1}{4} \right| < \left(\sum_{y \in V''_{\mathtt{s}}(\boldsymbol{A}) \setminus \mathscr{F}(\boldsymbol{A}''_{\mathtt{s}})} d''_{\mathtt{s}}(y) \right)^2 \log^{-3} n \right\}.$$

To complete the proof, consider the random variable

$$\boldsymbol{X} = \frac{\sum_{y \in V''_{\mathtt{s}}(\boldsymbol{A}) \setminus \mathscr{F}(\boldsymbol{A}''_{\mathtt{s}})} d''_{\mathtt{s}}(y) \mathbf{1}\left\{\boldsymbol{x}''_{\mathtt{s},y} = 0\right\}}{\sum_{y \in V''_{\mathtt{s}}(\boldsymbol{A}) \setminus \mathscr{F}(\boldsymbol{A}''_{\mathtt{s}})} d''_{\mathtt{s}}(y)}.$$

Then on $\mathscr{U} \cap \mathscr{E} \cap \mathscr{R}$ we have $\mathbb{E}[\boldsymbol{X} \mid \boldsymbol{A}] \sim 1/2$ because $\boldsymbol{x}''_{\mathtt{s},y} = 0$ with probability $1/2$ for every $y \in V''_{\mathtt{s}}(\boldsymbol{A}) \setminus \mathscr{F}(\boldsymbol{A}''_{\mathtt{s}})$. Moreover, because $\mathscr{U} \cap \mathscr{E} \cap \mathscr{R} \subseteq \mathscr{S}$ the conditional second moment works out to be $\mathbb{E}[\boldsymbol{X}^2 \mid \boldsymbol{A}] \sim 1/4$. Hence, Chebyshev's inequality shows that $\mathbb{P}[|\boldsymbol{X} - 1/2| < \varepsilon/4 \mid \boldsymbol{A}] = 1 - o(1)$. In particular, on $\mathscr{U} \cap \mathscr{E} \cap \mathscr{R}$ there exists a vector $\xi \in \ker \boldsymbol{A}''_{\mathtt{s}}$ such that

$$\left| \frac{\sum_{y \in V''_{\mathtt{s}}(\boldsymbol{A}) \setminus \mathscr{F}(\boldsymbol{A}''_{\mathtt{s}})} d''_{\mathtt{s}}(y) \mathbf{1}\left\{\xi''_y = 0\right\}}{\sum_{y \in V''_{\mathtt{s}}(\boldsymbol{A}) \setminus \mathscr{F}(\boldsymbol{A}''_{\mathtt{s}})} d''_{\mathtt{s}}(y)} - \frac{1}{2} \right| < \frac{\varepsilon}{4}.$$

Recalling the definition of the event (8.36), we conclude that $\xi \in \mathscr{K}_\varepsilon$ and thus $\mathscr{K}_\varepsilon \neq \emptyset$.

Acknowledgment. We are grateful to Jane Gao for a helpful conversation at the beginning of this project that brought the two-peaked nature of the function Φ_d to our attention.

REFERENCES

[1] D. Achlioptas, A. Coja-Oghlan: Algorithmic barriers from phase transitions. Proc. 49th FOCS (2008) 793–802.

[2] D. Achlioptas, M. Molloy: The solution space geometry of random linear equations. Random Structures and Algorithms **46** (2015) 197–231.

[3] P. Ayre, A. Coja-Oghlan, P. Gao, N. Müller: The satisfiability threshold for random linear equations. Combinatorica, in press.

[4] A. Bandyopadhyay, D. Gamarnik: Counting without sampling: asymptotics of the log-partition function for certain statistical physics models. Random Structures and Algorithms **33** (2008) 452–479.

[5] V. Bapst, A. Coja-Oghlan: Harnessing the Bethe free energy. Random Structures and Algorithms **49** (2016) 694–741.

[6] J. Barbier, D. Panchenko: Strong replica symmetry in high-dimensional optimal Bayesian inference. arXiv:2005.03115 (2020).

[7] B. Bollobás: Random graphs. Cambridge University Press (2001).

[8] C. Bordenave, M. Lelarge, J. Salez: The rank of diluted random graphs. Ann. Probab. **39** (2011) 1097–1121.

[9] C. Bordenave, M. Lelarge, J. Salez: Matchings on infinite graphs. Probability Theory and Related Fields **157** (2013) 183–208.

[10] S. Cocco, O. Dubois, J. Mandler, R. Monasson: Rigorous decimation-based construction of ground pure states for spin glass models on random lattices. Phys. Rev. Lett. **90** (2003) 047205.

[11] A. Coja-Oghlan, O. Cooley, M. Kang, J. Lee, J. B. Ravelomanana: Warning Propagation on random graphs. arXiv:2102.00970.

[12] A. Coja-Oghlan, O. Cooley, M. Kang, K. Skubch: How does the core sit inside the mantle? Random Structures and Algorithms **51** (2017) 459–482.

[13] A. Coja-Oghlan, O. Cooley, M. Kang, K. Skubch: Core forging and local limit theorems for the k-core of random graphs. Journal of Combinatorial Theory, Series B **137** (2019) 178–231.

[14] A. Coja-Oghlan, W. Perkins, K. Skubch: Limits of discrete distributions and Gibbs measures on random graphs. European Journal of Combinatorics **66** (2017) 37–59.

[15] A. Coja-Oghlan, A. Ergür, P. Gao, S. Hetterich, M. Rolvien: The rank of sparse random matrices. Proc. 31st SODA (2020) 579–591.

[16] A.Coja-Oghlan, M. Hahn-Klimroth: The cut metric for probability distributions. SIAM J. on Discrete Mathematics, in press.

[17] A. Coja-Oghlan, F. Krzakala, W. Perkins, L. Zdeborová: Information-theoretic thresholds from the cavity method. Advances in Mathematics **333** (2018) 694–795.

[18] A. Coja-Oghlan, W. Perkins: Belief Propagation on replica symmetric random factor graph models. Annales de l'institut Henri Poincare D **5** (2018) 211–249.

[19] A. Coja-Oghlan, W. Perkins: Spin systems on Bethe lattices. Communications in Mathematical Physics **372** (2019) 441–523.

[20] H. Connamacher, M. Molloy: The satisfiability threshold for a seemingly intractable random constraint satisfaction problem. SIAM J. Discret. Math. **26** (2012) 768–800.

[21] O. Cooley, J. Lee, J. B. Ravelomanana: Warning Propagation: stability and subcriticality. arXiv:2111.15577.

[22] C. Cooper, A. Frieze, W. Pegden: On the rank of a random binary matrix. Electronic Journal of Combinatorics **26** (2019) #P4.12. .

[23] M. Dietzfelbinger, A. Goerdt, M. Mitzenmacher, A. Montanari, R. Pagh, M. Rink: Tight thresholds for cuckoo hashing via XORSAT. Proc. 37th ICALP (2010) 213–225.

[24] J. Ding, A. Sly, N. Sun: Proof of the satisfiability conjecture for large k. Proc. 47th STOC (2015) 59–68.

[25] O. Dubois, J. Mandler: The 3-XORSAT threshold. Proc. 43rd FOCS (2002) 769–778.

[26] P. Erdős, A. Rényi: On the evolution of random graphs. Magayar Tud. Akad. Mat. Kutato Int. Kozl. **5** (1960) 17–61.

[27] E. Friedgut: Sharp thresholds of graph properties, and the k-SAT problem. J. AMS **12** (1999) 1017–1054.

[28] J. Huang: Invertibility of adjacency matrices for random d-regular graphs. arXiv:1807.06465.

[29] M. Ibrahimi, Y. Kanoria, M. Kraning, A. Montanari: The set of solutions of random XORSAT formulae. Annals of Applied Probability **25** (2015) 2743–2808.

[30] V. Kolchin: Consistency of a system of random congruences. Discrete Math. Appl. **3** (1993) 103–113.

[31] V. Kolchin: Random graphs and systems of linear equations in finite fields. Random Structures and Algorithms **5** (1995) 425–436.

[32] J. Komlós and E. Szemerédi: Limit distributions for the existence of Hamilton circuits in a random graph. Discrete Mathematics **43** (1983) 55–63.

[33] F. Krzakala, A. Montanari, F. Ricci-Tersenghi, G. Semerjian, L. Zdeborová: Gibbs states and the set of solutions of random constraint satisfaction problems. Proc. National Academy of Sciences **104** (2007) 10318–10323.

[34] M. Mézard, A. Montanari: Information, physics and computation. Oxford University Press 2009.

[35] M. Mézard, F. Ricci-Tersenghi, R. Zecchina: Two solutions to diluted p-spin models and XORSAT problems. Journal of Statistical Physics **111** (2003) 505–533.

[36] G. Miller, G. Cohen: The rate of regular LDPC codes. IEEE Transactions on Information Theory **49** (2003) 2989–2992.

[37] M. Molloy: The freezing threshold for k-colourings of a random graph. J. ACM **65** (2018) #7

[38] M. Molloy, B. Reed: A critical point for random graphs with a given degree sequence. Random Structures and Algorithms **6** (1995) 161–179.

[39] M. Molloy, R. Restrepo: Frozen variables in random boolean constraint satisfaction problems. Proc. 24th SODA (2013) 1306–1318.

[40] A. Montanari: Estimating random variables from random sparse observations. European Transactions on Telecommunications **19**(4) (2008) 385–403.

[41] B. Pittel, J. Spencer, N. Wormald: Sudden emergence of a giant k-core in a random graph. J. Combin. Theory Ser. B, 67 (1996) 111–151.

[42] B. Pittel, G. Sorkin: The satisfiability threshold for k-XORSAT. Combinatorics, Probability and Computing **25** (2016) 236–268.

[43] M. Wainwright, E. Maneva, E. Martinian: Lossy source compression using low-density generator matrix codes: analysis and algorithms. IEEE Transactions on Information theory **56** (2010) 1351–1368.

[44] L. Zdeborová, F. Krzakala: Statistical physics of inference: thresholds and algorithms. Advances in Physics **65** (2016) 453–552.

Appendix A. The pinning operation and the overlap

A.1. **Proof of Proposition 2.11.** Let A be an $m \times n$-matrix over $\mathbb{F}_2$ and let $\boldsymbol{s}_1, \boldsymbol{s}_2, \ldots \in [n]$ be a sequence of uniformly distributed random variables, mutually independent and independent of all other sources of randomness. Further, for an integer $t \geq 0$ let $A[t]$ be the matrix obtained by adding t more rows to A such that the j-th new row contains precisely one non-zero entry in position $\boldsymbol{s}_j$. The proof of Proposition 2.11 is based on the following fact.

Lemma A.1 ([15, Lemma 3.1])**.** *For $\varepsilon > 0, \ell > 0$ let $T = T(\varepsilon, \ell) = \lceil 4\ell^3/\varepsilon^4 \rceil + 1$. Then for all $m, n > 0$ and all $m \times n$-matrices A over $\mathbb{F}_2$ the following is true. Draw $\boldsymbol{t} \in [T]$ uniformly and choose $\boldsymbol{x} \in \ker A[\boldsymbol{t}]$ randomly. Then*

$$\sum_{\substack{i_1,\ldots,i_\ell \in [n] \\ \sigma \in \mathbb{F}_2^\ell}} \mathbb{E}\left| \mathbb{P}\left[\boldsymbol{x}_{i_1} = \sigma_1, \ldots, \boldsymbol{x}_{i_\ell} = \sigma_\ell \mid A[\boldsymbol{t}]\right] - \prod_{h=1}^{\ell} \mathbb{P}\left[\boldsymbol{x}_{i_h} = \sigma_h \mid A[\boldsymbol{t}]\right] \right| < \varepsilon n^\ell.$$

To prove Proposition 2.11 we will combine Lemma A.1 with the observation that the random matrix $\boldsymbol{A}$ is essentially invariant under the random perturbation required by Lemma A.1. To be precise, let $\mathcal{Z}$ be the set of all indices $i \in [n]$ such that $\boldsymbol{A}_{ij} = 0$ for all $j \in [n]$. Further, for an integer $t \geq 0$ let $\boldsymbol{A}\langle t \rangle$ be the matrix obtained from $\boldsymbol{A}$ as follows. If $|\mathcal{Z}| \leq t$, then $\boldsymbol{A}\langle t \rangle = \boldsymbol{A}$. Otherwise draw a family $\boldsymbol{z}_1, \ldots, \boldsymbol{z}_t \in \mathcal{Z}$ of t distinct row indices uniformly at random and obtain $\boldsymbol{A}\langle t \rangle$ from $\boldsymbol{A}$ by replacing the $\boldsymbol{i}_h$-th entry in row $\boldsymbol{z}_h$ by one for $h = 1, \ldots, t$, where $\boldsymbol{i}_h$ is chosen uniformly at random from $[n]$ independently for each $h \in [t]$. Thus, instead of attaching t new rows as in Lemma A.1 we simply insert a single non-zero entry into t random all-zero rows of $\boldsymbol{A}$.

Lemma A.2. *Let $d > 0$, let $T = o(\sqrt{n})$ be an integer and choose $\boldsymbol{t} \in [T]$ uniformly. Then $d_{\mathrm{TV}}(\boldsymbol{A}, \boldsymbol{A}\langle \boldsymbol{t} \rangle) = o(1)$.*

Proof. Because each entry of $\boldsymbol{A}$ is non-zero with probability d/n independently, the number $\boldsymbol{X}$ of rows of $\boldsymbol{A}$ with at most one non-zero entry has distribution $\mathrm{Bin}(n, (1-d/n)^n + d(1-d/n)^{n-1})$. Further, given $\boldsymbol{X}$ the number $\boldsymbol{X}_0$ of all-zero rows has a binomial distribution

$$\boldsymbol{X}_0 \sim \mathrm{Bin}\left(\boldsymbol{X}, \frac{(1-d/n)^n}{(1-d/n)^n + d(1-d/n)^{n-1}}\right).$$

Let $\boldsymbol{A} \mid (\boldsymbol{X}, \boldsymbol{X}_0)$ denote the distribution of $\boldsymbol{A}$ given $\boldsymbol{X}, \boldsymbol{X}_0$. We have $\boldsymbol{X} \geq \exp(-d)n$ w.h.p. Given $\boldsymbol{X} \geq \exp(-d)n$ the conditional variance satisfies $\mathrm{Var}[\boldsymbol{X}_0 \mid \boldsymbol{X}] = \Omega(n)$. Therefore, the local limit theorem for the binomial distribution implies that $\boldsymbol{A} \mid (\boldsymbol{X}, \boldsymbol{X}_0)$ and $\boldsymbol{A} \mid (\boldsymbol{X}, \boldsymbol{X}_0 - \boldsymbol{t})$ have total variation distance $o(1)$. Furthermore, $\boldsymbol{A} \mid (\boldsymbol{X}, \boldsymbol{X}_0 - \boldsymbol{t})$ is distributed precisely as $\boldsymbol{A}\langle \boldsymbol{t} \rangle$. □

Proof of Proposition 2.11. The proposition is an immediate consequence of Lemmas A.1 and A.2. □

A.2. **Proof of Corollary 2.12.** Due to Proposition 2.11 we may assume that $\boldsymbol{A}$ satisfies

$$\frac{1}{n^2} \sum_{h,i=1}^{n} \left| \mathbb{P}\left[\boldsymbol{x}_h = \sigma_1, \boldsymbol{x}_i = \sigma_2 \mid \boldsymbol{A}\right] - \mathbb{P}\left[\boldsymbol{x}_h = \sigma_1 \mid \boldsymbol{A}\right] \mathbb{P}\left[\boldsymbol{x}_i = \sigma_2 \mid \boldsymbol{A}\right] \right| = o(1) \qquad \text{for all } \sigma_1, \sigma_2 \in \mathbb{F}_2. \tag{A.1}$$

Hence, fix $x \in \ker \boldsymbol{A}$. For $\sigma \in \mathbb{F}_2$ let $\mathscr{I}(x, \sigma) = \{i \in [n] \setminus \mathscr{F}(\boldsymbol{A}) : x_i = \sigma\}$. Further, define

$$R_\sigma(x, x') = \frac{1}{n} \sum_{i \in \mathscr{I}(x,\sigma)} \mathbf{1}\left\{x'_i = \sigma\right\}.$$

Then Fact 2.17 implies that

$$\mathbb{E}\left[R_\sigma(x, \boldsymbol{x}') \mid \boldsymbol{A}\right] = \frac{|\mathscr{I}(x, \sigma)|}{2n}. \tag{A.2}$$

Moreover, (A.1) implies that $\mathrm{Var}\left[R_\sigma(x, \boldsymbol{x}') \mid \boldsymbol{A}\right] = o(1)$. Combining this bound with (A.2) and applying Chebyshev's inequality, we conclude that

$$\mathbb{E}\left[\left| R_\sigma(x, \boldsymbol{x}') - \frac{|\mathscr{I}(x, \sigma)|}{2n} \right| \mid \boldsymbol{A}\right] = o(1). \tag{A.3}$$

Further, since $R(x, \boldsymbol{x}') = f(\boldsymbol{A}) + \sum_{\sigma \in \mathbb{F}_2} R_\sigma(x, \boldsymbol{x}')$, (A.3) shows that

$$\mathbb{E}\left[\left| R(x, \boldsymbol{x}') - \left(f(\boldsymbol{A}) + (1 - f(\boldsymbol{A}))/2\right) \right| \mid \boldsymbol{A}\right] = o(1) \qquad \text{for every } x \in \ker \boldsymbol{A}. \tag{A.4}$$

Averaging (A.4) on $x \in \ker \boldsymbol{A}$ completes the proof.

Appendix B. Proof of Lemma 2.13

We first note that since in the pairing model we must connect variable nodes with check nodes, certainly $\mathscr{G}_{\mathtt{s}}$ cannot contain any loops. We therefore need to show that there is at least a constant probability of creating no double-edges.

Suppose that $d_1,\dots,d_n$ are the degrees of variable nodes in $G_{\mathtt{s}}(\boldsymbol{A})$ (where we set $d_i=0$ if the corresponding node is not in $G_{\mathtt{s}}(\boldsymbol{A})$), and similarly let $\hat{d}_1,\dots,\hat{d}_n$ be the degrees of check nodes. Let $m:=\sum_{i=1}^n d_i=\sum_{i=1}^n \hat{d}_i$. It follows from Proposition 2.6 that w.h.p. $m=\Theta(n)$. It also follows from the fact that the degree of a node in $G_{\mathtt{s}}(\boldsymbol{A})$ are necessarily at most its degree in $G(\boldsymbol{A})$ that w.h.p. $\sum_{i=1}^n d_i^2,\sum_{i=1}^n \hat{d}_i^2=O(n)$. In what follows, we will implicitly condition on these high probability events.

Let $X=X(d_1,\dots,d_n,\hat{d}_1,\dots,\hat{d}_n)$ be the random variable counting the number of double-edges in $\mathscr{G}_{\mathtt{s}}$. Then we have

$$\mathbb{E}[X]=\sum_{i=1}^n\sum_{j=1}^n 2\binom{d_i}{2}\binom{\hat{d}_j}{2}\frac{1}{m(m-1)}=O(1).$$

Similarly, it is an easy exercise to show that for any integer $\ell\in\mathbb{N}$ the ℓ-th moment of X satisfies $\mathbb{E}[(X)_\ell]=(1+o(1))\mathbb{E}[X]^\ell$. Therefore X is asymptotically distributed as a $\mathrm{Po}(\mathbb{E}[X])$ random variable, and we have $\mathbb{P}[X=0]\to\exp(-\mathbb{E}[X])>0$, as required.

To show that $\mathscr{G}_{\mathtt{s}}$ conditioned on being simple has the same distribution as $G_{\mathtt{s}}(\boldsymbol{A})$, we simply need to observe that every simple bipartite graph with the appropriate distribution is equally likely to be $G_{\mathtt{s}}(\boldsymbol{A})$. To see this, consider two Tanner graphs S,S' with the same degree distribution, and a Tanner graph H such that $H_{\mathtt{s}}=S$. Let H' be the Tanner graph obtained from H by replacing S with S', but otherwise leaving edges unchanged. Then the peeling process used to obtain the slush is completely identical on $H\setminus S$ and $H'\setminus S'$, and therefore $H'_{\mathtt{s}}=S'$. Since H,H' have the same number of edges, both are equally likely to be $G(\boldsymbol{A})$. Summing over all possibilities for H such that $H_{\mathtt{s}}=S$, we deduce that S,S' are equally likely to be $G_{\mathtt{s}}(\boldsymbol{A})$.

Appendix C. Proof of Lemma 2.14

For the first part of the lemma, notice that $|\partial v|$ is distributed as a binomial random variable with parameter n and p for any $v\in V(\boldsymbol{A})\cup C(\boldsymbol{A})$. Suppose $v\in V(\boldsymbol{A})$ and let $c=\lceil\log(n)/2\rceil$. Then we have

$$\begin{aligned}\mathbb{P}\left[\exists v:|\partial v|\geq c\right]&\leq n\binom{n}{c}p^c\leq n\binom{n}{c}\left(\frac{d}{n}\right)^c\\&\leq n\left(\frac{ed}{c}\right)^c=\exp\left[\left(1-\frac{\log 2}{2}\right)\log n-\frac{\log(n)}{2}\cdot\big(\log\log(n)\big)+O(\log\log n)\right]=o(1).\end{aligned}\tag{C.1}$$

Similarly, for a constraint $a\in C(\boldsymbol{A})$ we have

$$\mathbb{P}\left[\exists a:|\partial a|\geq c\right]=o(1).\tag{C.2}$$

Combining (C.1) and (C.2) completes the proof of the first part. For the second part, let x_0 be an arbitrary variable node. Then,

$$\mathbb{E}\left[\sum_{x\in V(\boldsymbol{A})}\frac{1}{\ell!}\prod_{j=1}^{\ell}(|\partial x|-j+1)\right]=\frac{n}{\ell!}\mathbb{E}\left[\prod_{j=1}^{\ell}(|\partial x_0|-j+1)\right]=\frac{n}{\ell!}\frac{n!}{(n-\ell)!}p^\ell\leq\frac{d^\ell n}{\ell!}.$$

Hence, the assertion follows from Markov's inequality.

Appendix D. Proof of Lemma 2.18

Assume, without loss of generality, that $0<c_1<10^{-5}$. Moreover, let $c_0>0$, define $a=\exp(c_1)>1$ and $\log_a^{(m)}n:=\log_a\ldots\log_a n$, where the logarithm with basis a is taken m times. For any $m\in\mathbb{N}$ (or more precisely for any m such that we have $s_m>0$), define

$$s_m:=6\log_a^{(m)}n.$$

Let us set $q_j:=\max\{w_i:i\in P_j\}$, and define the event

$$\mathscr{E}_{j,m}:=\{s_{m+1}<\max\{q_j,|P_j|\}\leq s_m\}$$

and the set

$$E_m:=\{j:\mathscr{E}_{j,m}\text{ holds}\}.$$

Note in particular that $\bigcup_{m' \geq m} \mathscr{E}_{j,m'}$ is the event that $|P_j| \leq s_m$ and $w_i \leq s_m$ for all $i \in P_j$, i.e. both the partition class and all associated weights are at most s_m. We also observe that $\bigcup_{m=1}^{\infty} E_m = [\ell]$. We further define

$$x_m := \frac{1}{n} \sum_{j \in E_m} \left(\sum_{i \in P_j} w_i \right)^2,$$

so in particular we have

$$x = \sum_{m=1}^{\infty} x_m. \tag{D.1}$$

We therefore aim to bound each x_m. Let $m_0 = m_0(n)$ be the largest integer such that $s_{m_0} \geq \frac{100 \log(1/c_1)}{c_1}$.

We first consider the case when $m \leq m_0$. Observe that if $j \in E_m$, then we have $|P_j| \leq s_m$ and for all $i \in P_j$ we have $w_i \leq s_m$, and therefore

$$\left(\sum_{i \in P_j} w_i \right)^2 \leq s_m^4. \tag{D.2}$$

On the other hand, we can bound $|E_m|$ from above by making a case distinction. Let us define

$$E_m^{(1)} := \left\{ j : \mathscr{E}_{j,m} \text{ holds and } q_j \geq |P_j| \right\},$$
$$E_m^{(2)} := \left\{ j : \mathscr{E}_{j,m} \text{ holds and } q_j \leq |P_j| \right\}.$$

Case 1: $q_j \geq |P_j|$.
Then we have $w_i \geq s_{m+1}$ for some $i \in P_j$, but since this can hold for at most $c_0 a^{-s_{m+1}} n \leq c_0 s_m^{-5} n$ values of i, we have

$$|E_m^{(1)}| \leq c_0 s_m^{-5} n.$$

Case 2: $q_j \leq |P_j|$.
Then we have $|P_j| \geq s_{m+1}$, which can also only hold for at most $c_0 a^{-s_{m+1}} n \leq c_0 s_m^{-5} n$ values of j, so

$$|E_m^{(2)}| \leq c_0 s_m^{-5} n.$$

Thus we have $|E_m| \leq 2 c_0 s_m^{-5} n$ and together with (D.2) we deduce that $x_m \leq 2 c_0 s_m^{-1}$. Thus (D.1) gives

$$x \leq 2 c_0 \sum_{m=1}^{m_0} \frac{1}{s_m} + \sum_{m=m_0+1}^{\infty} x_m. \tag{D.3}$$

We further observe that for any $m \leq m_0$ we have

$$\frac{s_m}{s_{m-1}} = \frac{6 \log_a \left(\frac{s_{m-1}}{6} \right)}{s_{m-1}} \leq \frac{6 \log_a s_{m-1}}{s_{m-1}} \leq \frac{6 \log_a s_{m_0}}{s_{m_0}}.$$

We have

$$\frac{6 \log_a s_{m_0}}{s_{m_0}} = \frac{6}{100 \log(1/c_1)} \Big(\log 100 + \log(1/c_1) + \log\log(1/c_1) \Big).$$

In order to bound the ratio $\frac{6 \log_a s_{m_0}}{s_{m_0}}$, we define the function

$$g(c_1) = \frac{6}{10} \left(\log(100) + \log\left(\frac{1}{c_1} \right) + \log\log\left(\frac{1}{c_1} \right) \right) - \log\left(\frac{1}{c_1} \right).$$

We have $\lim_{c_1 \to 0} g(c_1) = -\infty$ and $g(10^{-5}) < -0.375985860$. Also,

$$g'(c_1) = \frac{2}{5 c_1} - \frac{3}{5 c_1 \log(1/c_1)} > 0,$$

so g is increasing in that interval and $g(c_1) < 0$. Thus, we have $\frac{6 \log_a s_{m_0}}{s_{m_0}} < 1/10$ because $\frac{6 \log_a s_{m_0}}{s_{m_0}} < 1/10$ is equivalent to $g(c_1) < 0$. Therefore,

$$\sum_{m=1}^{m_0} \frac{1}{s_m} \leq \frac{1}{s_{m_0}} \left(1 + \frac{1}{10} + \frac{1}{100} + \ldots \right) \leq 10^{-9}. \tag{D.4}$$

It remains to estimate $\sum_{m=m_0+1}^{\infty} x_m$, for which we now restrict attention to i and j such that $w_i, |P_j| \leq s_{m_0+1} \leq 100\frac{\log(1/c_1)}{c_1}$. Then we have $\left(\sum_{i\in P_j} w_i\right)^2 \leq 10^8 \left(\frac{\log(1/c_1)}{c_1}\right)^4$, and we trivially have $|\bigcup_{m\geq m_0+1} E_m| \leq \ell \leq n$, therefore

$$\sum_{m=m_0+1}^{\infty} x_m \leq 10^8 \left(\frac{\log(1/c_1)}{c_1}\right)^4 \tag{D.5}$$

and substituting (D.4) and (D.5) into (D.3) gives

$$x \leq 2\cdot c_0 \cdot 10^{-9} + 10^8 \left(\frac{\log(1/c_1)}{c_1}\right)^4.$$

For the case $c_1 \geq 10^{-5}$, choose c_1' such that $c_1' \leq 10^{-5}$, then $c_0 \exp(-c_1 t) \leq c_0 \exp(-c_1' t)$. Thus, by considering the pair (c_0, c_1') and the above reasoning we get

$$c_2 = 2\cdot c_0 \cdot 10^{-9} + 10^8 \left(\frac{\log(1/c_1')}{c_1'}\right)^4.$$

AMIN COJA-OGHLAN, acoghlan@math.uni-frankfurt.de, GOETHE UNIVERSITY, MATHEMATICS INSTITUTE, 10 ROBERT MAYER ST, FRANKFURT 60325, GERMANY.

OLIVER COOLEY, cooley@math.tugraz.at, GRAZ UNIVERSITY OF TECHNOLOGY, INSTITUTE OF DISCRETE MATHEMATICS, STEYRERGASSE 30, 8010 GRAZ, AUSTRIA

MIHYUN KANG, kang@math.tugraz.at, GRAZ UNIVERSITY OF TECHNOLOGY, INSTITUTE OF DISCRETE MATHEMATICS, STEYRERGASSE 30, 8010 GRAZ, AUSTRIA

JOON LEE, lee@math.uni-frankfurt.de, GOETHE UNIVERSITY, MATHEMATICS INSTITUTE, 10 ROBERT MAYER ST, FRANKFURT 60325, GERMANY.

JEAN RAVELOMANANA, raveloma@math.uni-frankfurt.de, GOETHE UNIVERSITY, MATHEMATICS INSTITUTE, 10 ROBERT MAYER ST, FRANKFURT 60325, GERMANY.

D THE FULL RANK CONDITION FOR SPARSE RANDOM MATRICES

AMIN COJA-OGHLAN, PU GAO, MAX HAHN-KLIMROTH, JOON LEE, NOELA MÜLLER, MAURICE ROLVIEN

ABSTRACT. We derive a sufficient condition for a sparse random matrix with given numbers of non-zero entries in the rows and columns having full row rank. The result covers both matrices over finite fields with independent non-zero entries and $\{0,1\}$-matrices over the rationals. The sufficient condition is generally necessary as well. MSc: 60B20, 15B52

1. INTRODUCTION

1.1. **Background and motivation.** Few subjects in combinatorics have had as profound an impact on other disciplines as combinatorial random matrix theory. Prominent applications include powerful error correcting codes called low-density parity check codes [43], data compression [1, 48] and hashing [19]. Needless to mention, random combinatorial matrices are of keen interest to statistical physicists, too [36]. It therefore comes as no surprise that the subject has played a central role in probabilistic combinatorics since the early days [27, 28, 29, 30]. The current state of affairs is that the theory of dense random matrices is significantly more advanced than that of sparse ones with a bounded average number of non-zero entries per row or column [46, 47]. This is in part because concentration techniques apply more easily in the dense case. Another reason is that the study of sparse random matrices is closely tied to the investigation of satisfiability thresholds of random constraint satisfaction problems, an area where many fundamental questions still await a satisfactory solution [4].

Perhaps the most basic question to be asked about any random matrix model is whether the resulting matrix will likely have full rank. This paper contributes a succinct sufficient condition that covers a broad range of sparse random matrix models. As we will see, the condition is essentially necessary as well. The main result can be seen as a satisfiability threshold theorem as the full rank property is equivalent to a random linear system of equations possessing a solution w.h.p. This formulation generalises a number of prior results such as the satisfiability threshold theorem for the random k-XORSAT problem, one of the most intensely studied random constraint satisfaction problems (e.g., [2, 19, 21, 25, 40]). In addition, the main theorem covers other important random matrix models, including those that low-density parity check codes rely on [43].

The classical approach to tackling the full rank problem is the second moment method [3, 4]. This technique was pioneered in the seminal work on the k-XORSAT threshold of Dubois and Mandler [21]. Characteristic of this approach is the emergence of complicated analytic optimisation problems that encode entropy-probability trade-offs resulting from large deviations problems. Tackling these optimisation problems turns out to be rather challenging even in relatively simple special cases such as random k-XORSAT, as witnessed by the intricate calculations that Pittel and Sorkin [40] and Goerdt and Falke [23] had to go through. For the general model that we investigate here this proof technique thus appears futile.

We therefore pursue a totally different proof strategy, largely inspired by ideas from spin glass theory [36, 37]. In statistical physics jargon, the second moment method constitutes an "annealed" computation. This means that we effectively average over all random matrices, including atypical specimens apt to boost the average. By contrast, the present work relies on a "quenched" strategy based on a coupling argument that implicitly discards such pathological events. In effect, we will show that a truncated moment calculation confined to certain benign "equitable" solutions suffices to determine the satisfiability threshold. This part of the proof is an extension of prior work of (some of) the authors on the normalised rank and variations on the random k-XORSAT problem [6, 10]. In addition, to actually compute the truncated second moment we need to determine the precise expected number of equitable solutions. To this end, we devise a new proof ingredient that combines local limit theorem techniques with algebraic ideas, particularly the combinatorial analysis of certain integer lattices. This technique can be seen as a generalisation of an argument of Huang [24] for the study of adjacency matrices of d-regular random graphs.

Amin Coja-Oghlan is supported by DFG CO 646/3 and DFG CO 646/5. Max Hahn-Klimroth is supported by DFG CO 646/5. Noela Müller is supported by NWO Gravitation grant NETWORKS-024.002.003.

Let us proceed to present the main results of the paper. The first theorem deals with random matrices over finite fields. As an application we obtain a result on sparse $\{0,1\}$-matrices over the rationals.

1.2. **Results.** We work with the comprehensive random matrix model from [10]. Hence, let $\boldsymbol{d} \geq 0$, $\boldsymbol{k} \geq 3$ be independent integer-valued random variables such that $\mathbb{E}[\boldsymbol{d}^{2+\eta}] + \mathbb{E}\left[\boldsymbol{k}^{2+\eta}\right] < \infty$ for an arbitrarily small $\eta > 0$. Let $(\boldsymbol{d}_i, \boldsymbol{k}_i)_{i\geq 1}$ be independent copies of $(\boldsymbol{d}, \boldsymbol{k})$ and set $d = \mathbb{E}[\boldsymbol{d}]$, $k = \mathbb{E}[\boldsymbol{k}]$. Moreover, let $\mathfrak{d}$ and $\mathfrak{k}$ be the greatest common divisors of the support of $\boldsymbol{d}$ and $\boldsymbol{k}$, respectively. Further, let $n > 0$ be an integer divisible by $\mathfrak{k}$ and let $\boldsymbol{m}$ be a Poisson variable with mean dn/k, independent of $(\boldsymbol{d}_i, \boldsymbol{k}_i)_i$. Routine arguments reveal that the event

$$\sum_{i=1}^{n} \boldsymbol{d}_i = \sum_{j=1}^{\boldsymbol{m}} \boldsymbol{k}_j \tag{1.1}$$

occurs with probability at least $\Omega(n^{-1/2})$ [10, Proposition 1.7]. Given (1.1) let $\mathbb{G} = \mathbb{G}_n(\boldsymbol{d}, \boldsymbol{k})$ be a simple random bipartite graph on a set $\{a_1 \ldots, a_{\boldsymbol{m}}\}$ of *check nodes* and a set $\{x_1, \ldots, x_n\}$ of *variable nodes* such that the degree of a_i equals $\boldsymbol{k}_i$ and the degree of x_j equals $\boldsymbol{d}_j$ for all i, j. Following coding theory jargon, we refer to $\mathbb{G}$ as the *Tanner graph*. The edges of $\mathbb{G}$ are going to mark the positions of the non-zero entries of the random matrix. The entries themselves will depend on whether we deal with a finite field or the rationals.

1.2.1. *Finite fields.* Suppose that $q \geq 2$ is a prime power, let $\mathbb{F}_q$ signify the field with q elements and let $\boldsymbol{\chi}$ be a random variable that takes values in the set $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ of units of $\mathbb{F}_q$. Moreover, let $(\boldsymbol{\chi}_{i,j})_{i,j\geq 1}$ be copies of $\boldsymbol{\chi}$, mutually independent and independent of the $\boldsymbol{d}_i, \boldsymbol{k}_i$, $\boldsymbol{m}$ and $\mathbb{G}$. Finally, let $\mathbb{A} = \mathbb{A}_n(\boldsymbol{d}, \boldsymbol{k}, \boldsymbol{\chi})$ be the $\boldsymbol{m} \times n$-matrix with entries

$$\mathbb{A}_{i,j} = \mathbb{1}\{a_i x_j \in E(\mathbb{G})\} \cdot \boldsymbol{\chi}_{i,j}.$$

Hence, the i-th row of $\mathbb{A}$ contains $\boldsymbol{k}_i$ non-zero entries and the j-th column contains $\boldsymbol{d}_j$ non-zero entries.

The following theorem provides a sufficient condition for $\mathbb{A}$ having full row rank. The condition comes in terms of the probability generating functions $D(x)$ and $K(x)$ of $\boldsymbol{d}$ and $\boldsymbol{k}$. Since $\mathbb{E}[\boldsymbol{d}^2] + \mathbb{E}[\boldsymbol{k}^2] < \infty$, we may define

$$\Phi : [0,1] \to \mathbb{R}, \qquad z \mapsto D\left(1 - K'(z)/k\right) - \frac{d}{k}\left(1 - K(z) - (1-z)K'(z)\right). \tag{1.2}$$

Theorem 1.1. *If q and $\mathfrak{d}$ are coprime and*

$$\Phi(z) < \Phi(0) \qquad \text{for all } 0 < z \leq 1, \tag{1.3}$$

then $\mathbb{A}$ has full row rank over $\mathbb{F}_q$ w.h.p.

Observe that the function Φ does not depend on q. Hence, neither does (1.3).

The sufficient condition (1.3) is generally necessary, too. Indeed, [10, Theorem 1.1] determines the likely value of the *normalised* rank of $\mathbb{A}$:

$$\frac{\mathrm{rk}(\mathbb{A})}{n} \xrightarrow{\mathbb{P}} 1 - \max_{z\in[0,1]} \Phi(z) \qquad \text{as } n \to \infty. \tag{1.4}$$

Since $\boldsymbol{k} \geq 3$, the definition (1.2) ensures that $\Phi(0) = 1 - d/k$ and thus $n\Phi(0) \sim n - \boldsymbol{m}$ w.h.p. Hence, (1.4) implies that $\mathrm{rk}(\mathbb{A}) \leq \boldsymbol{m} - \Omega(n)$ w.h.p. unless $\Phi(z)$ attains its maximum at $z = 0$. In other words, $\mathbb{A}$ has full row rank *only if* $\Phi(z) \leq \Phi(0)$ for all $0 < z \leq 1$. Indeed, in Section 1.3 we will discover examples that requite a strict inequality as in (1.3). The condition that q and $\mathfrak{d}$ be coprime is generally necessary as well, as we will see in Example 1.7 below.

Let us emphasise that (1.4) does not guarantee that $\mathbb{A}$ has full row rank w.h.p. even if (1.3) is satisfied. Rather due to the normalisation on the l.h.s. (1.4) only implies the much weaker statement $\mathrm{rk}(\mathbb{A}) = \boldsymbol{m} - o(n)$ w.h.p. Hence, in the case that (1.3) is satisfied, Theorem 1.1 improves over the asymptotic estimate (1.4) rather substantially. Unsurprisingly, this stronger result also requires a more delicate proof strategy.

1.2.2. *Zero-one matrices over the rationals.* Apart from matrices over finite fields, the rational rank of sparse random $\{0,1\}$-matrices has received a great deal of attention [46, 47]. The random graph $\mathbb{G}$ naturally induces a $\{0,1\}$-matrix, namely the $\boldsymbol{m} \times n$-biadjacency matrix $\mathbb{B} = \mathbb{B}(\mathbb{G})$. Explicitly, $\mathbb{B}_{ij} = \mathbb{1}\{a_i x_j \in E(\mathbb{G})\}$. As an application of Theorem 1.1 we obtain the following result.

Corollary 1.2. *If* (1.3) *is satisfied then the random matrix $\mathbb{B}$ has full row rank over $\mathbb{Q}$ w.h.p.*

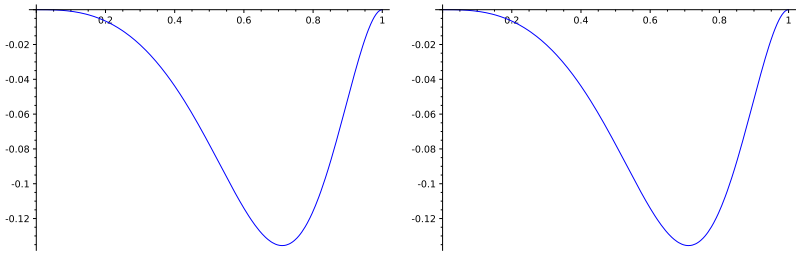

FIGURE 1. Left: Example 1.3 with $D(z) = \exp(6.5(z-1))$ and $K(z) = z^7$. Middle: Example 1.4 with $D(z) = K(z) = (z^3 + z^4)/2$.

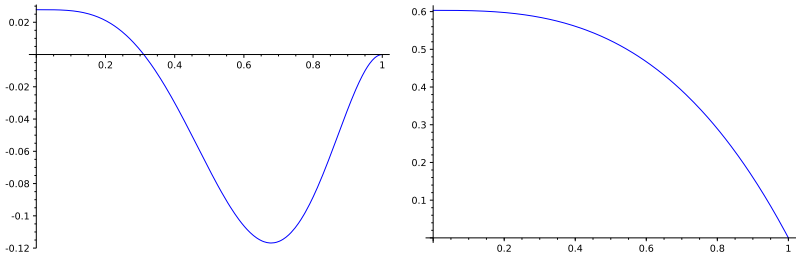

FIGURE 2. Left: Example 1.5 with $D(z) = z^3, K(z) = z^8$. Right: Example 1.6 with $D(z) = \sum_{\ell=1}^{\infty} \zeta(3.5)^{-1} z^\ell \ell^{-3.5}$ and $K(x) = x^3$.

Since (1.4) holds for random matrices over the rationals as well, Corollary 1.2 is optimal to the extent that $\mathbb{B}$ fails to have full row rank w.h.p. if $\max_{x\in[0,1]} \Phi(x) > \Phi(0)$. Moreover, in Example 1.4 we will see that $\mathbb{B}$ does not generally have full rank w.h.p. unless $x = 0$ is the unique maximiser of Φ.

1.3. **Examples.** To illustrate the power of Theorem 1.1 and Corollary 1.2 we consider a few instructive special cases of distributions $\boldsymbol{d}, \boldsymbol{k}, \boldsymbol{\chi}$.

Example 1.3 (random k-XORSAT)**.** In random k-XORSAT we are handed a number of independent random constraints c_i of the type

$$c_i = y_{i1} \text{ XOR } \cdots \text{ XOR } y_{ik}, \tag{1.5}$$

where each y_{ij} is either one of n available Boolean variables $x_1, \ldots, x_n$ or a negation $\neg x_1, \ldots, \neg x_n$. The obvious question is to determine the satisfiability threshold, i.e., the maximum number of random constraints can be satisfied simultaneously w.h.p.

Because Boolean XOR boils down to addition over $\mathbb{F}_2$, this problem can be rephrased as the full rank problem for the random matrix $\mathbb{A}$ with $q = 2$, $\boldsymbol{k} = k$ fixed to a deterministic value and $\boldsymbol{d} \sim \mathrm{Po}(d)$ for a parameter $d > 0$. To elaborate, because the constraints c_i are drawn uniformly and independently, we can think of each as tossing k balls randomly into n bins that represent $x_1, \ldots, x_n$. If there are $\boldsymbol{m} \sim \mathrm{Po}(dn/k)$ constraints c_i, the joint distribution of the variable degrees coincides with the distribution of $(\boldsymbol{d}_1, \ldots, \boldsymbol{d}_n)$ subject to the condition (1.1). Furthermore, the random negation patterns of the constraints (1.5) amount to choosing a random right-hand side vector $\boldsymbol{y}$ for which we are to solve $\mathbb{A}x = \boldsymbol{y}$.

Since the generating functions of $\boldsymbol{d}, \boldsymbol{k}$ work out to be $D(z) = \exp(d(z-1))$ and $K(z) = z^k$, we obtain

$$\Phi_{d,k}(z) = \exp(-dz^{k-1}) - \frac{d}{k}\left(1 - kz^{k-1} + (k-1)z^k\right).$$

Thus, Theorem 1.1 implies that for a given $k \geq 3$ the threshold of d up to which random k-XORSAT is satisfiable w.h.p. equals the largest d such that

$$\Phi_{d,k}(z) < \Phi_{d,k}(0) = 1 - d/k \qquad \text{for all } 0 < z \leq 1. \tag{1.6}$$

A few lines of calculus verify that (1.6) matches the formulas for the k-XORSAT threshold derived by combinatorial methods tailored to this specific case [19, 21, 40, 37]. Theorem 1.1 also encompasses the generalisations to other finite fields $\mathbb{F}_q$ from [6, 23].

Example 1.4 (identical distributions)**.** An interesting scenario arises when $\boldsymbol{d}, \boldsymbol{k}$ are identically distributed. For example, suppose that $\mathbb{P}[\boldsymbol{d} = 3] = \mathbb{P}[\boldsymbol{d} = 4] = \mathbb{P}[\boldsymbol{k} = 3] = \mathbb{P}[\boldsymbol{k} = 4] = 1/2$. Thus, $D(z) = K(z) = (z^3 + z^4)/2$ and

$$\Phi(z) = \frac{256z^{12} + 768z^{11} + 864z^{10} - 1808z^9 - 4959z^8 - 3780z^7 + 6111z^6 + 10584z^5 - 3234z^4 - 4802z^3}{4802}.$$

This function attains two identical maxima, namely $\Phi(0) = \Phi(1) = 0$. Since the degrees $\boldsymbol{k}_i, \boldsymbol{d}_i$ are chosen independently subject only to (1.1), the probability that $\mathbb{A}$ has more rows than columns works out to be $1/2 + o(1)$. As a consequence, $\mathbb{A}$ cannot have full row rank w.h.p. This example shows that the condition that 0 be the *unique* maximiser of $\Phi(x)$ is generally necessary $\mathbb{A}$ to ensure full row rank. The same applies to the rational rank of $\mathbb{B}$.

Example 1.5 (fixed $\boldsymbol{d}, \boldsymbol{k}$)**.** Suppose that both $\boldsymbol{d} = d, \boldsymbol{k} = k \geq 3$ are constants rather than genuinely random. Then

$$\Phi(z) = \left(1 - z^{k-1}\right)^d - \frac{d}{k}\left(1 - kz^{k-1} + (k-1)z^k\right).$$

Clearly, $\mathbb{A}$ cannot have full row rank unless $d \leq k$, while Theorem 1.1 implies that $\mathbb{A}$ has full row rank w.h.p. if $d < k$. This result was previously established via the second moment method [38]. But in the critical case $d = k$ the function $\Phi(z)$ attains its identical maxima at $z = 0$ and $z = 1$. Specifically, $0 = \Phi(0) = \Phi(1) > \Phi(z)$ for all $0 < z < 1$. Hence, Theorem 1.1 does not cover this special case. Nonetheless, Huang [24] proved that the random $\{0,1\}$-matrix $\mathbb{B}$ has full rational rank w.h.p. The proof is based on a delicate moment computation in combination with a precise local expansion around the equitable solutions.

Example 1.6 (power laws)**.** Let $\mathbb{P}(\boldsymbol{d} = \ell) \propto \ell^{-\alpha}$ for some $\alpha > 3$ and $\boldsymbol{k} = k \geq 3$. Thus,

$$D(z) = \frac{1}{\zeta(\alpha)} \sum_{\ell=1}^{\infty} \frac{z^\ell}{\ell^\alpha}, \qquad K(z) = z^k, \qquad \Phi(z) = D\left(1 - z^{k-1}\right) - \frac{\zeta^{-1}(\alpha)\zeta(\alpha-1)}{k}\left(1 - kz^{k-1} + (k-1)z^k\right).$$

Since

$$\Phi'(z) = -(k-1)z^{k-2}D'\left(1 - z^{k-1}\right) + \frac{\zeta^{-1}(\alpha)\zeta(\alpha-1)}{k}\left(k(k-1)(z^{k-1} - z^{k-2})\right) < 0,$$

the function $\Phi(z)$ is strictly decreasing on $(0,1)$. Therefore, (1.3) is satisfied.

Example 1.7 (zero row sums)**.** Theorem 1.1 requires the assumption that q and the g.c.d. $\mathfrak{d}$ of the support of $\boldsymbol{d}$ be coprime. This assumption is indeed necessary. To see this, consider the case that $q = 2$, $\boldsymbol{\chi} = 1$, $\boldsymbol{d} = 4$ and $\boldsymbol{k} = 8$ deterministically. Then the rows of $\mathbb{A}$ always sum to zero. Hence, $\mathbb{A}$ cannot have full row rank.

2. Overview

In contrast to much of the prior work on the rank problem, random k-XORSAT and random constraint satisfaction problems generally, the proofs of the main results do not rely on an "annealed" second moment computation. Such arguments appear to be far too susceptible to large deviations effects to extend to as general a random matrix model as we deal with here. Instead, we proceed by way of a "quenched" argument that enables us to discard pathological events. As a result, it suffices to carry out the moment calculation in the particularly benign case of "equitable" solutions.

This proof strategy draws on but substantially generalises tools that were developed towards the approximate rank formula (1.4) and variations on random k-XORSAT [6, 10]. In addition, to actually prove that $\mathbb{A}$ has full rank with *high* probability we will need to carry out a meticulous, asymptotically exact calculation of the expected number of equitable solutions. A key element of this analysis will be a delicate analysis of the lattices generated by certain integer vectors that encode conceivable equitable solutions. This part of the proof, which generalises a part of Huang's argument for the adjacency matrices of random d-regular graphs [24], combines local limit techniques with a whiff of linear algebra.

To describe the proof strategy in detail let us first explore the "annealed" path, discover its pitfalls and then apply the lessons learned to develop a workable "quenched" strategy. The bulk of the proof deals with the random matrix model from Section 1.2.1 over the finite field $\mathbb{F}_q$; the rational case from Corollary 1.2 comes out as an easy consequence.

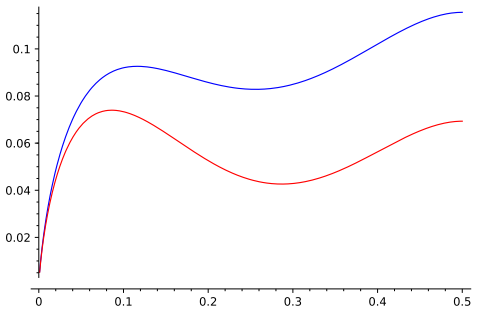

FIGURE 3. The r.h.s. of (2.4) for $d = 2.5$ (blue) and $d = 2.7$ (red) in the interval $[0, \frac{1}{2}]$.

In order to reduce fluctuations we are going to condition on the σ-algebra $\mathfrak{A}$ generated by $\boldsymbol{m}, (\boldsymbol{k}_i)_{i\geq 1}, (\boldsymbol{d}_i)_{i\geq 1}$ and by the numbers $\boldsymbol{m}(\chi_1, \ldots, \chi_\ell)$ of checks of degree $\ell \geq 3$ with coefficients $\chi_1, \ldots, \chi_\ell \in \mathbb{F}_q^*$. We write $\mathbb{P}_{\mathfrak{A}} = \mathbb{P}[\cdot \mid \mathfrak{A}]$ and $\mathbb{E}_{\mathfrak{A}} = \mathbb{E}[\cdot \mid \mathfrak{A}]$ for brevity.

2.1. **Moments and deviations.** We already alluded to how the full rank problem for the random matrix $\mathbb{A}$ over $\mathbb{F}_q$ can be viewed as a random constraint satisfaction problem. Indeed, suppose we draw a right-hand side vector $\boldsymbol{y} \in \mathbb{F}_q^{\boldsymbol{m}}$ independently of $\mathbb{A}$. Then $\mathbb{A}$ has full row rank w.h.p. iff the random linear system $\mathbb{A}x = \boldsymbol{y}$ admits a solution w.h.p. For if $\mathrm{rk}\,\mathbb{A} < \boldsymbol{m}$, then the image $\mathbb{A}\mathbb{F}_q^n$ is a proper subspace of $\mathbb{F}_q^{\boldsymbol{m}}$ and thus the random linear system $\mathbb{A}x = \boldsymbol{y}$ has a solution with probability at most $1 - 1/q$. Naturally, the random linear system is nothing but a random constraint satisfaction problem with $\boldsymbol{m}$ constraints and n variables.

Over the past two decades the second moment method has emerged as the default approach to pinpointing satisfiability thresholds of random constraint satisfaction problems [3, 4]. Indeed, one of the first success stories was the random 3-XORSAT problem, which boils down directly to a full rank problem over $\mathbb{F}_2$ [21]. In fact, as we saw in Example 1.3, to mimic 3-XORSAT we just set $q = 2$, $\boldsymbol{d} = \mathrm{Po}(d)$ for some $d > 0$ and $\boldsymbol{k} = 3$ deterministically. In addition, draw $\boldsymbol{y} \in \mathbb{F}_2^{\boldsymbol{m}}$ uniformly and independently of everything else.

We try the second moment method on the number $\boldsymbol{Z} = \boldsymbol{Z}(\mathbb{A}, \boldsymbol{y})$ of solutions to $\mathbb{A}x = \boldsymbol{y}$ given $\mathfrak{A}$. Since $\boldsymbol{y}$ is independent of $\mathbb{A}$, for any fixed vector $x \in \mathbb{F}_2^n$ the event $\mathbb{A}x = \boldsymbol{y}$ has probability $2^{-\boldsymbol{m}}$. Consequently,

$$\mathbb{E}_{\mathfrak{A}}[\boldsymbol{Z}] = 2^{n-\boldsymbol{m}}. \tag{2.1}$$

Hence, (2.1) recovers the obvious condition that we cannot have more rows than columns. Since $\boldsymbol{m} \sim \mathrm{Po}(dn/3)$, (2.1) boils down to $d < 3$.

The second moment method now rests on the hope that we may be able to show that $\mathbb{E}_{\mathfrak{A}}[\boldsymbol{Z}^2] \sim \mathbb{E}_{\mathfrak{A}}[\boldsymbol{Z}]^2$. Then Chebyshev's inequality would imply $\boldsymbol{Z} \sim \mathbb{E}_{\mathfrak{A}}[\boldsymbol{Z}]$ w.h.p., and thus, in light of (2.1), that $\mathbb{A}x = \boldsymbol{y}$ has a solution w.h.p.

Concerning the computation of $\mathbb{E}_{\mathfrak{A}}[\boldsymbol{Z}^2]$, because the set of solutions is either empty or a translation of the kernel, we obtain

$$\mathbb{E}_{\mathfrak{A}}[\boldsymbol{Z}^2] = \sum_{\sigma,\tau\in\mathbb{F}_q^n} \mathbb{P}_{\mathfrak{A}}\left[\mathbb{A}\sigma = \mathbb{A}\tau = \boldsymbol{y}\right] = \sum_{\sigma,\tau\in\mathbb{F}_q^n} \mathbb{P}_{\mathfrak{A}}\left[\mathbb{A}\sigma = \boldsymbol{y}\right]\mathbb{P}_{\mathfrak{A}}\left[\sigma - \tau \in \ker\mathbb{A}\right] = \mathbb{E}_{\mathfrak{A}}[\boldsymbol{Z}]\,\mathbb{E}_{\mathfrak{A}}|\ker\mathbb{A}|. \tag{2.2}$$

To calculate the expected kernel size we notice that the probability that a vector x is in the kernel depends on its Hamming weight. For instance, the zero vector always belongs to the kernel, while the all-ones vector $\mathbb{1}$ does not w.h.p. More systematically, invoking inclusion/exclusion, we find that for a vector x of Hamming weight w we have $\mathbb{P}_{\mathfrak{A}}[x \in \ker\mathbb{A}] \sim \left[(1 + (1-2w/n)^3)/2\right]^{\boldsymbol{m}}$. Since the total number of such vectors comes to $\binom{n}{w}$, we obtain

$$\mathbb{E}_{\mathfrak{A}}|\ker\mathbb{A}| = \sum_{w=0}^{n}\binom{n}{w}\left(\frac{1+(1-2w/n)^3}{2}\right)^{\boldsymbol{m}}. \tag{2.3}$$

Taking logarithms, invoking Stirling's formula and parametrising $w = zn$, we simplify (2.3) to

$$\log\mathbb{E}_{\mathfrak{A}}|\ker\mathbb{A}| \sim n\cdot\max_{z\in[0,1]} -z\log z - (1-z)\log(1-z) + \frac{\boldsymbol{m}}{n}\log\frac{1+(1-2z)^3}{2} \qquad \text{(cf. [21])}. \tag{2.4}$$

If we substitute $z = 1/2$ into (2.4), the expression further simplifies to $(n - \boldsymbol{m})\log 2$. Hence, if the maximum is attained at another value $z \neq 1/2$, then (2.4) yields $\mathbb{E}_{\mathfrak{A}}|\ker\mathbb{A}| \gg 2^{n-\boldsymbol{m}}$ and the second moment method fails.

Figure 3 displays (2.4) for $d = 2.5$ and $d = 2.7$. While for $d = 2.5$ the function takes its maximum at $z = 1/2$, for $d = 2.7$ the maximum is attained at $z \approx 0.085$. However, the true random 3-XORSAT threshold is $d \approx 2.75$ [21]. Thus, the naive second moment calculation falls short of the real threshold.

How so? The expression (2.4) does not determine the "likely" but the expected size of the kernel, a value prone to large deviations effects. Indeed, because the number of vectors in the kernel scales exponentially with n, an exponentially unlikely event that causes an exceptionally large kernel may end up dominating $\mathbb{E}_{\mathfrak{A}}|\ker\mathbb{A}|$. Precisely such an event manifests itself in the left local maxima in Figure 3. Moreover, as we approach the satisfiability threshold such large deviations issues are compounded by a diminishing error tolerance. Indeed, while for $d = 2.5$ the value at $z = 1/2$ just swallows the spurious maximum, this is no longer the case for $d = 2.7$.

For random k-XORSAT Dubois and Mandler managed to identify the precise large deviations effect at work. It stems from fluctuations of a densely connected sub-graph of $\mathbb{G}$ called the 2-core, obtained by iteratively pruning nodes of degree less than two along with their neighbours (if any). Dubois and Mandler pinpointed the 3-XORSAT threshold by applying the second moment method to the minor $\mathbb{A}^{(2)}$ induced by $\mathbb{G}^{(2)}$ while conditioning on the 2-core having its typical dimensions.

The technical difficulty is that the rows of $\mathbb{A}^{(2)}$ are no longer independent. Indeed, $\mathbb{A}^{(2)}$ is distributed as a random matrix with a truncated Poisson $\boldsymbol{d}^{(2)} \sim \mathrm{Po}_{\geq 2}(d')$ with $d' = d'(d,k) > 0$ as the distribution of the variable degrees. Unfortunately, the given-degrees model leads to a fairly complicated moment computation. Instead of the humble one-dimensional problem from (2.4) we now face parameters $(z_i)_{i\geq 2}$ that gauge the fraction of variables of each possible degree i set to one. Additionally, on the constraint side we need to keep track of the number of equations with zero and with two variables set to one. Of course, these variables are tied together through the constraint that the total Hamming weight on the variable side match that on the constraint side.

With a deal of diligence Dubois and Mandler managed to solve this optimisation problem. However, even just the step on to check degrees $k > 3$ turns out to be tricky because now we need to keep track of all the possible ways in which a k-ary parity constraint can be satisfied [19, 40]. Yet even these difficulties are eclipsed by those that result from merely advancing to fields of size $q = 3$ [23].

Not to mention entirely general degree distributions $\boldsymbol{d}, \boldsymbol{k}$ and general fields $\mathbb{F}_q$ as in Theorem 1.1. The ensuing optimisation problem comes in terms of variables $(z_i)_{i\in\mathrm{supp}\boldsymbol{d}}$ that range over the space $\mathscr{P}(\mathbb{F}_q)$ of probability distributions on $\mathbb{F}_q$. Additionally, there is a second set of variables $(\hat{z}_{\chi_1,\ldots,\chi_\ell})_{\ell\in\mathrm{supp}\boldsymbol{k},\chi_1,\ldots,\chi_\ell\in\mathrm{supp}\boldsymbol{\chi}}$ to go with the rows of $\mathbb{A}$ whose non-zero entries are precisely $\chi_1,\ldots,\chi_\ell$. These variables range over probability distributions on solutions $\sigma \in \mathbb{F}_q^\ell$ to $\chi_1\sigma_1 + \cdots + \chi_\ell\sigma_\ell = 0$. In terms of these variables we would need to solve

$$\max \quad \sum_{\sigma\in\mathbb{F}_q} \mathbb{E}\left[(\boldsymbol{d}-1)z_{\boldsymbol{d}}(\sigma)\log z_{\boldsymbol{d}}(\sigma)\right] - \frac{d}{k}\mathbb{E}\left[\sum_{\substack{\sigma_1,\ldots,\sigma_{\boldsymbol{k}}\in\mathbb{F}_q\\ \boldsymbol{\chi}_{1,1}\sigma_1+\cdots+\boldsymbol{\chi}_{1,\boldsymbol{k}}\sigma_{\boldsymbol{k}}=0}} \hat{z}_{\boldsymbol{\chi}_{1,1},\ldots,\boldsymbol{\chi}_{1,\boldsymbol{k}}}(\sigma_1,\ldots,\sigma_{\boldsymbol{k}})\log\hat{z}_{\boldsymbol{\chi}_{1,1},\ldots,\boldsymbol{\chi}_{1,\boldsymbol{k}}}(\sigma_1,\ldots,\sigma_{\boldsymbol{k}})\right] \tag{2.5}$$

$$\text{s.t.} \quad \mathbb{E}[\boldsymbol{d}z_{\boldsymbol{d}}(\tau)] = \mathbb{E}\left[\sum_{\substack{\sigma_1,\ldots,\sigma_{\boldsymbol{k}}\in\mathbb{F}_q\\ \boldsymbol{\chi}_{1,1}\sigma_1+\cdots+\boldsymbol{\chi}_{1,\boldsymbol{k}}\sigma_{\boldsymbol{k}}=0}} \boldsymbol{k}\mathbb{1}\{\sigma_1=\tau\}\,\hat{z}_{\boldsymbol{\chi}_{1,1},\ldots,\boldsymbol{\chi}_{1,\boldsymbol{k}}}(\sigma_1,\ldots,\sigma_{\boldsymbol{k}})\right] \qquad \text{for all } \tau\in\mathbb{F}_q.$$

As in random 3-XORSAT, a simple calculation shows that the value of (2.5) evaluated at the "equitable" solution

$$z_i(\sigma) = q^{-1} \qquad \hat{z}_{\chi_1,\ldots,\chi_\ell}(\sigma_1,\ldots,\sigma_\ell) = q^{1-\ell} \qquad \text{for all } i,\chi_1,\ldots,\chi_\ell \tag{2.6}$$

hits the value $(1-d/k)\log q$, which matches the normalised first moment $n^{-1}\log\mathbb{E}_{\mathfrak{A}}[\boldsymbol{Z}]$.

In summary, the second moment method hardly seems like a promising path towards Theorem 1.1. Not only does (2.5) seem unwieldy as even for very special cases of $\boldsymbol{d}, \boldsymbol{k}$ an analytic solution remains elusive [23]. Even worse, just in the case of "unabridged" random k-XORSAT large deviations effects may cause spurious maxima. In effect, even if we could miraculously figure out the precise conditions for (2.5) being attained at the uniform solution, this would hardly determine for what $\boldsymbol{d}, \boldsymbol{k}$ the random matrix $\mathbb{A}$ actually has full row rank w.h.p.

2.2. **Quenching and truncating.** The large deviations issues ultimately result from our attempt at computing the mean of $|\ker\mathbb{A}|$, a (potentially) exponential quantity. The mathematical physics prescription is to compute the expectation of its logarithm instead [36]. In the present algebraic setting this comes down to computing the mean of the nullity $\mathrm{nul}\,\mathbb{A} = \dim\ker\mathbb{A}$, or equivalently of the rank $\mathrm{rk}\,\mathbb{A} = n - \mathrm{nul}\,\mathbb{A}$. This "quenched average" is always of order $O(n)$ and therefore immune to large deviations effects. In fact, even if on some unfortunate event of

exponentially small probability $\exp(-\Omega(n))$ the kernel of $\mathbb{A}$ were quite large, the ensuing boost to $\mathbb{E}_{\mathfrak{A}}[\operatorname{nul}\mathbb{A}]$ remains negligible.

Yet computing the quenched average $\mathbb{E}_{\mathfrak{A}}[\operatorname{nul}\mathbb{A}]$ does not suffice to prove Theorem 1.1. Indeed, (1.4) already provides an asymptotic formula for $\mathbb{E}_{\mathfrak{A}}[\operatorname{nul}\mathbb{A}]$. But as we saw due to the normalisation on the l.h.s. (1.4) merely implies that $\operatorname{rk}\mathbb{A} = \boldsymbol{m} - o(n)$ w.h.p. To actually prove that $\operatorname{rk}\mathbb{A} = \boldsymbol{m}$ w.h.p. we will combine the quenched computation with a truncated moment argument calculation. Specifically, we will harness an enhanced version of (1.4) to prove that under the assumptions of Theorem 1.1 the only combinatorially meaningful solutions to (2.5) asymptotically coincide with the equitable solution (2.6), around which we will subsequently expand (2.5) carefully.

To carry this programme out, let $\boldsymbol{x}_{\mathbb{A}} = (\boldsymbol{x}_{\mathbb{A},i})_{i\in[n]} \in \mathbb{F}_q^n$ be a random vector from the kernel of $\mathbb{A}$. Consider the event

$$\mathfrak{O} = \left\{ \sum_{\sigma,\tau\in\mathbb{F}_q} \sum_{i,j=1}^{n} \left| \mathbb{P}\left[\boldsymbol{x}_{\mathbb{A},i} = \sigma,\ \boldsymbol{x}_{\mathbb{A},j} = \tau \mid \mathbb{A}\right] - q^{-2} \right| = o(n^2) \right\}. \tag{2.7}$$

Then by Chebyshev's inequality on $\mathfrak{O}$ w.h.p. we have

$$\sum_{i=1}^{n} \mathbb{1}\left\{\boldsymbol{d}_i = \ell, \boldsymbol{x}_{\mathbb{A},i} = \sigma\right\} = \mathbb{P}[\boldsymbol{d} = \ell]\, n/q + o(n) \qquad \text{for all } \sigma \in \mathbb{F}_q,\ \ell \in \operatorname{supp}\boldsymbol{d}.$$

Hence, on $\mathfrak{O}$ the only combinatorially relevant value of $z_\ell(\sigma)$ from (2.5) is the uniform $1/q$ for every ℓ, σ, because for every ℓ asymptotically almost all kernel vectors set about an equal number of variables of degree ℓ to each of the q possible values. Thanks to this observation will prove that w.h.p.

$$\mathbb{E}_{\mathfrak{A}}[\boldsymbol{Z} \cdot \mathbb{1}\{\mathbb{A} \in \mathfrak{O}\}] \sim \mathbb{E}_{\mathfrak{A}}[\boldsymbol{Z}] \sim q^{n-\boldsymbol{m}} \qquad \text{and} \tag{2.8}$$

$$\mathbb{E}_{\mathfrak{A}}\left[\boldsymbol{Z}^2 \cdot \mathbb{1}\{\mathbb{A} \in \mathfrak{O}\}\right] \sim \mathbb{E}_{\mathfrak{A}}[\boldsymbol{Z}]^2, \tag{2.9}$$

provided that (1.3) is satisfied. Theorem (1.1) will turn out to be an easy consequence of (2.8)–(2.9), and Corollary 1.2 of Theorem 1.1.

Thus, the challenge is to prove (2.8)–(2.9). Specifically, while the second asymptotic equality in (2.8) is easy, the proof of the first is where we require knowledge of the "quenched average" (1.4). In fact, instead of just applying (1.4) as is we will need to perform a "quenched" computation for a slightly enhanced random matrix from scratch. Second, the key challenge towards the proof of (2.9) is to obtain an exact asymptotic equality here, rather than the weaker estimate $\mathbb{E}_{\mathfrak{A}}\left[\boldsymbol{Z}^2 \cdot \mathbb{1}\{\mathbb{A} \in \mathfrak{O}\}\right] = O(\mathbb{E}_{\mathfrak{A}}[\boldsymbol{Z}]^2)$. This will require a meticulous expansion of the second moment around the uniform solution, which will involve the detailed analysis of the lattices generated by integer vectors that encode conceivable values of $z_i, \hat{z}_{\chi_1,\ldots,\chi_\ell}$ from (2.5).

2.3. **The truncated first moment.** Let us begin with (2.8). Although we know the approximate nullity (1.4) of $\mathbb{A}$ already, this does not suffice to actually prove that $\mathfrak{O}$ is a "likely" event. To this end we need to study a slightly modified matrix instead. Specifically, for an integer $t \geq 0$ obtain $\mathbb{A}_{[t]}$ from $\mathbb{A}$ by adding t more rows that contain precisely three non-zero entries. The positions of these non-zero entries are chosen uniformly, mutually independently and independently of everything else, and the non-zero entries themselves are independent copies of $\boldsymbol{\chi}$. We require the following lower bound on the rank of $\mathbb{A}_{[t]}$.

Proposition 2.1. *If* (1.3) *is satisfied then there exists* $\delta_0 = \delta_0(\boldsymbol{d}, \boldsymbol{k}) > 0$ *such that for all* $0 < \delta < \delta_0$ *we have*

$$\liminf_{n\to\infty} \frac{1}{n} \mathbb{E}[\operatorname{nul}\mathbb{A}_{[\lfloor\delta n\rfloor]}] \leq 1 - \frac{d}{k} - \delta. \tag{2.10}$$

The proof of Proposition 2.1 relies on the Aizenman-Sims-Starr scheme, a coupling argument inspired by spin glass theory [5]. The technique was also used in [10] to prove the rank formula (1.4). While we mostly follow that proof strategy and can even reuse some of the intermediate deliberations, a subtle modification is required to accommodate the additional ternary equations. The details can be found in Section 4.

How does Proposition 2.1 facilitate the proof of (2.8)? Assuming (1.3), we obtain from (1.4) that $\operatorname{nul}\mathbb{A}/n \sim 1 - d/k$ w.h.p. Hence, (2.10) shows that nearly each one of the of the additional ternary rows added to $\mathbb{A}_{[\lfloor\delta n\rfloor]}$ reduces the nullity. We are going to argue that this is possible only if $\mathbb{A} \in \mathfrak{O}$ w.h.p.

To see this, let us think about the kernel of a general $M \times N$ matrix A over $\mathbb{F}_q$ for a short moment. Draw $\boldsymbol{x}_A = (\boldsymbol{x}_{A,i})_{i\in[N]} \in \ker A$ uniformly at random. For any given coordinate $\boldsymbol{x}_{A,i}$, $i \in [N]$ there are two possible scenarios: either $\boldsymbol{x}_{A,i} = 0$ deterministically, or $\boldsymbol{x}_{A,i}$ is uniformly distributed over $\mathbb{F}_q$. (This is because if we multiply $\boldsymbol{x}_A$ by a

scalar $t \in \mathbb{F}_q$ we obtain $t\boldsymbol{x}_A \in \ker A$.) We therefore call coordinate i *frozen* if $x_i = 0$ for all $x \in \ker A$ and unfrozen otherwise. Let $\mathfrak{F}(A)$ be the set of frozen coordinates.

If $\mathbb{A}$ had many frozen coordinates then adding an extra random row with three non-zero entries could hardly decrease the nullity w.h.p. For if all three non-zero coordinates fall into the frozen set, then we get the new equation "for free", i.e., $\operatorname{nul}\mathbb{A}_{[1]} = \operatorname{nul}\mathbb{A}$. Thus, Proposition 2.1 implies that $|\mathfrak{F}(\mathbb{A})| = o(n)$ w.h.p. We conclude that $\boldsymbol{x}_{\mathbb{A},i}$ is uniformly distributed over $\mathbb{F}_q$ for all but $o(n)$ coordinates $i \in [n]$. However, this does not yet imply that $\boldsymbol{x}_{\mathbb{A},i}, \boldsymbol{x}_{\mathbb{A},j}$ are independent for most i, j, as required by $\mathfrak{D}$. Yet a more careful argument based on the "pinning lemma" from [10] does. The proof of the following statement can be found in Section 5.

Proposition 2.2. *Assume that* (1.3) *is satisfied. Then* (2.8) *holds w.h.p.*

2.4. **Expansion around the equitable solution.** As outlined earlier, now that we know (2.8) we can establish (2.9) by expanding (2.5) around the uniform distribution (2.6). At first glance, this may not seem entirely immediate because (2.8) only appears to fix the variables $(z_i(\sigma))_{i,\sigma}$ of (2.5) that correspond to the variable nodes. But thanks to a certain inherent symmetry property the optimal $\hat{z}_{\chi_1,\ldots,\chi_\ell}$ to go with the check nodes end up being nearly equitable as well. This observation by itself now suffices to show without further ado that

$$\mathbb{E}_{\mathfrak{A}}[\boldsymbol{Z}^2 \cdot \mathbb{1}\{\mathbb{A} \in \mathfrak{O}\}] = O\big(\mathbb{E}_{\mathfrak{A}}[\boldsymbol{Z} \cdot \mathbb{1}\{\mathbb{A} \in \mathfrak{O}\}]^2\big). \tag{2.11}$$

Yet the estimate (2.11) is not quite precise enough to complete the proof of Theorem 1.1. Indeed, to apply Chebyshev's inequality we would need asymptotic equality as in (2.9) rather than just an $O(\cdot)$-bound; Huang [24] faced the same issue in the case $\boldsymbol{d} = \boldsymbol{k}$ constant and q prime. The proof of this seemingly innocuous improvement actually constitutes one of the main technical obstacles that we need to surmount.

As a first step, using a careful local expansion we will show that the dominant contribution to the second moment actually comes from $(z_\ell)_\ell$ such that

$$\sum_{\ell \in \operatorname{supp}\boldsymbol{d}} \mathbb{P}[\boldsymbol{d} = \ell] \sum_{\sigma \in \mathbb{F}_q} |z_\ell(\sigma) - q^{-1}| = O(n^{-1/2}). \tag{2.12}$$

But even once we know (2.12) a critical issue remains because we allow general distributions of degrees $\boldsymbol{d}, \boldsymbol{k}$ and matrix entries $\boldsymbol{\chi}$. In effect, to estimate the kernel size accurately we need to investigate the conceivable frequencies of field values that can lead to solutions. Specifically, for an integer $k_0 \geq 3$ and $\chi_1, \ldots, \chi_{k_0} \in \mathbb{F}_q^*$ let

$$\mathscr{S}_q(\chi_1, \ldots, \chi_{k_0}) = \left\{\sigma \in \mathbb{F}_q^{k_0} : \sum_{i=1}^{k_0} \chi_i \sigma_i = 0\right\} \tag{2.13}$$

comprise all solutions to a linear equation with coefficients $\chi_1, \ldots, \chi_{k_0} \in \mathbb{F}_q$. For each $\sigma \in \mathscr{S}_q(\chi_1, \ldots, \chi_{k_0})$ the vector

$$\hat{\sigma} = \left(\sum_{i=1}^{k_0} \mathbb{1}\{\sigma_i = s\}\right)_{s \in \mathbb{F}_q^*} \in \mathbb{Z}^{\mathbb{F}_q^*} \tag{2.14}$$

tracks the frequencies with which the various non-zero field elements appear. Depending on the coefficients $\chi_1, \ldots, \chi_{k_0}$, the frequency vectors $\hat{\sigma}$ may be confined to a proper sub-grid of the integer lattice. For example, in the case $q = k_0 = 3$ and $\chi_1 = \chi_2 = \chi_3 = 1$ they span the sub-lattice spanned by $\binom{1}{1}$ and $\binom{0}{3}$. The following proposition characterises the lattice spanned by the frequency vectors for general k_0 and $\chi_1, \ldots, \chi_{k_0}$.

Proposition 2.3. *Let $k_0 \geq 3$, let $\chi_1, \ldots, \chi_{k_0} \in \mathbb{F}_q^*$ and let $\mathfrak{M}_q(\chi_1, \ldots, \chi_{k_0}) \subseteq \mathbb{Z}^{\mathbb{F}_q^*}$ be the $\mathbb{Z}$-module generated by the frequency vectors $\hat{\sigma}$ for $\sigma \in \mathscr{S}_q(\chi_1, \ldots, \chi_{k_0})$. Then $\mathfrak{M}_q(\chi_1, \ldots, \chi_{k_0})$ has a basis $\mathfrak{b}_1, \ldots, \mathfrak{b}_{q-1}$ of non-negative integer vectors with $\|\mathfrak{b}_i\|_1 \leq 3$ for all $1 \leq i \leq q-1$ such that $\det(\mathfrak{b}_1 \cdots \mathfrak{b}_{q-1}) = q^{\mathbb{1}\{\chi_1 = \cdots = \chi_{k_0}\}}$.*

A vital feature of Proposition 2.3 is that the module basis consists of non-negative integer vectors with small ℓ_1-norm. In effect, the basis vectors are "combinatorially meaningful" towards our purpose of counting solutions. Perhaps surprisingly, the proof of Proposition 2.3 turns out to be rather delicate, with details depending on whether q is a prime or a prime power, among other things. The details can be found in Section 6.

In addition to the subgrid constraints imposed by the linear equations themselves, we need to take a divisibility condition into account. Indeed, for any assignment $\sigma \in \mathbb{F}_q^n$ of values to variables the frequencies of the various field elements $s \in \mathbb{F}_q$ are divisible by the g.c.d. $\mathfrak{d}$ of $\operatorname{supp}(\boldsymbol{d})$, i.e.

$$\mathfrak{d} \mid \sum_{i=1}^{n} \boldsymbol{d}_i \mathbb{1}\{\sigma_i = s\} \qquad \text{for all } s \in \mathbb{F}_q. \tag{2.15}$$

Thus, to compute the expected kernel size we need to study the intersection of the sub-grid (2.15) with the grid spanned by the frequency vectors $\hat{\sigma}$ for $\sigma \in \mathscr{S}_q(\boldsymbol{\chi}_{1,1},\ldots,\boldsymbol{\chi}_{1,\boldsymbol{k}})$. Specifically, by way of estimating the number of assignments represented by each grid point and calculating the ensuing satisfiability probability, we obtain the following.

Proposition 2.4. *Assume that q and $\mathfrak{d}$ are coprime and that* (1.3) *is satisfied. Then* (2.9) *holds w.h.p.*

We prove Proposition 2.4 in Section 7. Combining Propositions 2.1–2.4, we now establish the main theorem.

Proof of Theorem 1.1. The assumption (1.3) implies that $1 - d/k = \Phi(0) > \Phi(1) = 0$. Combining Propositions 2.2 and 2.4, we obtain (2.8)–(2.9). Hence, Chebyshev's inequality implies that $\boldsymbol{Z} \geq q^{n-\boldsymbol{m}} = q^{n(1-d/k+o(1))} > 0$ w.h.p. Consequently, the random linear system $\mathbb{A}x = \boldsymbol{y}$ has a solution w.h.p., and thus $\mathrm{rk}\,\mathbb{A} = \boldsymbol{m}$ w.h.p. □

Proof of Corollary 1.2. Let q be a prime that does not divide $\mathfrak{d}$ and let $\boldsymbol{\chi} = 1$ deterministically. Obtain the matrix $\bar{\mathbb{B}} \in \mathbb{F}_q^{\boldsymbol{m}\times n}$ by reading the $\{0,1\}$-entries of $\mathbb{B}$ as elements of $\mathbb{F}_q$. Then the distribution of $\bar{\mathbb{B}}$ coincides with the distribution of the random $\mathbb{F}_q$-matrix $\mathbb{A}$. Hence, Theorem 1.1 implies that $\bar{\mathbb{B}}$ has full row rank w.h.p.

Suppose that indeed $\mathrm{rk}\,\bar{\mathbb{B}} = \boldsymbol{m}$. We claim that then the rows of $\mathbb{B}$ are linearly independent. Indeed, assume that $z^\top\mathbb{B} = 0$ for some vector $z = (z_1,\ldots,z_{\boldsymbol{m}})^\top \in \mathbb{Z}^{\boldsymbol{m}}$. Factoring out $\gcd(z_1,\ldots,z_{\boldsymbol{m}})$ if necessary, we may assume that the vector $\bar{z} \in \mathbb{F}_q^{\boldsymbol{m}}$ with entries $\bar{z}_i = z_i + q\mathbb{Z}$ is non-zero. Since $z^\top\mathbb{B} = 0$ implies that $\bar{z}^\top\bar{\mathbb{B}} = 0$, the rows of $\bar{\mathbb{B}}$ are linearly dependent, in contradiction to our assumption that $\bar{\mathbb{B}}$ has full row rank. □

2.5. **Discussion and related work.** The present proof strategy draws on the prior work [6, 10] on the rank of random matrices. Specifically, toward the proof of Proposition 2.1 we extend the Aizenman-Sims-Starr technique from [10] and to prove Proposition 2.2 we generalise an argument from [6]. Additionally, the expansion around the centre carried out in the proof of Proposition 2.4 employs some of the techniques developed in the study of satisfiability thresholds, particularly the extensive use of local limit theorems and auxiliary probability spaces [12, 13].

The principal new proof ingredient is the asymptotically precise analysis of the second moment by means of the study of the sub-grids of the integer lattice induced by the constraints as sketched in Section 2.4. This issue that was absent in the prior literature on variations on random k-XORSAT [6, 10, 15] and on other random constraint satisfaction problems [12, 13]. However, in the study of the random regular matrix from Example 1.5 Huang [24] faced a similar issue in the special case $\boldsymbol{d} = \boldsymbol{k}$ constant and $\boldsymbol{\chi} = 1$ deterministically. Proposition 2.3, whose proof is based on a combinatorial investigation of lattices in the general case, constitutes a generalisation of the case Huang studied. A further feature of Proposition 2.3 absent in [24] is the explicit ℓ_1-bound on the basis vectors. This bound facilitates the proof of Proposition 2.4, which ultimately carries out the expansion around the equitable solution.

Satisfiability thresholds of random constraint satisfaction problems have been studied extensively in the statistical physics literature via a non-rigorous technique called the "cavity method". The cavity method comes in two installments: the simpler "replica symmetric ansatz" associated with the Belief Propagation message passing scheme, and the more intricate "replica symmetry breaking ansatz". The proof of Theorem 1.1 demonstrates that the former renders the correct prediction as to the satisfiability threshold of random linear equations. By contrast, in quite a few problems, notoriously random k-SAT, replica symmetry breaking occurs [14, 20].

An intriguing question for future work might be to understand the "critical" case of Φ that attain their global max at 0 and another point left open by Theorem 1.1. While Example 1.4 shows that it cannot generally be true that $\mathbb{A}$ has full row rank w.h.p., the regular case where $\boldsymbol{d} = \boldsymbol{k} = d$ are fixed to the same constant provides an intriguing example. For this scenario Huang proved that the random $\{0,1\}$-matrix $\mathbb{B}$ has full rank w.h.p. [24]. The proof, based effectively on a moment computation over finite fields and local limit techniques, also applies to the adjacency matrices of random d-regular graphs.

While the present paper deals with sparse random matrices with a bounded average number of non-zero entries in each row and column, the case of dense random matrices has received a great deal of attention, too. Komlós [30] first shows that dense square random $\{0,1\}$-matrices are regular over the rationals w.h.p.; Vu [46] suggested an alternative proof. The computation of the exponential order of the singularity probability subsequently led to a series of intriguing articles [26, 44, 45]. By contrast, the singularity probability of a dense square matrix over a finite field converges to a value strictly between zero and one [31, 32, 34, 35].

Apart from the sparse and dense case, the regime of intermediate densities has been studied as well. Balakin [7] and Blömer, Karp and Welzl [8] dealt with the rank of such random matrices of intermediate densities over finite

fields. In addition, Costello and Vu [16, 17] studied the rational rank of random symmetric matrices of an intermediate density.

Indeed, an interesting open problem appears to be the extension of the present methods to the symmetric case. In particular, it would be interesting to see if the present techniques can be used to add to the line of works on the adjacency matrices of random graphs, which have been approached by means of techniques based on local weak convergence or Littlewood-Offord techniques [9, 22].

2.6. **Organisation.** After some preliminaries in Section 3 we begin with the proof of Proposition 2.1 in Section 4. The proof relies on an Aizenman-Sims-Starr coupling argument, some details of which are deferred to Section 8. Section 5 deals with the proof of Proposition 2.2. Subsequently we prove Proposition 2.3 in Section 6, thereby laying the ground for the proof of Proposition 2.4 in Section 7.

3. Preliminaries

Unsurprisingly, the proofs of the main results involve a few concepts and ideas from linear algebra. We mostly follow the terminology from [10], summarised in the following definition.

Definition 3.1 ([10, Definition 2.1])**.** *Let A be an $m \times n$-matrix over a field $\mathbb{F}$.*

- *A set $\emptyset \neq I \subseteq [n]$ is a **relation** of A if there exists a row vector $y \in \mathbb{F}^{1\times m}$ such that $\emptyset \neq \operatorname{supp}(yA) \subseteq I$.*
- *If $I = \{i\}$ is a relation of A, then we call i **frozen** in A. Let $\mathfrak{F}(A)$ be the set of all frozen $i \in [n]$ and let*

$$\mathfrak{f}(A) = |\mathfrak{F}(A)|/n.$$

- *A set $I \subseteq [n]$ is a **proper relation** of A if $I \setminus \mathfrak{F}(A)$ is a relation of A.*
- *For $\delta > 0$, $\ell \geq 1$ we say that A is (δ, ℓ)-**free** if there are no more than δn^ℓ proper relations $I \subseteq [n]$ of size $|I| = \ell$.*

Thus, a relation is set of column indices such that the support of a non-zero linear combination yA of rows of A is contained in that set of indices. Of course, every single row induces a relation on the column indices where it has non-zero entries. An important special case is a relation consisting of one coordinate i only. If such a relation exists, then $x_i = 0$ for all vectors $x \in \ker A$, which is why we call such a coordinate i frozen. Furthermore, a proper relation is a relation that is not just built up of frozen variables. Finally, we introduce the term (δ, ℓ)-free to express that A has "relatively few" relations of size ℓ as we will generally employ this term for bounded ℓ and small $\delta > 0$.

The following observation will aid the Aizenman-Sims-Starr coupling argument, where we will need to study the effect of adding a few extra rows and columns to a random matrix.

Lemma 3.2 ([10, Lemma 2.4])**.** *Let A, B, C be matrices of size $m \times n$, $m' \times n$ and $m' \times n'$, respectively, and let $I \subseteq [n]$ be the set of all indices of non-zero columns of B. Moreover, obtain B_* from B by replacing for each $i \in I \cap \mathfrak{F}(A)$ the i-th column of B by zero. Unless I is a proper relation of A we have*

$$\operatorname{nul}\begin{pmatrix} A & 0 \\ B & C \end{pmatrix} - \operatorname{nul} A = n' - \operatorname{rk}(B_* \; C). \tag{3.1}$$

Apart from Lemma 3.2 we will harness an important trick called the "pinning operation". The key insight is that for *any* given matrix we can diminish the number of short proper relations by simply expressly freezing a few random coordinates. The basic idea behind the pinning operation goes back to the work of Montanari [39] and has been used in other contexts [11, 42]. The version of the construction that we use here goes as follows.

Definition 3.3 ([10, Definition 2.2])**.** *Let A be an $m \times n$ matrix and let $\theta \geq 0$ be an integer. Let $\boldsymbol{i}_1, \boldsymbol{i}_2, \ldots, \boldsymbol{i}_\theta \in [n]$ be uniformly random and mutually independent column indices. Then the matrix $A[\theta]$ is obtained by adding θ new rows to A such that for each $j \in [\theta]$ the j-th new row has precisely one non-zero entry, namely a one in the $\boldsymbol{i}_j$-th column.*

Proposition 3.4 ([10, Proposition 2.3])**.** *For any $\delta > 0$, $\ell > 0$ there exists $\Theta_0 = \Theta_0(\delta, \ell) > 0$ such that for all $\Theta > \Theta_0$ and for any matrix A over any field $\mathbb{F}$ the following is true. With $\boldsymbol{\theta} \in [\Theta]$ chosen uniformly at random we have $\mathbb{P}\left[A[\boldsymbol{\theta}] \text{ is } (\delta, \ell)\text{-free}\right] > 1 - \delta$.*

As a fairly immediate application of Proposition 3.4 we conclude that if the pinning operation applied to a random matrix over a finite field leaves us with few frozen variables, a decorrelation condition akin to the event $\mathfrak{O}$ from (2.7) will be satisfied. For a matrix A we continue to denote by $\boldsymbol{x}_A$ a random vector from $\ker A$.

Corollary 3.5 ([10, Lemma 4.2]). *For any $\zeta > 0$ and any prime power $q > 0$ there exist $\xi > 0$ and $\Theta_0 > 0$ such that for any $\Theta > \Theta_0$ for large enough n the following is true. Let A be a $m \times n$-matrix over $\mathbb{F}_q$. Suppose that for a uniformly random $\boldsymbol{\theta} \in [\Theta]$ we have $\mathbb{E}|\mathfrak{F}(A[\boldsymbol{\theta}])| < \xi n$. Then*

$$\sum_{\sigma,\tau\in\mathbb{F}_q}\sum_{i,j=1}^{n}\mathbb{E}\left|\mathbb{P}\left[\boldsymbol{x}_i=\sigma,\boldsymbol{x}_j=\tau \mid A[\boldsymbol{\theta}]\right]-q^{-2}\right|<\zeta n^2.$$

As mentioned earlier, at a key junction of the moment computation we will need to estimate the number of integer lattice points that satisfy certain linear relations. The following elementary estimate will prove useful.

Lemma 3.6. [33, p. 135] *Let $\mathfrak{M} \subseteq \mathbb{R}^\ell$ be a $\mathbb{Z}$-module with basis $b_1, \ldots, b_\ell$. Then*

$$\lim_{r\to\infty}\frac{|\{x\in\mathfrak{M}:\|x\|\le r\}|}{\mathrm{vol}\left(\{x\in\mathbb{R}^\ell:\|x\|\le r\}\right)}=\frac{1}{|\det(b_1\cdots b_\ell)|}.$$

The definition of the random Tanner graph in Section 1.2.1 provides that $\mathbb{G}$ is simple. Commonly it is easier to conduct proofs for an auxiliary random multigraph drawn from a pairing model and then lift the results to the simple random graph. This is how we proceed as well. Thus, given (1.1) we let $\boldsymbol{G}$ be the random bipartite graph on the set $\{x_1, \ldots, x_n\}$ of variable nodes and $\{a_1, \ldots, a_{\boldsymbol{m}}\}$ of check nodes generated by drawing a perfect matching $\boldsymbol{\Gamma}$ of the complete bipartite graph on

$$\bigcup_{i=1}^{n}\{x_i\}\times[\boldsymbol{d}_i]\qquad\text{and}\qquad\bigcup_{i=1}^{\boldsymbol{m}}\{a_i\}\times[\boldsymbol{k}_i]$$

and contracting the sets $x_i \times [\boldsymbol{d}_i]$ and $a_i \times [\boldsymbol{k}_i]$ of variable/check clones. We also let $\boldsymbol{A}$ be the random matrix to go with this random multi-graph. Hence,

$$\boldsymbol{A}_{ij}=\boldsymbol{\chi}_{i,j}\sum_{u=1}^{\boldsymbol{k}_i}\sum_{v=1}^{\boldsymbol{d}_j}\mathbb{1}\{\{(a_i,u),(x_j,v)\}\in\boldsymbol{\Gamma}\}\ .$$

Routine arguments show that $\boldsymbol{G}$ is simple with a non-vanishing probability.

Proposition 3.7 ([10, Lemma 4.3]). *We have $\mathbb{P}\left[\boldsymbol{G}\text{ is simple}\mid\sum_{i=1}^{n}\boldsymbol{d}_i=\sum_{i=1}^{\boldsymbol{m}}\boldsymbol{k}_i\right]=\Omega(1)$.*

When working with the random graphs $\mathbb{G}$ or $\boldsymbol{G}$ we occasionally encounter the size-biased versions $\hat{\boldsymbol{d}}, \hat{\boldsymbol{k}}$ of the degree distributions defined by

$$\mathbb{P}\left[\hat{\boldsymbol{d}}=\ell\right]=\ell\mathbb{P}\left[\boldsymbol{d}=\ell\right]/d,\qquad\mathbb{P}\left[\hat{\boldsymbol{k}}=\ell\right]=\ell\mathbb{P}\left[\boldsymbol{k}=\ell\right]/k\qquad(\ell\ge0).\tag{3.2}$$

In particular, these distributions occur in the Aizenman-Sims-Starr coupling argument. In that context we will also need the following crude but simple tail bound.

Lemma 3.8 ([10, Lemma 1.8]). *Let $(\boldsymbol{\lambda}_i)_{i\ge1}$ be a sequence of independent copies of an integer–valued random variable $\boldsymbol{\lambda} \ge 0$ with $\mathbb{E}\left[\boldsymbol{\lambda}^r\right] < \infty$ for some $r > 2$. Further, let s be a sequence such that $s = \Theta(n)$. Then for all $\delta > 0$,*

$$\mathbb{P}\left[\left|\sum_{i=1}^{s}(\boldsymbol{\lambda}_i-\mathbb{E}\left[\boldsymbol{\lambda}\right])\right|>\delta n\right]=o(1/n).$$

Finally, throughout the article we use the common $O(\cdot)$-notation to refer to the limit $n \to \infty$. In addition, we will sometimes need to deal with another parameter $\varepsilon > 0$. In such cases we use $O_\varepsilon(\cdot)$ and similar symbols to refer to the double limit $\varepsilon \to 0$ after $n \to \infty$.

4. Proof of Proposition 2.1

4.1. **Overview.** The first ingredient of the proof of Proposition 2.1 is a coupling argument inspired by the Aizenman-Sims-Starr scheme from mathematical physics [5], which also constituted the main ingredient of the proof of the approximate rank formula (1.4) from [10]. Indeed, the coupling argument here is quite similar to that from [10], with some extra bells and whistles to accommodate the additional ternary equations. We therefore defer that part of the proof to Section 8. The Aizenman-Sims-Starr argument leaves us with a variational formula for the rank of $\mathbb{A}_{\lfloor\delta n\rfloor}$. The second proof ingredient is to solve this variational problem. Harnessing the assumption (1.3), we will obtain the explicit expression for the rank provided by Proposition 2.1.

Let us come to the details. As explained in Section 3, we will have an easier time working with the pairing model versions $\boldsymbol{G}, \boldsymbol{A}$ of the Tanner graph and the random matrix. Moreover, to facilitate the coupling argument we will

need to poke a few holes, known as "cavities" in physics jargon, into the random matrix. More precisely, we will slightly reduce the number of check nodes and tolerate a small number of variable nodes x_i of degree less than $\boldsymbol{d}_i$. The cavities will provide the flexibility needed to set up the coupling argument.

Formally, let $\varepsilon, \delta \in (0,1)$ and let $\Theta \geq 0$ be an integer. Ultimately Θ will depend on ε but not on n or δ. We then construct the random matrix $\boldsymbol{A}[n, \varepsilon, \delta, \Theta]$ as follows. Let

$$\boldsymbol{m}_\varepsilon \sim \mathrm{Po}((1-\varepsilon) d n/k), \qquad \boldsymbol{m}_\delta \sim \mathrm{Po}(\delta n), \qquad \boldsymbol{\theta} \sim \mathrm{unif}([\Theta]). \tag{4.1}$$

The Tanner multigraph $\boldsymbol{G}[n, \varepsilon, \delta, \Theta]$ has variable nodes $x_1, \ldots, x_n$ and check nodes $a_1, \ldots, a_{\boldsymbol{m}_\varepsilon}, t_1, \ldots, t_{\boldsymbol{m}_\delta}, p_1, \ldots, p_{\boldsymbol{\theta}}$. To connect them draw a random maximum matching $\boldsymbol{\Gamma}[n, \varepsilon]$ of the complete bipartite graph with vertex classes

$$V_1 = \bigcup_{i=1}^{\boldsymbol{m}_\varepsilon} \{a_i\} \times [\boldsymbol{k}_i] \qquad \text{and} \qquad V_2 = \bigcup_{j=1}^{n} \{x_j\} \times [\boldsymbol{d}_j].$$

For every matching edge $\{(a_i, h), (x_j, \ell)\} \in \boldsymbol{\Gamma}[n, \varepsilon]$, $h \in [\boldsymbol{k}_i]$, $\ell \in [\boldsymbol{d}_j]$, between a clone of x_h and a clone of a_i we insert an a_i-x_j-edge into $\boldsymbol{G}[n, \varepsilon, \delta, \Theta]$. Moreover, the check nodes $t_1, \ldots, t_{\boldsymbol{m}_\delta}$ each independently choose three neighboring variables uniformly with replacement random among $\{x_1, \ldots, x_n\}$. Further, check node p_ℓ for $\ell \in [\boldsymbol{\theta}]$ is adjacent to x_ℓ only. Finally, to obtain the random $(\boldsymbol{\theta} + \boldsymbol{m}_\varepsilon + \boldsymbol{m}_\delta) \times n$-matrix $\boldsymbol{A}[n, \varepsilon, \delta, \Theta]$ from $\boldsymbol{G}[n, \varepsilon, \delta, \Theta]$ we let

$$\boldsymbol{A}[n, \varepsilon, \delta, \Theta]_{p_i, x_h} = \mathbb{1}\{i = h\} \qquad (i \in [\boldsymbol{\theta}], h \in [n]), \tag{4.2}$$

$$\boldsymbol{A}[n, \varepsilon, \delta, \Theta]_{a_i, x_h} = \boldsymbol{\chi}_{i,h} \sum_{\ell=1}^{\boldsymbol{k}_i} \sum_{s=1}^{\boldsymbol{d}_h} \mathbb{1}\{(x_h, s), (a_i, \ell)\} \in \boldsymbol{\Gamma}[n, \varepsilon]\} \qquad (i \in [\boldsymbol{m}_\varepsilon], h \in [n]), \tag{4.3}$$

$$\boldsymbol{A}[n, \varepsilon, \delta, \Theta]_{t_i, x_h} = \boldsymbol{\chi}_{\boldsymbol{m}_\varepsilon + i, h} \sum_{\ell=1}^{3} \mathbb{1}\{\boldsymbol{i}_{i,\ell} = h\} \qquad (i \in [\boldsymbol{m}_\delta], h \in [n]). \tag{4.4}$$

Applying the Aizenman-Sims-Starr scheme to the matrix $\boldsymbol{A}[n, \varepsilon, \delta, \Theta]$, we obtain the following variational bound.

Proposition 4.1. *There exist $\delta_0 > 0$, $\Theta_0(\varepsilon) > 0$ such that for all $0 < \delta < \delta_0$ and any $\Theta = \Theta(\varepsilon) \geq \Theta_0(\varepsilon)$ we have*

$$\limsup_{\varepsilon \to 0} \limsup_{n \to \infty} \frac{1}{n} \mathbb{E}[\mathrm{nul}(\boldsymbol{A}[n, \varepsilon, \delta, \Theta])] \leq \max_{\alpha, \beta \in [0,1]} \Phi(\alpha) + \left(\exp\left(-3\delta\beta^2\right) - 1\right) D(1 - K'(\alpha)/k) - \delta + 3\delta\beta^2 - 2\delta\beta^3. \tag{4.5}$$

The proof of Proposition 4.1, carried out in Section 8 in detail, resembles that of the rank formula (1.4), except that we have to accommodate the additional ternary checks t_i. Their presence is the reason why the optimisation problem on the r.h.s. comes in terms of two variables α, β rather than a single variable as (1.4).

To complete the proof of Proposition 2.1 we need to solve the optimisation problem (4.5). This is the single place where we require that $\Phi(z)$ take its unique global max at $z = 0$, which ultimately implies that the optimiser of (4.5) is $\alpha = \beta = 0$. This fact in turn implies the following.

Proposition 4.2. *For any $\boldsymbol{d}, \boldsymbol{k}$ that satisfy* (1.3) *there exists $\delta_0 > 0$ such that for all $0 < \delta < \delta_0$ we have*

$$\max_{\alpha, \beta \in [0,1]} \Phi(\alpha) + \left(\exp\left(-3\delta\beta^2\right) - 1\right) D(1 - K'(\alpha)/k) - \delta + 3\delta\beta^2 - 2\delta\beta^3 = 1 - \frac{d}{k} - \delta.$$

The proof of Proposition 4.2 can be found in Section 4.2. Finally, in Section 4.3 we will see that Proposition 2.1 is an easy consequence of Propositions 4.1 and 4.2.

4.2. **Proof of Proposition 4.2.** Let

$$\tilde{\Phi}_\delta(\alpha, \beta) = \Phi(\alpha) + \left(\exp\left(-3\delta\beta^2\right) - 1\right) D(1 - K'(\alpha)/k) - \delta + 3\delta\beta^2 - 2\delta\beta^3 \qquad (\alpha, \beta \in [0,1]).$$

Assuming (1.3), we are going to prove that for small enough δ,

$$\max_{\alpha, \beta \in [0,1]} \tilde{\Phi}_\delta(\alpha, \beta) = \tilde{\Phi}_\delta(0,0) = 1 - \frac{d}{k} - \delta, \tag{4.6}$$

whence the assertion is immediate.

The C^1-function $\tilde{\Phi}_\delta$ attains its maximum either at a boundary point of the compact domain $[0,1]^2$ or at a point where the partial derivatives vanish. Beginning with the former, we consider four cases.

Case 1: $\alpha = 0$**:** we have

$$\tilde{\Phi}_\delta(0,\beta) = \tilde{\Phi}_\delta(0,0) + 3\delta\beta^2 - 2\delta\beta^3 - (1-\exp\left(-3\delta\beta^2\right)). \tag{4.7}$$

Expanding the exponential function, we see that $3\delta\beta^2 - 2\delta\beta^3 - (1-\exp\left(-3\delta\beta^2\right)) = -2\delta\beta^3 + O_\delta(\delta^2\beta^4)$. Since $-2\delta\beta^3 + O_\delta(\delta^2\beta^4)$ is non-positive for all $\beta \in [0,1]$, (4.7) yields $\max_\beta \tilde{\Phi}_\delta(0,\beta) = \tilde{\Phi}_\delta(0,0)$ for small enough $\delta > 0$.

Case 2: $\beta = 0$**:** the assumption (1.3) ensures that Φ is maximised in 0. Therefore, as $\tilde{\Phi}_\delta(\alpha,0) = \Phi(\alpha) - \delta$, the maximum on $\{(\alpha,0) : \alpha \in [0,1]\}$ is attained in $\alpha = 0$.

Case 3: $\alpha = 1$**:** we obtain

$$\tilde{\Phi}_\delta(1,\beta) = \Phi(1) - \delta + 3\delta\beta^2 - 2\delta\beta^3 = \delta(3\beta^2 - 2\beta^3 - 1).$$

Since $-2\beta^3 + 3\beta^2 \le 1$ for all $\beta \in [0,1]$ and $d/k < 1$, for small enough δ we obtain $\tilde{\Phi}_\delta(1,\beta) \le 1 - d/k - \delta = \tilde{\Phi}_\delta(0,0)$.

Case 4: $\beta = 1$**:** we have

$$\tilde{\Phi}_\delta(\alpha,1) = \Phi(\alpha) - (1-\exp(-3\delta))D\left(1 - \frac{K'(\alpha)}{k}\right). \tag{4.8}$$

Because D and K' are continuous on $[0,1]$ due to the assumption $\mathbb{E}[\boldsymbol{d}^2] + \mathbb{E}[\boldsymbol{k}^2] < \infty$, for any $\zeta > 0$ there exists $\hat{\alpha} > 0$ such that $D(1-K'(\alpha)/k) > 1-\zeta$ for all $0 < \alpha < \hat{\alpha}$. Therefore, (4.8) shows that for small enough $\delta > 0$ and $0 < \alpha < \hat{\alpha}$ we have $\tilde{\Phi}_\delta(\alpha,1) < \tilde{\Phi}_\delta(\alpha,0) \le \tilde{\Phi}_\delta(0,0)$. On the other hand, for $\hat{\alpha} \le \alpha \le 1$ the difference $\Phi(\alpha) - \Phi(0)$ is uniformly negative because of our assumption (1.3) that Φ attains its unique global maximum at $\alpha = 0$. Hence, for δ small enough and $\hat{\alpha} \le \alpha \le 1$ we obtain $\tilde{\Phi}_\delta(\alpha,1) < \tilde{\Phi}_\delta(0,0)$.

Combining Cases 1–4, we obtain

$$\max_{(\alpha,\beta)\in\partial[0,1]^2} \tilde{\Phi}_\delta(\alpha,\beta) = \tilde{\Phi}_\delta(0,0). \tag{4.9}$$

Moving on to the interior of $[0,1]^2$, we calculate the derivatives

$$\frac{\partial\tilde{\Phi}_\delta}{\partial\alpha} = \Phi'(\alpha) + \left(1-\exp\left(-3\delta\beta^2\right)\right)\frac{K''(\alpha)}{k}D'(1-K'(\alpha)/k) = \frac{K''(\alpha)}{k}\left(d(1-\alpha) - \exp\left(-3\delta\beta^2\right)D'(1-K'(\alpha)/k)\right),$$
$$\frac{\partial\tilde{\Phi}_\delta}{\partial\beta} = 6\delta\beta\left(1-\beta-\exp\left(-3\delta\beta^2\right)D(1-K'(\alpha)/k)\right).$$

Hence, potential maximisers (α,β) in the interior of $[0,1]^2$ satisfy

$$d(1-\alpha) = D'(1-K'(\alpha)/k)\exp\left(-3\delta\beta^2\right) \qquad \text{and} \qquad 1-\beta = \exp\left(-3\delta\beta^2\right)D(1-K'(\alpha)/k). \tag{4.10}$$

Substituting (4.10) into $\tilde{\Phi}_\delta$, we obtain

$$\begin{aligned}\tilde{\Phi}_\delta(\alpha,\beta) &= \Phi(\alpha) - \delta + \left(\exp\left(-3\delta\beta^2\right)-1\right)D(1-K'(\alpha)/k) + 3\delta\beta^2 - 2\delta\beta^3\\ &= \Phi(\alpha) - \delta + (1-\beta)(1-\exp\left(3\delta\beta^2\right)) + 3\delta\beta^2 - 2\delta\beta^3\\ &\le \Phi(\alpha) - \delta - 3\delta\beta^2(1-\beta) + 3\delta\beta^2 - 2\delta\beta^3 = \Phi(\alpha) - \delta + \delta\beta^3.\end{aligned} \tag{4.11}$$

To estimate the r.h.s. we consider the cases of small and large α separately. Specifically, by continuity for any $\zeta > 0$ there is $0 < \hat{\alpha} < \delta$ such that $D(1-K'(\alpha)/k) > 1-\zeta$ for all $0 < \alpha < \hat{\alpha}$.

Case 1: $0 < \alpha < \hat{\alpha}$**:** Since $D(1-K'(\alpha)/k) > 1-\zeta$, (4.10) implies that for $\beta > 0$

$$1-\beta > (1-3\delta\beta^2)(1-\zeta) = 1-\zeta-3\delta\beta^2(1-\zeta).$$

In particular, small $\hat{\alpha}$ implies that also β is small. More precisely, after choosing δ,ζ small enough, we may assume that $\beta < \hat{\beta}$ for any fixed $\hat{\beta} > 0$. In this case, we may thus restrict to solutions $(\alpha,\beta) \in (0,1)^2$ to (4.10) where *both* coordinates are sufficiently small. Also here, we distinguish three cases that all lead to contradictions.

(A) If the solution satisfies $\alpha = \beta$, consider the function

$$x \mapsto 1 - x - \exp\left(-3\delta x^2\right)D(1-K'(x)/k)$$

whose zeros determine the solutions to the right equation in (4.10) under the assumption $\alpha = \beta$. Its value is zero at $x = 0$ and it has derivative

$$-1 + 6\delta x \exp\left(-3\delta x^2\right) D(1 - K'(x)/k) + \exp\left(-3\delta x^2\right) D'(1 - K'(x)/k) \frac{K''(x)}{k},$$

which is negative in a neighbourhood of $x = 0$. Thus (α, α) cannot be a solution to (4.10) for $\alpha \in (0, \hat{\alpha})$.

(B) Assume now that $\alpha < \beta$. Then the right equation of (4.10) yields

$$1 - \beta > \exp\left(-3\delta\beta^2\right) D\left(1 - K'(\beta)/k\right) > \left(1 - 3\delta\beta^2\right)\left(1 - \frac{d}{k} K'(\beta)\right).$$

Now since $\boldsymbol{k} \geq 3$, $K'(\beta) = O_\beta(\beta^2)$. But then the above equation yields a contradiction for β small enough and thus $(\alpha, \beta) \in (0, \hat{\alpha}) \times (0, \hat{\beta})$ with $\alpha < \beta$ is no possible solution.

(C) Finally, if $\alpha > \beta$, the left equation of (4.10) yields

$$d(1 - \alpha) > \exp\left(-3\delta\alpha^2\right) D'\left(1 - K'(\alpha)/k\right) > d\left(1 - 3\delta\alpha^2\right)\left(1 - \frac{\mathbb{E}\left[\boldsymbol{d}^2\right]}{dk} K'(\alpha)\right).$$

Now since $\boldsymbol{k} \geq 3$, $K'(\beta) = O_\beta(\beta^2)$. But then the above equation yields a contradiction for β small enough and thus $(\alpha, \beta) \in (0, \hat{\alpha}) \times (0, \hat{\beta})$ with $\alpha > \beta$ is no possible solution.

Hence, (4.10) has no solution with $0 < \alpha < \hat{\alpha}$.

Case 2: $\hat{\alpha} \leq \alpha < 1$: because $\Phi(\alpha) < \Phi(0)$ for all $0 < \alpha \leq 1$, (4.11) shows that we can choose δ small enough so that $\tilde{\Phi}_\delta(\alpha, \beta) < \tilde{\Phi}_\delta(0, 0)$ for all $\alpha \geq \hat{\alpha}$ and all $\beta \in [0, 1]$.

Combining both cases and recalling (4.9), we obtain (4.6).

4.3. **Proof of Proposition 2.1.** Combining Propositions 4.1 and 4.2, we see that

$$\frac{1}{n}\mathbb{E}\left[\mathrm{nul}(\boldsymbol{A}[n, \varepsilon, \delta, \Theta])\right] \leq 1 - \frac{d}{k} - \delta + o_\varepsilon(1). \tag{4.12}$$

The only (small) missing piece is that we still need to extend this result to the original random matrix $\mathbb{A}_{[\lfloor \delta n \rfloor]}$ based on the simple random factor graph $\mathbb{G}$. To this end we apply the following lemma.

Lemma 4.3 ([10, Lemma 4.8])**.** *For any fixed $\Theta > 0$ there exists a coupling of $\boldsymbol{A}$ and $\boldsymbol{A}[n, \varepsilon, 0, \Theta]$ such that*

$$\mathbb{E}\left|\operatorname{nul} \boldsymbol{A} - \operatorname{nul} \boldsymbol{A}[n, \varepsilon, 0, \Theta]\right| = O_\varepsilon(\varepsilon n).$$

Let $\boldsymbol{A}_{[\lfloor \delta n \rfloor]}$ be the matrix obtained from $\boldsymbol{A}$ by adding $\lfloor \delta n \rfloor$ random ternary equations. Combining (4.12) with Lemma 4.3 and observing that each of the unary checks p_i can alter the nullity by at most one, we obtain

$$\frac{1}{n}\mathbb{E}\left[\mathrm{nul}(\boldsymbol{A}_{[\lfloor \delta n \rfloor]})\right] \leq 1 - \frac{d}{k} - \delta + o(1). \tag{4.13}$$

Furthermore, since changing a single edge of the Tanner graph $\boldsymbol{G}$ or a single entry of $\boldsymbol{A}$ can change the rank by at most one, the Azuma–Hoeffding inequality shows that $\mathrm{nul}(\boldsymbol{A}_{[\lfloor \delta n \rfloor]})$ is tightly concentrated. Thus, (4.13) implies

$$\mathbb{P}\left[\frac{1}{n}\mathrm{nul}(\boldsymbol{A}_{[\lfloor \delta n \rfloor]}) \leq 1 - \frac{d}{k} - \delta + o(1)\right] = 1 - o(1/n). \tag{4.14}$$

Finally, combining (4.14) with Lemma 3.7, we conclude that

$$\mathbb{P}\left[\frac{1}{n}\mathrm{nul}(\mathbb{A}_{[\lfloor \delta n \rfloor]}) \leq 1 - \frac{d}{k} - \delta + o(1)\right] = 1 - o(1/n),$$

which implies the assertion because $\mathrm{nul}(\mathbb{A}_{[\lfloor \delta n \rfloor]}) \leq n$ deterministically.

5. Proof of Proposition 2.2

We recall that $\boldsymbol{A}$ is the random $\boldsymbol{m} \times n$-matrix generated by way of the pairing model. Moreover, we continue to let $\boldsymbol{A}[n, \varepsilon, \delta, \Theta]$ be the matrix from Section 4 with $\boldsymbol{m}_\varepsilon \sim \mathrm{Po}((1 - \varepsilon) dn/k)$ checks with independent degrees $\boldsymbol{k}_i$, another $\boldsymbol{m}_\delta \sim \mathrm{Po}(\delta n)$ ternary checks and further $\boldsymbol{\theta} \sim \mathrm{unif}([\Theta])$ unary checks (cf. (4.1)). Lemma 4.3 shows that the nullity of the second model approaches that of the first as $\varepsilon \to 0$.

We now go on to prove that if the matrix $\boldsymbol{A}[\boldsymbol{\theta}_0]$ obtained from $\boldsymbol{A}$ by adding a few random unary checks has many frozen coordinates, then the nullity of $\boldsymbol{A}[n, \varepsilon, \delta, \Theta]$ would be greater than permitted by Proposition 2.1; we

use an argument similar to [6, proof of Proposition 2.7]. Invoking Corollary 3.5 will then complete the proof of Proposition 2.2.

Lemma 5.1. *Assume that for some $\Theta_0 > 0$ and $\boldsymbol{\theta}_0 \sim \mathrm{unif}([\Theta_0])$ we have*

$$\limsup_{n\to\infty} \frac{1}{n}\mathbb{E}\,|\mathfrak{F}(\boldsymbol{A}[\boldsymbol{\theta}_0])| > 0.$$

Then for any $\delta_0 > 0$ there exists $0 < \delta < \delta_0$ and $\Theta_1 = \Theta_1(\varepsilon)$ such that for any $\Theta = \Theta(\varepsilon) > \Theta_1(\varepsilon)$ we have

$$\limsup_{\varepsilon\to 0}\limsup_{n\to\infty} \frac{1}{n}\mathbb{E}\,[\mathrm{nul}(\boldsymbol{A}\,[n,\varepsilon,\delta,\Theta])] > 1 - \frac{d}{k} - \delta.$$

Proof. For an integer $\ell \geq 0$ obtain $\boldsymbol{A}_{[\ell]}[\boldsymbol{\theta}_0]$ from $\boldsymbol{A}[\boldsymbol{\theta}_0]$ by adding ℓ random ternary equations. Moreover, let $\boldsymbol{\lambda} = \mathrm{Po}(\delta n)$. Since $\mathrm{nul}\,\boldsymbol{A}_{[\boldsymbol{\lambda}]}[\boldsymbol{\theta}_0] \geq \mathrm{nul}\,\boldsymbol{A} - \boldsymbol{\lambda} - \boldsymbol{\theta}_0$, Lemma 4.3 implies that for any $\Theta = \Theta(\varepsilon)$,

$$\mathbb{E}\left|\mathrm{nul}\,\boldsymbol{A}_{[\boldsymbol{\lambda}]}[\boldsymbol{\theta}_0] - \mathrm{nul}\,\boldsymbol{A}\,[n,\varepsilon,\delta,\Theta]\right| = \mathbb{E}\left|\mathrm{nul}\,\boldsymbol{A}_{[\boldsymbol{\lambda}]}[\boldsymbol{\theta}_0] - \mathrm{nul}\,\boldsymbol{A}\,[n,\varepsilon,0,\Theta]\right| + O_\varepsilon(\delta n) = O_\varepsilon((\varepsilon+\delta)n + \Theta) = O_\varepsilon(\varepsilon n). \quad (5.1)$$

We now estimate the nullity of $\boldsymbol{A}_{[\boldsymbol{\lambda}]}[\boldsymbol{\theta}_0]$ under the assumption that for a large n,

$$\mathbb{P}\,[|\mathfrak{F}(\boldsymbol{A}[\boldsymbol{\theta}_0])| > \zeta n] > \zeta \qquad \text{for some } \zeta > 0. \quad (5.2)$$

Because adding equations can only increase the set of frozen variables, we have $\mathfrak{F}(\boldsymbol{A}_{[\ell]}[\boldsymbol{\theta}_0]) \subseteq \mathfrak{F}(\boldsymbol{A}_{[\ell+1]}[\boldsymbol{\theta}_0])$ for all $\ell \geq 0$. Therefore, (5.2) implies that

$$\mathbb{P}\left[\left|\mathfrak{F}(\boldsymbol{A}_{[\ell]}[\boldsymbol{\theta}_0])\right| > \zeta n\right] > \zeta \qquad \text{for all } \ell \geq 0. \quad (5.3)$$

We now claim that

$$\frac{1}{n}\mathbb{E}\left[\mathrm{nul}\,\boldsymbol{A}_{[\boldsymbol{\lambda}]}[\boldsymbol{\theta}_0]\right] \geq 1 - d/k - \delta + \delta\zeta^4 + o(1). \quad (5.4)$$

To prove (5.4) it suffices to show that for any $\ell \geq 0$,

$$\mathbb{E}\left[\mathrm{nul}\,\boldsymbol{A}_{[\ell+1]}[\boldsymbol{\theta}_0] - \mathrm{nul}\,\boldsymbol{A}_{[\ell]}[\boldsymbol{\theta}_0]\right] \geq \zeta^4 - 1 + o(1). \quad (5.5)$$

Indeed, we obtain (5.4) from (5.5) and the nullity formula $n^{-1}\mathbb{E}[\mathrm{nul}\,\boldsymbol{A}_{[0]}[\boldsymbol{\theta}_0]] = n^{-1}\mathbb{E}[\mathrm{nul}\,\boldsymbol{A}] + o(1) = 1 - d/k + o(1)$ from (1.4) by writing a telescoping sum.

To establish (5.5) we observe that $\mathrm{nul}\,\boldsymbol{A}_{[\ell+1]}[\boldsymbol{\theta}_0] - \mathrm{nul}\,\boldsymbol{A}_{[\ell]}[\boldsymbol{\theta}_0] \geq -1$ because we obtain $\boldsymbol{A}_{[\ell+1]}[\boldsymbol{\theta}_0]$ from $\boldsymbol{A}_{[\ell]}[\boldsymbol{\theta}_0]$ by adding a single ternary equation. Furthermore, if $|\mathfrak{F}(\boldsymbol{A}_{[\ell]}[\boldsymbol{\theta}_0])| \geq \zeta n$, then with probability $\zeta^3 + o(1)$ all three variables of the new ternary equation are frozen in $\boldsymbol{A}_{[\ell]}[\boldsymbol{\theta}_0]$, in which case $\mathrm{nul}\,\boldsymbol{A}_{[\ell+1]}[\boldsymbol{\theta}_0] = \mathrm{nul}\,\boldsymbol{A}_{[\ell]}[\boldsymbol{\theta}_0]$. Hence, (5.4) follows from (5.5), which follows from (5.3). Finally, combining (5.1) and (5.4) completes the proof. □

Proof of Proposition 2.2. The proposition follows from Corollary 3.5 and Lemma 5.1. □

6. Proof of Proposition 2.3

The proof proceeds very differently depending on whether the coefficients $\chi_1,\ldots,\chi_{k_0}$ are identical or not. The following two lemmas summarise the analyses of the two cases.

Lemma 6.1. *For any prime power q and any $\chi \in \mathbb{F}_q^*$ the $\mathbb{Z}$-module $\mathfrak{M}_q(\chi,\chi,\chi)$ possesses a basis $(\mathfrak{b}_1,\ldots,\mathfrak{b}_{q-1})$ of non-negative integer vectors $\mathfrak{b}_i \in \mathbb{Z}^{\mathbb{F}_q^*}$ for all $i \in [q-1]$ such that*

$$\|\mathfrak{b}_i\|_1 \leq 3 \quad \text{and} \quad \sum_{s\in\mathbb{F}_q^*} \mathfrak{b}_{i,s}\,s = 0 \quad \text{for all } i \in [q-1], \text{ and} \quad \det\left(\mathfrak{b}_1 \;\cdots\; \mathfrak{b}_{q-1}\right) = q.$$

Furthermore, for any $k_0 > 3$ we have $\mathfrak{M}_q\underbrace{(\chi,\ldots,\chi)}_{k_0 \text{ times}} = \mathfrak{M}_q(\chi,\chi,\chi)$.

Lemma 6.2. *Suppose that q is a prime power, that $k_0 \geq 3$ and that $\chi_1,\ldots,\chi_{k_0} \in \mathbb{F}_q^*$ satisfy $|\{\chi_1,\ldots,\chi_{k_0}\}| \geq 2$. Then*

$$\mathfrak{M}_q(\chi_1,\ldots,\chi_{k_0}) = \mathbb{Z}^{\mathbb{F}_q^*}.$$

Furthermore, $\mathfrak{M}_q(\chi_1,\ldots,\chi_{k_0})$ possesses a basis $(\mathfrak{b}_1,\ldots,\mathfrak{b}_{q-1})$ of non-negative integer vectors $\mathfrak{b}_i \in \mathbb{Z}^{\mathbb{F}_q^*}$ such that

$$\|\mathfrak{b}_i\|_1 \leq 3 \quad \text{and} \quad \sum_{s\in\mathbb{F}_q^*} \mathfrak{b}_{i,s}\,s = 0 \quad \text{for all } i \in [q-1].$$

Clearly, Proposition 2.3 is an immediate consequence of Lemmas 6.1 and 6.2. We proceed to prove the former in Section 6.1 and the latter in Section 6.2.

6.1. **Proof of Lemma 6.1.** Because we can just factor out any scalar, it suffices to consider the module

$$\mathfrak{M} = \mathfrak{M}_q \underbrace{(1,\dots,1)}_{k_0 \text{ times}}.$$

Being a $\mathbb{Z}$-module, $\mathfrak{M}$ is free, but it is not entirely self-evident that a basis with the additional properties stated in Lemma 6.1 exists. Indeed, while it is easy enough to come up with $q-1$ linearly independent vectors in $\mathfrak{M}$ that all have an ℓ_1-norm bounded by 3, it is more difficult to show that these vectors generate $\mathfrak{M}$. In the proof of Lemma 6.1, we sidestep this difficulty by working with two sets of vectors $\mathscr{B}_1$ and $\mathscr{B}_2$. The first set $\mathscr{B}_1$ is easily seen to generate $\mathfrak{M}$, while $\mathscr{B}_2$ is a set of linearly independent vectors in $\mathfrak{M}$ with ℓ_1-norms bounded by 3. To argue that $\mathscr{B}_2$ generates $\mathfrak{M}$, too, it then suffices to show that the determinant of the change of basis matrix equals one.

To interpret the bases as subsets of $\mathbb{Z}^{q-1}$ rather than $\mathbb{Z}^{\mathbb{F}_q^*}$ in the following, we fix some notation for the elements of $\mathbb{F}_q$. Throughout this section, we let $q = p^\ell$ for a prime p and $\ell \in \mathbb{N}$. If $\ell = 1$, we regard $\mathbb{F}_q$ as the set $\{0,\dots,p-1\}$ with mod p arithmetic. If $\ell \geq 2$, the field elements can be written as

$$\{a_0 + a_1\mathbb{X} + \ldots + a_{\ell-1}\mathbb{X}^{\ell-1} : a_j \in \mathbb{F}_p \text{ for } j = 0,\dots,\ell-1\},$$

with mod $g(\mathbb{X})$ arithmetic for a prime polynomial $g(\mathbb{X}) \in \mathbb{F}_p[\mathbb{X}]$ of degree ℓ. Exploiting this representation of the field elements as polynomials, we define the length $\mathrm{len}(a_0 + a_1\mathbb{X} + \ldots + a_{\ell-1}\mathbb{X}^{\ell-1})$ of an element of $\mathbb{F}_q$ to be the number of its non-zero coefficients. Finally, let

$$\mathbb{F}_q^{(\geq 2)} = \big\{h \in \mathbb{F}_q : \mathrm{len}(h) \geq 2\big\} \tag{6.1}$$

be the set of all elements of $\mathbb{F}_q$ with length at least two. Of course, if $\ell = 1$, $\mathbb{F}_q^{(\geq 2)}$ is empty.

Recall that we view $\mathfrak{M}$ as a subset of $\mathbb{Z}^{\mathbb{F}_q^*}$ that is generated by the vectors

$$\left(\sum_{i=1}^{k_0} \mathbb{1}\{\sigma_i = s\}\right)_{s\in\mathbb{F}_q^*}, \quad \sigma \in \mathscr{S}_0(1,\dots,1).$$

In the above representation, the generators are indexed by $\mathbb{F}_q^*$ rather than by the set $[q-1]$. But to carry out the determinant calculation, it is immensely useful to represent both $\mathscr{B}_1$ and $\mathscr{B}_2$ as matrices with a convenient structure. Hence, there is ambiguity in the choice of a bijection $f : \mathbb{F}_q^* \to \{1,\dots,q-1\}$ that maps the non-zero elements of $\mathbb{F}_q$ to coordinates in $\mathbb{Z}^{\mathbb{F}_q^*}$. To put a clear structure to the matrices in this subsection, we will soon choose f in a particular way. With the above notation, we will from now on fix a bijection f that is monotonically decreasing with respect to the length function on $\mathbb{F}_q^*$: If $\mathrm{len}(h_1) < \mathrm{len}(h_2)$ for $h_1, h_2 \in \mathbb{F}_q^*$, then $f(h_1) > f(h_2)$. More precisely, f maps the $(p-1)^\ell$ elements in $\mathbb{F}_q^*$ of maximal length ℓ to the interval $[(p-1)^\ell]$, the $\ell(p-1)^{\ell-1}$ elements of length $\ell-1$ to the interval $\{(p-1)^\ell+1,\dots,(p-1)^\ell+\ell(p-1)^{\ell-1}\}$, and so on. For elements of length one, we further specify that

$$f(a\mathbb{X}^i) = q-1-(\ell-i)(p-1)+a \quad \text{for } i \in \{0,\dots\ell-1\} \text{ and } a \in [p-1].$$

For our purposes, there is no need to fully specify the values of f within sets of constant length greater than one, but one could follow the lexicographic order, for example. The benefit of such an ordering will become apparent in the next two subsections.

6.1.1. *First basis $\mathscr{B}_1$.* The idea behind the first set $\mathscr{B}_1$ is that it consists of vectors whose coordinates can be easily seen to correspond to element statistics of a valid solution while ignoring the ℓ_1-restriction formulated in Lemma 6.1. We build $\mathscr{B}_1$ from frequency vectors of solutions of the form

$$\Big(a_0 + a_1\mathbb{X} + \ldots + a_{\ell-1}\mathbb{X}^{\ell-1}\Big) + \sum_{i=0}^{\ell-1} a_i \cdot ((p-1)\mathbb{X}^i) = 0.$$

That is, we take any element $a_0 + a_1\mathbb{X} + \ldots + a_{\ell-1}\mathbb{X}^{\ell-1}$ from $\mathbb{F}_q^*$ and cancel it by a linear combination of elements from $\{p-1, (p-1)\mathbb{X}, \dots, (p-1)\mathbb{X}^{\ell-1}\} \subseteq \mathbb{F}_q^*$. Formally, let $e_1,\dots,e_{q-1}$ denote the canonical basis of $\mathbb{Z}^{q-1}$. The set of

$$M_p = \begin{array}{c} \\ 1 \\ 2 \\ \\ \\ \\ \\ \\ p-1 \end{array} \begin{array}{c} \begin{array}{cccccccc} 1 & 2 & & . & . & . & . & p-1 \end{array} \\ \begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & \ddots & & & & \\ & & & & \ddots & & & \\ & & & & & 1 & & \\ 1 & 2 & 3 & & \cdots & & p-2 & p \end{pmatrix} \end{array}.$$

FIGURE 4. The matrix M_p.

statistics of all frequency vectors of the form described above then reads

$$\mathscr{B}_1 = \left\{ e_{f(\sum_{i=0}^{\ell-1} a_i \mathbb{X}^i)} + \sum_{i=0}^{\ell-1} a_i e_{f(-\mathbb{X}^i)} : \sum_{i=0}^{\ell-1} a_i \mathbb{X}^i \in \mathbb{F}_q^* \right\}.$$

A moment of thought shows that $|\mathscr{B}_1| = q-1$. Indeed, it is helpful to notice that for any $h \in \mathbb{F}_q^* \setminus \{-1, \ldots, -\mathbb{X}^{\ell-1}\}$, there is exactly one element with a non-zero position in coordinate $f(h)$, and this coordinate is 1. That is, there is basically exactly one element in $\mathscr{B}_1$ associated with each element of $\mathbb{F}_q^*$. Generally, the elements of $\mathscr{B}_1$ can be ordered to yield a lower triangular matrix M_q. To sketch this matrix, we first consider the case $\ell = 1$. In this case, with our choice of indexing function f, the elements of $\mathscr{B}_1$ can be ordered to give the matrix displayed in Figure 4. For the case of fields of prime order, this basis is already implicitly mentioned in [24].

Note that this reduces to $M_2 = (2)$ in the case $p = 2$. In this representation, rows are indexed by the field elements they represent, while columns are indexed by the field elements they are associated with. For $\ell \geq 2$, we can use the matrix M_p for the compact representation of M_q displayed in Figure 5.

In the matrix M_q, the upper left block is an identity matrix of the appropriate dimension, the upper right is a zero matrix, the lower left is a matrix that only has non-zero entries in rows that correspond to $-1, \ldots, -\mathbb{X}^{\ell-1}$ while the lower right is a block diagonal matrix whose blocks are given by M_p. In particular, M_p is a lower triangular matrix. Because M_p has determinant p the following is immediate.

Claim 6.3. *We have* $\det(M_q) = p^\ell = q$.

Let $\mathfrak{B}_1$ denote the $\mathbb{Z}$-module generated by the elements of $\mathscr{B}_1$. Then the lower triangular structure of M_q also implies the following.

Claim 6.4. *The rank of* $\mathscr{B}_1$ *is* $q-1$.

The following lemma shows that the module $\mathfrak{M}$ is contained in $\mathfrak{B}_1$.

Lemma 6.5. *The* $\mathbb{Z}$*-module* $\mathfrak{M}$ *is contained in the* $\mathbb{Z}$*-module* $\mathfrak{B}_1$.

Proof. We show that each element of $\mathfrak{M}$ can be written as a linear combination of elements of $\mathscr{B}_1$. To this end it is sufficient to show that every frequency vector of a solution to an equation with exactly k_0 non-zero entries and all-one coefficients can be written as a linear combination of the elements of $\mathscr{B}_1$. Let thus $x \in \mathbb{N}^{q-1}$ be such a frequency vector, that is $\|x\|_1 \leq k_0$ and $\sum_{i=1}^{q-1} x_i f^{-1}(i) = 0$ in $\mathbb{F}_q$. Before we state a linear combination of x in terms of $\mathscr{B}_1$, observe that for each $j \in [q-1] \setminus \{q-1-(\ell-1)(p-1), q-1-(\ell-2)(p-1), \ldots, q-1\}$, there is exactly one basis vector with a non-zero entry in position j. Moreover, the entry of this basis vector in position j is 1. On the other hand, the basis vectors corresponding to the remaining ℓ columns $q-1-(\ell-1)(p-1), q-1-(\ell-2)(p-1), \ldots, q-1$ of M_q are actually integer multiples of the standard unit vectors, as

$$e_{f((p-1)\mathbb{X}^i)} + (p-1)e_{f(-\mathbb{X}^i)} = p e_{f((p-1)\mathbb{X}^i)}$$

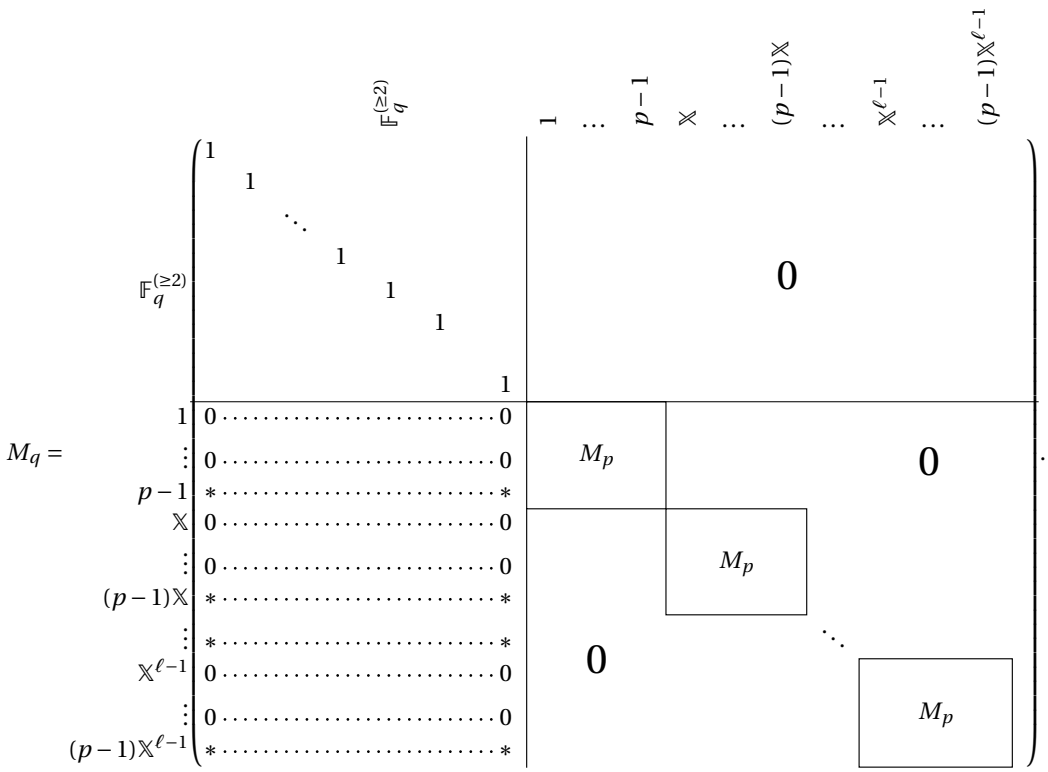

FIGURE 5. The matrix M_q for $\ell \geq 2$.

for $i = 0, \dots, \ell-1$. With these observations, the only valid candidate for a linear combination of x in terms of the elements of $\mathscr{B}_1$ is given by

$$x = \sum_{\sum_{i=0}^{\ell-1} a_i \mathbb{X}^i \in \mathbb{F}_q^* \setminus \{-1,\dots,-\mathbb{X}^{\ell-1}\}} x_{f(\sum_{i=0}^{\ell-1} a_i \mathbb{X}^i)} \left(e_{f(\sum_{i=0}^{\ell-1} a_i \mathbb{X}^i)} + \sum_{j=0}^{\ell-1} a_j e_{f(-\mathbb{X}^j)} \right)$$
$$+ \sum_{j=0}^{\ell-1} \frac{x_{f(-\mathbb{X}^j)} - \sum_{\sum_{i=0}^{\ell-1} a_i \mathbb{X}^i \in \mathbb{F}_q^* \setminus \{-1,\dots,-\mathbb{X}^{\ell-1}\}} a_j x_{f(\sum_{i=0}^{\ell-1} a_i \mathbb{X}^i)}}{p} \cdot p e_{f(-\mathbb{X}^j)}.$$

It remains to argue why the coefficients of the basis vectors $pe_{f(-1)}, \dots, pe_{f(-\mathbb{X}^{\ell-1})}$ in the second sum are integers. At this point, we will use that x is a solution statistic: Because

$$\sum_{\sum_{i=0}^{\ell-1} a_i \mathbb{X}^i \in \mathbb{F}_q^*} x_{f(\sum_{i=0}^{\ell-1} a_i \mathbb{X}^i)} \sum_{j=0}^{\ell-1} a_j \mathbb{X}^j = 0 \qquad \text{in} \quad \mathbb{F}_q$$

and the additive group $(\mathbb{F}_q, +)$ is isomorphic to $((\mathbb{F}_p)^\ell, +)$, all "components" in the above sum must be zero and thus

$$\sum_{\sum_{i=0}^{\ell-1} a_i \mathbb{X}^i \in \mathbb{F}_q^*} x_{f(\sum_{i=0}^{\ell-1} a_i \mathbb{X}^i)} a_j = 0 \qquad \text{in} \quad \mathbb{F}_p$$

for all $j = 0, \dots, \ell-1$. However, isolating the contribution from $\{-1, \dots, -\mathbb{X}^{\ell-1}\}$ yields

$$0 = \sum_{\sum_{i=0}^{\ell-1} a_i \mathbb{X}^i \in \mathbb{F}_q^*} x_{f(\sum_{i=0}^{\ell-1} a_i \mathbb{X}^i)} a_j = -x_{f(-\mathbb{X}^j)} + \sum_{\sum_{i=0}^{\ell-1} a_i \mathbb{X}^i \in \mathbb{F}_q^* \setminus \{-1,\dots,-\mathbb{X}^{\ell-1}\}} a_j x_{f(\sum_{i=0}^{\ell-1} a_i \mathbb{X}^i)} \qquad \text{in} \quad \mathbb{F}_p, \tag{6.3}$$

as the coefficient a_j of $\mathbb{X}^j$ in $-\mathbb{X}^i$ is zero unless $i = j$. Therefore, the right hand side in (6.3) is divisible by p and the claim follows. □

6.1.2. *Second basis $\mathscr{B}_2$.* In this subsection, we define a candidate set for the vectors $(\mathfrak{b}_1,\dots,\mathfrak{b}_{q-1})$ in the statement of Lemma 6.1. That is, we define a set $\mathscr{B}_2$ all whose elements have non-negative components and ℓ_1-norm at most three. In other words, we are looking for solutions to

$$x_1+\ldots+x_{k_0}=0 \tag{6.4}$$

with at most three different non-zero components.

Here again, our construction basically associates one basis vector to each element of $\mathbb{F}_q^*$. However, due to the ℓ_1-restriction, there is less freedom in choosing the remaining non zero-coordinates. Our approach to design a set that satisfies this restriction while retaining a representation in a convenient block lower triangular matrix structure is to distinguish between elements of length one and of length at least two. We will therefore construct $\mathscr{B}_2$ via two sets $\mathscr{B}^{(1)}$ and $\mathscr{B}^{(\geq 2)}$ such that $\mathscr{B}_2$ is given as

$$\mathscr{B}_2=\mathscr{B}^{(1)}\cup\mathscr{B}^{(\geq 2)}. \tag{6.5}$$

Let us start with an element $h=\sum_{i=0}^{\ell-1}a_i\mathbb{X}^i$ of length at least two in $\mathbb{F}_q$. Assume that its leading coefficient is a_r for $r\in[\ell-1]$. If a variable in (6.4) takes value h, we may cancel its contribution to an equation by subtracting the two elements $a_r\mathbb{X}^r$ and $h-a_r\mathbb{X}^r$, both of which are shorter than h:

$$\sum_{i=0}^{\ell-1}a_i\mathbb{X}^i-a_r\mathbb{X}^r-\left(\sum_{i=0}^{\ell-1}a_i\mathbb{X}^i-a_r\mathbb{X}^r\right)=0.$$

This solution corresponds to the vector

$$e_{f(h)}+e_{f(-a_r\mathbb{X}^r)}+e_{f(-h+a_r\mathbb{X}^r)}.$$

This idea for field elements $h\in\mathbb{F}_q^{(\geq 2)}$ of length at least two then yields the $q-1-\ell(p-1)$ integer vectors

$$\mathscr{B}^{(\geq 2)}=\left\{e_{f(h)}+e_{f(-a_r\mathbb{X}^r)}+e_{f(-h+a_r\mathbb{X}^r)}:r\in[\ell-1]\text{ and }h=\sum_{i=0}^{r}a_i\mathbb{X}^i\in\mathbb{F}_q^{(\geq 2)}\text{ with }a_r\neq 0\right\}.$$

For a field element h of length one, an analogous shortening operation would correspond to the vector

$$e_{f(h)}+e_{f(-h)}.$$

If $p=2$, this procedure applied to all field elements of length one yields ℓ distinct vectors and we are done. However, if $p>2$, employing this idea for all elements of length one would only lead to $\ell(p-1)/2$ rather than $\ell(p-1)$ additional vectors, as h and $-h$ are distinct and obviously give rise to the same statistic. As a consequence, for $p>2$, we need to deviate from the above construction and come up with a modified "short-solution" scheme. Let $h=a_r\mathbb{X}^r$ be an element of length one. If $a_r\in\{1,\dots(p-1)/2\}$, we simply associate the vector $e_{f(h)}+e_{f(-h)}$ to it, as indicated. If on the other hand $a_r\in\{(p+1)/2,\dots,p-1\}$, we let h correspond to the vector

$$e_{f(h)}+e_{f(-\mathbb{X}^r)}+e_{f(-h+\mathbb{X}^r)}.$$

With this, for $p>2$, the part of $\mathscr{B}_2$ that corresponds to field elements of length one is given by the set

$$\mathscr{B}^{(1)}=\bigcup_{r=0}^{\ell-1}\left(\left\{e_{f(a_r\mathbb{X}^r)}+e_{f(-a_r\mathbb{X}^r)}:a_r\in[(p-1)/2]\right\}\cup\left\{e_{f(-a_r\mathbb{X}^r)}+e_{f(-\mathbb{X}^r)}+e_{f(a_r\mathbb{X}^r+\mathbb{X}^r)}:a_r\in[(p-1)/2]\right\}\right). \tag{6.6}$$

If $p=2$, in line with the above discussion, we simply let

$$\mathscr{B}^{(1)}=\bigcup_{r=0}^{\ell-1}\left\{2e_{f(\mathbb{X}^r)}\right\}. \tag{6.7}$$

Again, a moment of thought shows that in any case, $|\mathscr{B}_2|=|\mathscr{B}_1|=q-1$. Let $\mathfrak{B}_2$ denote the $\mathbb{Z}$-module generated by the elements of $\mathscr{B}_2$. Our choice of $\mathscr{B}_2$ has the advantage that again, its elements may be represented in a block lower triangular matrix. For this representation, it is instructive to consider the case $\ell=1$ first. In this case and with our choice of f, the elements of $\mathscr{B}_2$ can be arranged as the columns of a matrix A_p as in Figure 6.

Here, as in the construction of M_p, column i corresponds to the unique vector associated to $i\in\mathbb{F}_q$. In the special case $p=2$, this matrix reduces to

$$A_2=(2).$$

For $\ell\geq 2$, the elements of $\mathscr{B}_2$ may then be visualised in the matrix from Figure 7.

$$A_p = \begin{pmatrix}
1 & 0 & \cdots & \cdots & 0 & 0 & \cdots & \cdots & \cdots & 0 \\
0 & \ddots & \ddots & & \vdots & \vdots & & & \iddots & 1 \\
\vdots & \ddots & \ddots & \ddots & \vdots & \vdots & & \iddots & \iddots & 0 \\
\vdots & & \ddots & \ddots & 0 & \vdots & \iddots & \iddots & \iddots & \vdots \\
0 & \cdots & \cdots & 0 & 1 & 0 & 1 & 0 & \cdots & 0 \\
0 & \cdots & \cdots & 0 & 1 & 2 & 0 & \cdots & \cdots & 0 \\
\vdots & & \iddots & \iddots & 0 & 0 & 1 & \ddots & & \vdots \\
\vdots & \iddots & \iddots & \iddots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\
0 & \iddots & \iddots & & \vdots & 0 & \cdots & 0 & 1 & 0 \\
1 & 0 & \cdots & \cdots & 0 & 1 & \cdots & \cdots & 1 & 2
\end{pmatrix}. \tag{6.8}$$

FIGURE 6. The matrix A_p.

$$A_q = \begin{array}{c}
\\
\\
\\
\\
\\
\\
\\
\\
1 \\
\vdots \\
p-1 \\
\mathbb{X} \\
\vdots \\
(p-1)\mathbb{X} \\
\vdots \\
\mathbb{X}^{\ell-1} \\
\vdots \\
(p-1)\mathbb{X}^{\ell-1}
\end{array}
\begin{array}{c}
\mathbb{F}_q^{(\geq 2)} \\
\left(\begin{array}{cccccccc}
1 & & & & & & & \\
* & 1 & & & & & & \\
* & * & \ddots & & & & & \\
* & \cdots & * & 1 & & & & \\
* & \cdots & * & 1 & 1 & & & \\
* & \cdots & * & 1 & & \ddots & & \\
* & \cdots & * & 1 & & & 1 & \\
* & \cdots & * & 1 & & & & \\
* & \cdots & * & 1 & & & & \\
* & \cdots & * & 1 & & & & \\
* & \cdots & * & 1 & & & & \\
* & \cdots & * & 1 & & & & \\
* & \cdots & * & 1 & & & & \\
* & \cdots & * & 1 & & & & \\
* & \cdots & * & 1 & & & & \\
* & \cdots & * & 1 & & & &
\end{array}\right)
\end{array}
\begin{array}{c}
1 \quad \cdots \quad p-1 \quad \mathbb{X} \quad \cdots \quad (p-1)\mathbb{X} \quad \cdots \quad \mathbb{X}^{\ell-1} \quad \cdots \quad (p-1)\mathbb{X}^{\ell-1} \\
\left(\begin{array}{cccccccc}
 & & & & & & & \\
 & & & & & & & \\
 & & & & & & & \\
 & & & & & & & \\
 & & & & 0 & & & \\
 & & & & & & & \\
 & & & & & & & \\
 & & & & & & & \\
A_p & & & & & & & \\
 & & & & & & & \\
 & & & & & & & \\
 & A_p & & & & & & \\
 & & & & & & & \\
 & & \ddots & & & & & \\
 & & & & & & & \\
 & & & A_p & & & & \\
 & & & & & & & \\
 & & & & & & &
\end{array}\right)
\end{array}. \tag{6.9}$$

FIGURE 7. The matrix A_q for $\ell \geq 2$.

In A_q, column $i \in [q-1]$ corresponds to the unique vector that is associated with the field element $f^{-1}(i)$. Moreover, at this point, a moment of appreciation of our indexing choice f is in place: Because f is monotonically decreasing with respect to length, there are no entries above the diagonal in the first $|\mathbb{F}_q^{(\geq 2)}|$ columns, as we only cancel field elements by strictly shorter ones. Moreover, the remaining $\ell(p-1)$ columns are governed by a simple

block structure. As a concrete example, (6.8) with $p = 7$ reads

$$A_7 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 2 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 2 \end{pmatrix}$$

and A_7 would be used as a block matrix in any field of order 7^ℓ as shown in (6.9).

As each element of $\mathscr{B}_2$ corresponds to a solution with at most $3 \leq k_0$ non-zero components, we obtain the following.

Claim 6.6. *The $\mathbb{Z}$-module $\mathfrak{B}_2$ is contained in the $\mathbb{Z}$-module $\mathfrak{M}$.*

Thus far we know $\mathfrak{B}_2 \subseteq \mathfrak{M} \subseteq \mathfrak{B}_1$. Moreover, $\mathscr{B}_2$ has the desired ℓ_1-property. On the other hand, in comparison to $\mathscr{B}_1$, it is less clear that $\mathscr{B}_2$ generates $\mathfrak{M}$. It thus remains to show that in fact $\mathfrak{B}_2 = \mathfrak{B}_1$. We will do so by using the following fact, which is an immediate consequence of the adjugate matrix representation of the inverse matrix.

Fact 6.7. *If M is a free $\mathbb{Z}$-module with basis $x_1, \ldots, x_n$, a set of elements $y_1, \ldots, y_n \in M$ is a basis of M if and only if the change of basis matrix (c_{ij}) has determinant ± 1.*

We will apply Fact 6.7 to $M = \mathfrak{B}_1$ with $\{x_1, \ldots, x_n\} = \mathscr{B}_1$ and $\{y_1, \ldots, y_n\} = \mathscr{B}_2$. Let $C_q \in \mathbb{Z}^{(q-1)\times(q-1)}$ be the matrix whose entries comprise the coefficients when we express the elements of $\mathscr{B}_2$ by $\mathscr{B}_1$ (recall that $\mathfrak{B}_2 \subseteq \mathfrak{B}_1$) when we order the elements of $\mathscr{B}_1, \mathscr{B}_2$ as done in the construction of M_q and A_q. Thus $A_q = M_q C_q$. As

$$\det(A_q) = \det(M_q C_q) = \det(M_q) \cdot \det(C_q),$$

we do not need to compute C_q explicitly to apply Fact 6.7, but instead it suffices to compute $\det(M_q)$ and $\det(A_q)$. From Claim 6.3, $\det(M_q)$ is already known. Moreover, for A_q, the computation will not be too hard, as A_q is a block lower triangular matrix. Therefore, we are just left to calculate the determinant of the non-trivial diagonal blocks.

Lemma 6.8. *For any prime p we have $\det(A_p) = p$.*

Proof. The case $p = 2$ is immediate. We thus assume that $p > 2$ in the following. We transform A_p into a lower triangular matrix by elementary column operations. To this end, let $a_1, \ldots, a_{q-1}$ be the columns of A_p. The first $(p+1)/2$ columns already have the right form, so we do not alter this part of the matrix. For any $j = (p+3)/2, \ldots, p-1$, subtract column a_{p+1-j} from column a_j. This yields the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \ddots & 0 & 0 & 0 & \iddots & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & -1 & 0 & 0 \\ 0 & 0 & \iddots & 0 & 0 & 1 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & \ddots & -1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 \end{pmatrix}.$$

Next, we swap column $(p+1)/2$ successively with columns $(p+3)/2, \ldots$ up to $p-1$, yielding

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \ddots & 0 & 0 & 0 & \iddots & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & 2 \\ 0 & 0 & \iddots & 0 & 1 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & \ddots & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 2 & 1 \end{pmatrix}.$$

This changes the determinant by a factor of $(-1)^{(p-3)/2}$. Finally, in order to erase the entry 2 in row $(p+1)/2$ and column $p-1$, we add twice the sum of columns $(p+1)/2,\dots,p-2$ to column $p-1$. We thus obtain the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \ddots & 0 & 0 & 0 & \iddots & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & \iddots & 0 & 1 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & \ddots & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 2 & p \end{pmatrix}.$$

with determinant $(-1)^{(p-3)/2}p$. Multiplying with $(-1)^{(p-3)/2}$ from the column swaps yields the claim. □

Corollary 6.9. *For any prime p and $\ell \geq 1$, we have* $\det(A_q) = q$.

Finally, Claim 6.3 and Corollary 6.9 imply that $\det(C_q) = 1$. Thus, by Fact 6.7, $\mathscr{B}_2$ is a basis of $\mathfrak{B}_1$, which implies that $\mathfrak{B}_1 = \mathfrak{B}_2 = \mathfrak{M}$. The column vectors $\mathfrak{b}_1,\dots,\mathfrak{b}_{q-1}$ of A_q therefore enjoy the properties stated in Lemma 6.1.

6.2. **Proof of Lemma 6.2.** Assume w.l.o.g. that $\chi_1 = 1$. Moreover, by assumption, the set $\{\chi_1,\dots,\chi_{k_0}\}$ contains at least two different elements, and so we may also assume that $\chi_3 \neq 1$ (recall that $k_0 \geq 3$).

We define $(\mathfrak{b}_1,\dots,\mathfrak{b}_{q-1})$ by distinguishing between three cases:

Case 1: $p = 2$ and $\chi_2 = 1$.

Denote the order of χ_3^{-1} in $(\mathbb{F}_q^*,\cdot)$ by $\mathfrak{o}$, so that the elements $1,\chi_3^{-1},\dots,\chi_3^{-(\mathfrak{o}-1)}$ are pairwise distinct. Since $p = 2$ and $\mathfrak{o} \mid q-1$, $\mathfrak{o}$ is an odd number. Moreover, because $\chi_3^{-1} \neq 1$, $\mathfrak{o} \geq 3$. We now partition $\mathbb{F}_q^*$ into orbits of the action of $(\{1,\chi_3^{-1},\dots,\chi_3^{-(\mathfrak{o}-1)}\},\cdot)$ on $\mathbb{F}_q^*$ such that

$$\mathbb{F}_q^* = \dot{\bigcup}_{j=1}^{(q-1)/\mathfrak{o}} \mathfrak{O}_j,$$

where each orbit $\mathfrak{O}_j$ contains exactly $\mathfrak{o}$ elements. Suppose that $\mathfrak{O}_j = \{g_1^{(j)},\dots,g_{\mathfrak{o}}^{(j)}\}$, where the elements are indexed such that $g_{i+1}^{(j)} = \chi_3^{-1} g_i^{(j)}$.

To each $\mathfrak{O}_j$, we associate a set of potential basis vectors whose union over different j then yields the full set $(\mathfrak{b}_1,\dots,\mathfrak{b}_{q-1})$. More precisely, the set corresponding to $\mathfrak{O}_j$ is defined as

$$\mathfrak{B}_j = \bigcup_{i=1}^{\mathfrak{o}-1} \left\{ e_{g_i^{(j)}} + e_{g_{i+1}^{(j)}} \right\} \cup \left\{ e_{g_1^{(j)}} + e_{g_2^{(j)}} + e_{g_2^{(j)}+g_3^{(j)}} \right\}.$$

In this definition, we have used that for $\chi_1 = -\chi_2 = 1$ and any $h \in \mathbb{F}_q$,

$$\chi_1 \cdot h + \chi_2 \cdot 0 + \chi_3 \cdot \chi_3^{-1} h = 0 \qquad \text{as well as} \qquad \chi_1 \cdot h + \chi_2 \cdot \chi_3^{-1} h + \chi_3 \cdot (\chi_3^{-1} h + \chi_3^{-2} h) = 0.$$

Note that the element

$$g_2^{(j)} + g_3^{(j)} = (1 + \chi_3^{-1}) g_2^{(j)}$$

is nonzero and distinct from both $g_2^{(j)}$ and $g_3^{(j)}$. It might be one of $g_1^{(j)}, g_4^{(j)},\dots,g_{\mathfrak{o}}^{(j)}$.

We next argue that the union of the different $\mathfrak{B}_j$ generates $\mathbb{Z}^{\mathbb{F}_q^*}$. By linear transformation and using that $\mathfrak{o}$ is odd, $\mathfrak{B}_j$ has the same span as

$$\left\{ e_{g_1^{(j)}} + e_{g_2^{(j)}}, e_{g_1^{(j)}} - e_{g_3^{(j)}}, e_{g_1^{(j)}} + e_{g_4^{(j)}},\dots, e_{g_1^{(j)}} - e_{g_{\mathfrak{o}}^{(j)}} \right\} \cup \left\{ e_{g_1^{(j)}+g_2^{(j)}} \right\}.$$

Now, there are two cases.

(1) For all $j \in [(q-1)/\mathfrak{o}]$, $g_2^{(j)} + g_3^{(j)} \in \{g_1^{(j)}, g_4^{(j)},\dots,g_{\mathfrak{o}}^{(j)}\}$. In this case, either $e_{g_2^{(j)}+g_3^{(j)}} = e_{g_1^{(j)}}$, or we can subtract $e_{g_2^{(j)}+g_3^{(j)}}$ from or add it to the element $e_{g_1^{(j)}} \pm e_{g_2^{(j)}+g_3^{(j)}}$ to obtain $e_{g_1^{(j)}}$. After isolating $e_{g_1^{(j)}}$, a straightforward linear transformation yields a set of $\mathfrak{o}$ distinct unit vectors whose non-zero components are given by $\mathfrak{O}_j$. Thus, the union over all $\mathfrak{B}_j$ constitutes a set of linearly independent elements that generates $\mathbb{Z}^{\mathbb{F}_q^*}$.

(2) For all $j \in [(q-1)/\mathfrak{o}]$, $g_2^{(j)} + g_3^{(j)} \notin \{g_1^{(j)}, g_4^{(j)}, \dots, g_{\mathfrak{o}}^{(j)}\}$. In this case, consider the union $\bigcup_{j=1}^{(q-1)/\mathfrak{o}} \mathfrak{B}_j$, which has the same span as

$$\bigcup_{j=1}^{(q-1)/\mathfrak{o}} \left\{ e_{g_1^{(j)}} + e_{g_2^{(j)}}, e_{g_1^{(j)}} - e_{g_3^{(j)}}, e_{g_1^{(j)}} + e_{g_4^{(j)}}, \dots, e_{g_1^{(j)}} - e_{g_{\mathfrak{o}}^{(j)}} \right\} \cup \left\{ e_{g_1^{(j)} + g_2^{(j)}} \right\}.$$

Since for each j, the element $g_1^{(j)} + g_2^{(j)}$ must be contained in some $\mathfrak{O}_{j'}$ for $j \neq j'$, as in case (1), $e_{g_1^{(j)} + g_2^{(j)}}$ can be used to isolate $e_{g_1^{(j')}}$. After isolating $e_{g_1^{(j')}}$ for all j', these elements can be straightforwardly used to linearly transform the union over all $\mathfrak{B}_j$ into the standard basis $(e_h)_{h \in \mathbb{F}_q^*}$ of $\mathbb{Z}^{\mathbb{F}_q^*}$.

Finally, set $\bigcup_{j=1}^{(q-1)/\mathfrak{o}} \mathfrak{B}_j = \{\mathfrak{b}_1, \dots, \mathfrak{b}_{q-1}\}$.

Case 2: $p \neq 2$ and $\chi_2 = -1$.

We proceed almost exactly as before, only the choice of the "acyclic" basis vectors is different:

Denote the order of χ_3^{-1} in $(\mathbb{F}_q^*, \cdot)$ by $\mathfrak{o}$, so that the elements $1, \chi_3^{-1}, \dots, \chi_3^{-(\mathfrak{o}-1)}$ are pairwise distinct. Then $\mathfrak{o} \mid q-1$, and since $\chi_3^{-1} \neq 1$, $\mathfrak{o} \geq 2$. We now partition $\mathbb{F}_q^*$ into orbits of the action of $(\{1, \chi_3^{-1}, \dots, \chi_3^{-(\mathfrak{o}-1)}\}, \cdot)$ on $\mathbb{F}_q^*$ such that

$$\mathbb{F}_q^* = \dot{\bigcup}_{j=1}^{(q-1)/\mathfrak{o}} \mathfrak{O}_j,$$

where each orbit $\mathfrak{O}_j$ contains exactly $\mathfrak{o}$ elements. Suppose that $\mathfrak{O}_j = \{g_1^{(j)}, \dots, g_{\mathfrak{o}}^{(j)}\}$, where the elements are indexed such that $g_{i+1}^{(j)} = \chi_3^{-1} g_i^{(j)}$.

To each $\mathfrak{O}_j$, we associate a set of potential basis vectors whose union over different j then yields the full set $(\mathfrak{b}_1, \dots, \mathfrak{b}_{q-1})$. More precisely, the set corresponding to $\mathfrak{O}_j$ is defined as

$$\mathfrak{B}_j = \bigcup_{i=1}^{\mathfrak{o}-1} \left\{ e_{g_i^{(j)}} + e_{g_{i+1}^{(j)}} \right\} \cup \left\{ e_{g_1^{(j)}} + e_{g_2^{(j)}} + e_{2g_1^{(j)}} \right\}.$$

Here, we have used that for $\chi_1 = -\chi_2 = 1$ and $p \neq 2$,

$$\chi_1 \cdot 0 + \chi_2 \cdot h + \chi_3 \cdot \chi_3^{-1} h = 0 \qquad \text{and} \qquad \chi_1 \cdot h + \chi_2 \cdot 2h + \chi_3 \cdot \chi_3^{-1} h = 0.$$

Note that the element $2g_1^{(j)}$ is distinct from $g_1^{(j)}$. It might be one of $g_2^{(j)}, \dots, g_{\mathfrak{o}}^{(j)}$.

We next argue that the union of the different $\mathfrak{B}_j$ generates $\mathbb{Z}^{\mathbb{F}_q^*}$. By linear transformation, $\mathfrak{B}_j$ has the same span as

$$\left\{ e_{g_1^{(j)}} + e_{g_2^{(j)}}, e_{g_1^{(j)}} - e_{g_3^{(j)}}, e_{g_1^{(j)}} + e_{g_4^{(j)}}, \dots, e_{g_1^{(j)}} \pm e_{g_{\mathfrak{o}}^{(j)}} \right\} \cup \left\{ e_{2g_1^{(j)}} \right\}.$$

Now, there are two cases.

(1) For all $j \in [(q-1)/\mathfrak{o}]$, $2g_1^{(j)} \in \{g_2^{(j)}, \dots, g_{\mathfrak{o}}^{(j)}\}$. As in case 1, we can then subtract $e_{2g_2^{(j)}}$ from or add it to $e_{g_1^{(j)}} \pm e_{2g_2^{(j)}}$ to isolate $e_{g_1^{(j)}}$. After isolating $e_{g_1^{(j)}}$, a straightforward linear transformation yields a set of $\mathfrak{o}$ distinct unit vectors whose non-zero components are given by $\mathfrak{O}_j$. Thus, the union over all $\mathfrak{B}_j$ constitutes a set of linearly independent elements that generates $\mathbb{Z}^{\mathbb{F}_q^*}$.

(2) For all $j \in [(q-1)/\mathfrak{o}]$, $2g_1^{(j)} \notin \{g_2^{(j)}, \dots, g_{\mathfrak{o}}^{(j)}\}$. In this case, consider the union $\bigcup_{j=1}^{(q-1)/\mathfrak{o}} \mathfrak{B}_j$, which has the same span as

$$\bigcup_{j=1}^{(q-1)/\mathfrak{o}} \left\{ e_{g_1^{(j)}} + e_{g_2^{(j)}}, e_{g_1^{(j)}} - e_{g_3^{(j)}}, e_{g_1^{(j)}} + e_{g_4^{(j)}}, \dots, e_{g_1^{(j)}} \pm e_{g_{\mathfrak{o}}^{(j)}} \right\} \cup \left\{ e_{2g_1^{(j)}} \right\}.$$

Since for each j, the element $2g_1^{(j)}$ must be contained in some $\mathfrak{O}_{j'}$ for $j \neq j'$, as in case (1), $e_{2g_1^{(j)}}$ can be used to isolate $e_{g_1^{(j')}}$. After isolating $e_{g_1^{(j')}}$ for all j', these elements can be straightforwardly used to linearly transform the union over all $\mathfrak{B}_j$ into the standard basis $(e_h)_{h \in \mathbb{F}_q^*}$ of $\mathbb{Z}^{\mathbb{F}_q^*}$.

In any case, set $\bigcup_{j=1}^{(q-1)/\mathfrak{o}} \mathfrak{B}_j = \{\mathfrak{b}_1, \dots, \mathfrak{b}_{q-1}\}$.

Case 3: $\chi_2 \neq -1$.

Denote the order of $-\chi_2^{-1}$ in $(\mathbb{F}_q^*,\cdot)$ by $\mathfrak{o}$, so that the elements $1,-\chi_2^{-1},\dots,(-\chi_2^{-1})^{\mathfrak{o}-1}$ are pairwise distinct. Then $\mathfrak{o}\mid q-1$, and since $-\chi_2^{-1}\neq 1$, $\mathfrak{o}\geq 2$. We now partition $\mathbb{F}_q^*$ into orbits of the action of $(\{1,-\chi_2^{-1},\dots,(-\chi_2^{-1})^{\mathfrak{o}-1}\},\cdot)$ on $\mathbb{F}_q^*$ such that

$$\mathbb{F}_q^* = \dot{\bigcup}_{j=1}^{(q-1)/\mathfrak{o}} \mathfrak{O}_j,$$

where each orbit $\mathfrak{O}_j$ contains exactly $\mathfrak{o}$ elements. Suppose that $\mathfrak{O}_j=\{g_1^{(j)},\dots,g_{\mathfrak{o}}^{(j)}\}$, where the elements are indexed such that $g_{i+1}^{(j)}=-\chi_2^{-1}g_i^{(j)}$.

To each $\mathfrak{O}_j$, we associate a set of potential basis vectors whose union over different j then yields the full set $(\mathfrak{b}_1,\dots,\mathfrak{b}_{q-1})$. More precisely, the set corresponding to $\mathfrak{O}_j$ is defined as

$$\mathfrak{B}_j = \bigcup_{i=1}^{\mathfrak{o}-1}\left\{e_{g_i^{(j)}}+e_{g_{i+1}^{(j)}}\right\}\cup\left\{e_{g_1^{(j)}}+e_{g_2^{(j)}}+e_{(1-\chi_3)g_1^{(j)}}\right\}.$$

In the above, we have used that for $\chi_1=1$,

$$\chi_1\cdot h+\chi_2\cdot(-\chi_2^{-1})h+\chi_3\cdot 0=0 \qquad\text{and}\qquad \chi_1\cdot(1-\chi_3)h+\chi_2\cdot(-\chi_2^{-1})h+\chi_3\cdot h=0.$$

Note that the element $(1-\chi_3)g_1^{(j)}$ is distinct from $g_1^{(j)}$. It might be one of $g_2^{(j)},\dots,g_{\mathfrak{o}}^{(j)}$.

We next argue that the union of the different $\mathfrak{B}_j$ generates $\mathbb{Z}^{\mathbb{F}_q^*}$. By linear transformation, $\mathfrak{B}_j$ has the same span as

$$\left\{e_{g_1^{(j)}}+e_{g_2^{(j)}}, e_{g_1^{(j)}}-e_{g_3^{(j)}}, e_{g_1^{(j)}}+e_{g_4^{(j)}},\dots,e_{g_1^{(j)}}\pm e_{g_{\mathfrak{o}}^{(j)}}\right\}\cup\left\{e_{(1-\chi_3)g_1^{(j)}}\right\}.$$

Now, there are two cases.

(1) For all $j\in[(q-1)/\mathfrak{o}]$, $(1-\chi_3)g_1^{(j)}$ is one of the elements $g_2^{(j)},\dots,g_{\mathfrak{o}}^{(j)}$. As in case 1, we can then subtract $e_{2g_2^{(j)}}$ from or add it to $e_{g_1^{(j)}}\pm e_{(1-\chi_3)g_1^{(j)}}$ to isolate $e_{g_1^{(j)}}$. After isolating $e_{g_1^{(j)}}$, a straightforward linear transformation yields a set of $\mathfrak{o}$ distinct unit vectors whose non-zero components are given by $\mathfrak{O}_j$. Thus, the union over all $\mathfrak{B}_j$ constitutes a set of linearly independent elements that generates $\mathbb{Z}^{\mathbb{F}_q^*}$.

(2) For all $j\in[(q-1)/\mathfrak{o}]$, $(1-\chi_3)g_1^{(j)}$ is none of the elements $g_2^{(j)},\dots,g_{\mathfrak{o}}^{(j)}$. In this case, consider the union $\bigcup_{j=1}^{(q-1)/\mathfrak{o}}\mathfrak{B}_j$, which has the same span as

$$\bigcup_{j=1}^{(q-1)/\mathfrak{o}}\left\{e_{g_1^{(j)}}+e_{g_2^{(j)}}, e_{g_1^{(j)}}-e_{g_3^{(j)}}, e_{g_1^{(j)}}+e_{g_4^{(j)}},\dots,e_{g_1^{(j)}}\pm e_{g_{\mathfrak{o}}^{(j)}}\right\}\cup\left\{e_{(1-\chi_3)g_1^{(j)}}\right\}.$$

Since for each j, the element $(1-\chi_3)g_1^{(j)}$ must be contained in some $\mathfrak{O}_{j'}$ for $j\neq j'$, as in case (1), $e_{(1-\chi_3)g_1^{(j)}}$ can be used to isolate $e_{g_1^{(j')}}$. After isolating $e_{g_1^{(j')}}$ for all j', these elements can be straightforwardly used to linearly transform the union over all $\mathfrak{B}_j$ into the standard basis $(e_h)_{h\in\mathbb{F}_q^*}$ of $\mathbb{Z}^{\mathbb{F}_q^*}$.

In any case, set $\bigcup_{j=1}^{(q-1)/\mathfrak{o}}\mathfrak{B}_j=\{\mathfrak{b}_1,\dots,\mathfrak{b}_{q-1}\}$.

7. Proof of Proposition 2.4

7.1. **Overview.** The aim in this section is to bound the expected size of the kernel of $\boldsymbol{A}$ on $\mathfrak{O}$ from (2.7), i.e., $|\ker\boldsymbol{A}|\cdot\mathbb{1}\mathfrak{O}$. As in Section 2.1 we let $\mathfrak{A}$ be the σ-algebra generated by $\boldsymbol{m},(\boldsymbol{k}_i)_{i\geq 1},(\boldsymbol{d}_i)_{i\geq 1}$ and by the numbers $\boldsymbol{m}(\chi_1,\dots,\chi_\ell)$ of equations of degree $\ell\geq 3$ with coefficients $\chi_1,\dots,\chi_\ell\in\mathbb{F}_q^*$. Thus, the total degree $\boldsymbol{\Delta}=\sum_{i=1}^n\boldsymbol{d}_i$ is $\mathfrak{A}$-measurable.

Let us first observe that it suffices to count "nearly equitable" kernel vectors, in the following sense. For a vector $\sigma\in\mathbb{F}_q^n$ and $s\in\mathbb{F}_q$ define the empirical frequency

$$\rho_\sigma(s)=\sum_{i=1}^n\boldsymbol{d}_i\mathbb{1}\{\sigma_i=s\} \tag{7.1}$$

and let $\rho_\sigma=(\rho_\sigma(s))_{s\in\mathbb{F}_q}$. If $\mathfrak{O}$ occurs, then ρ_σ is nearly uniform for most kernel vectors. Formally, we have the following statement.

Fact 7.1. *For any $\varepsilon>0$ w.h.p. given $\mathfrak{A}$ we have $\mathbb{1}\mathfrak{O}\cdot|\ker\boldsymbol{A}|\leq(1+\varepsilon)\left|\left\{\sigma\in\ker\boldsymbol{A}:\|\rho_\sigma-q^{-1}\boldsymbol{\Delta}\mathbb{1}\|_1<\varepsilon\boldsymbol{\Delta}\right\}\right|$.*

Proof. Choose $\delta = \delta(\varepsilon, q) > 0$ small enough. Since $0 < \mathbb{E}[\boldsymbol{d}^2] < \infty$ we find a constant $d^* > 0$ such that

$$\boldsymbol{\Delta} > \sqrt{\delta} n \qquad \text{and} \qquad \sum_{i=1}^{n} \mathbb{1}\{\boldsymbol{d}_i > d^*\}\boldsymbol{d}_i < \delta\boldsymbol{\Delta} \qquad \text{w.h.p.} \tag{7.2}$$

Now, the definition (2.7) of $\mathfrak{O}$ implies that for any degree $\ell \le d^*$ a random vector $\boldsymbol{x}_{\boldsymbol{A}} \in \ker \boldsymbol{A}$ satisfies

$$\sum_{s,t \in \mathbb{F}_q} \sum_{i,j=1}^{n} \mathbb{1}\{\boldsymbol{d}_i = \boldsymbol{d}_j = \ell\} \left| \mathbb{P}\left[\boldsymbol{x}_{\boldsymbol{A},i} = s,\, \boldsymbol{x}_{\boldsymbol{A},j} = t \mid \boldsymbol{A}\right] - q^{-2} \right| = o(n^2) \quad \text{on } \mathfrak{O}. \tag{7.3}$$

By Chebyshev's inequality w.h.p. $\sum_{j=1}^{n} \mathbb{1}\{\boldsymbol{d}_j = \ell\} = \Omega(n)$ and consequently (7.3) shows that w.h.p. for a random vector $\boldsymbol{x}_{\boldsymbol{A}}$ we have

$$\left| \sum_{i=1}^{n} \mathbb{1}\{\boldsymbol{d}_i = \ell\} \left(\mathbb{1}\{\boldsymbol{x}_{\boldsymbol{A},i} = s\} - 1/q \right) \right| = o(n) \qquad \text{for all } s \in \mathbb{F}_q,\ \ell \le d^* \text{ on the event } \mathfrak{O}. \tag{7.4}$$

Combining (7.2) and (7.4) with the definition (7.1) of ρ_σ completes the proof. □

We proceed to contemplate different regimes of "nearly equitable" frequency vectors and employ increasingly subtle estimates to bound their contributions. To this end let $\mathfrak{P}_q$ be the set of all possible frequency vectors, i.e.,

$$\mathfrak{P}_q = \left\{ \rho_\sigma : \sigma \in \mathbb{F}_q^n \right\}.$$

Moreover, for $\varepsilon > 0$ let

$$\mathfrak{P}_q(\varepsilon) = \left\{ \rho \in \mathfrak{P}_q : \|\rho - q^{-1}\boldsymbol{\Delta}\mathbb{1}\| < \varepsilon\boldsymbol{\Delta} \right\}.$$

In addition, we introduce

$$\begin{aligned} \mathcal{Z}_\rho &= \left| \{\sigma \in \ker \boldsymbol{A} : \rho_\sigma = \rho\} \right| && (\rho \in \mathfrak{P}_q), \\ \mathcal{Z}_\varepsilon &= \sum_{\rho \in \mathfrak{P}_q(\varepsilon)} \mathcal{Z}_\rho && (\varepsilon \ge 0), \\ \mathcal{Z}_{\varepsilon,\varepsilon'} &= \mathcal{Z}_{\varepsilon'} - \mathcal{Z}_\varepsilon && (\varepsilon, \varepsilon' \ge 0). \end{aligned}$$

The following lemma sharpens the $\varepsilon\boldsymbol{\Delta}$ error bound from Fact 7.1 to $\omega n^{-1/2}\boldsymbol{\Delta}$.

Lemma 7.2. *For any fixed $\varepsilon > 0$ for large enough $\omega = \omega(\varepsilon) > 1$ w.h.p. we have $\mathbb{E}\left[\mathcal{Z}_{\omega n^{-1/2},\varepsilon} \mid \mathfrak{A}\right] < \varepsilon q^{n-\boldsymbol{m}}$.*

The proof of Lemma 7.2, which can be found in Section 7.2, is based on an expansion to the second order of the optimisation problem (2.5) around the equitable solution. Similar arguments have previously been applied in the theory of random constraint satisfaction problems, particularly random k-XORSAT (e.g. [4, 6, 21]).

For ρ that are within $O(n^{-1/2}\boldsymbol{\Delta})$ of the equitable solution such relatively routine arguments do not suffice anymore. Indeed, by comparison to examples of random CSPs that have been studied previously, sometimes by way of the small subgraph conditioning technique, a new challenge arises. Namely, due to the algebraic nature of our problem the conceivable empirical distributions $\rho_{\boldsymbol{x}}$ given that $\boldsymbol{x} \in \ker \boldsymbol{A}$ are confined to a proper sub-lattice of $\mathbb{Z}^q$. The same is true of $\mathfrak{P}_q$ unless $\mathfrak{d} = 1$. Hence, we need to work out how these lattices intersect. Moreover, for $\rho \in \mathfrak{P}_q$ we need to calculate the number of assignments σ such that $\rho_\sigma = \rho$ as well as the probability that such an assignment satisfies all equations. Seizing upon Proposition 2.3 and local limit theorem-type techniques, we will deal with these challenges in Section 7.3, where we prove the following.

Lemma 7.3. *For any $\varepsilon > 0$ for large enough $\omega = \omega(\varepsilon) > 1$ we have $\mathbb{E}[\mathcal{Z}_{\omega n^{-1/2}} \mid \mathfrak{A}] \le (1+\varepsilon) q^{n-\boldsymbol{m}}$ w.h.p.*

Proof of Proposition 2.4. This is an immediate consequence of Fact 7.1, Lemma 7.2 and Lemma 7.3. □

7.2. **Proof of Lemma 7.2.** As we just saw, on the one hand we need to count $\sigma \in \mathbb{F}_q^n$ such that ρ_σ hits a particular attainable $\rho \in \mathfrak{P}_q(\varepsilon)$. On the other hand, we need to estimate the probability that such a given σ satisfies all equations. The first of these, the entropy term, increases as ρ becomes more equitable. The second, probability term takes greater values for non-uniform ρ. Roughly, the more zero entries ρ contains, the better. The thrust of the proofs of Lemmas 7.2 and 7.3 is to show that the drop in entropy is an order of magnitude stronger than the boost to the success probability.

Toward the proof of Lemma 7.2 we can get away with relatively rough bounds, mostly disregarding constant factors. The first claim bounds the entropy term. Instead of counting assignments we will take a probabilistic viewpoint. Hence, let $\boldsymbol{\sigma} \in \mathbb{F}_q^n$ be a uniformly random assignment.

Claim 7.4. *There exists $C>0$ such that w.h.p. $\mathbb{P}\left[\|\rho_{\boldsymbol{\sigma}}-q^{-1}\boldsymbol{\Delta}\mathbb{1}\|_1>t\sqrt{\boldsymbol{\Delta}}\mid\mathfrak{A}\right]\leq C\exp(-nt^2/C)$ for all $t>0$.*

Proof. Since $\mathbb{E}[\boldsymbol{d}^2]<\infty$, this is an immediate consequence of Azuma–Hoeffding. □

Let us move on to the probability term. We proceed indirectly by way of Bayes' rule. Hence, fix $\rho\in\mathfrak{P}_q(\varepsilon)$ and let $\boldsymbol{\xi}=(\boldsymbol{\xi}_{ij})_{i,j\geq1}$ be an infinite array of $\mathbb{F}_q$-valued random variables with distribution $\boldsymbol{\Delta}^{-1}\rho$, mutually independent and independent of all other randomness. Moreover, let

$$\mathfrak{R}(\rho)=\bigcap_{s\in\mathbb{F}_q}\left\{\sum_{i=1}^{\boldsymbol{m}}\sum_{j=1}^{\boldsymbol{k}_i}\mathbb{1}\{\boldsymbol{\xi}_{ij}=s\}=\rho(s)\right\},\qquad\mathfrak{S}=\left\{\forall i\in[\boldsymbol{m}]:\sum_{j=1}^{\boldsymbol{k}_i}\boldsymbol{\chi}_{ij}\boldsymbol{\xi}_{ij}=0\right\}.\tag{7.5}$$

In words, $\mathfrak{R}(\rho)$ is the event that the empirical distribution induced by the random vector $\boldsymbol{\xi}_{ij}$, truncated at $i=\boldsymbol{m}$ and $j=\boldsymbol{k}_i$ for every i, works out to be $\rho\in\mathfrak{P}_q$. Furthermore, $\mathfrak{S}$ is the event that all $\boldsymbol{m}$ checks are satisfied if we substitute the independent values $\boldsymbol{\xi}_{ij}$ for the variables.

Crucially, $\mathfrak{S}$ ignores that the various equations share variables, or conversely that variables may appear in several distinct checks. Hence, the *unconditional* event $\mathfrak{S}$ effectively just deals with a linear system whose Tanner graph consists of $\boldsymbol{m}$ checks with degrees $\boldsymbol{k}_1,\ldots,\boldsymbol{k}_{\boldsymbol{m}}$ and $\sum_{i=1}^{\boldsymbol{m}}\boldsymbol{k}_i$ variable nodes of degree one each. However, the *conditional* probability $\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{S}\mid\mathfrak{R}(\rho)\right]$ equals the probability that a random assignment $\boldsymbol{\sigma}$ lies in the kernel of $\boldsymbol{A}$ given that $\rho_{\boldsymbol{\sigma}}=\rho$; in symbols,

$$\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{S}\mid\mathfrak{R}(\rho)\right]=\mathbb{P}_{\mathfrak{A}}\left[\boldsymbol{\sigma}\in\ker\boldsymbol{A}\mid\rho_{\boldsymbol{\sigma}}=\rho\right].\tag{7.6}$$

Indeed, given $\mathfrak{A}$ and given $\rho_{\boldsymbol{\sigma}}=\rho$ the randomness that remains amounts to just how the variable clones are matched to the check clones to form the random Tanner graph $\boldsymbol{G}$. We can think of this matching as randomly distributing $\sum_{i=1}^{n}\boldsymbol{d}_i\rho(s)$ "pebbles" with value s onto the $\boldsymbol{m}$ equations. The probability that the pebbles happen to satisfy all the equations is precisely equal to $\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{S}\mid\mathfrak{R}(\rho)\right]$.

We are going to see momentarily that the unconditional probabilities of $\mathfrak{R}(\rho)$ and $\mathfrak{S}$ are easy to calculate. In addition, we will be able to calculate the conditional probability $\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{S}\mid\mathfrak{R}(\rho)\right]$ by way of the local limit theorem for sums of independent random variables. Finally, Lemma 7.2 will follow from these estimates via Bayes' rule.

Claim 7.5. *We have $\mathbb{P}_{\mathfrak{A}}[\mathfrak{S}]=q^{\boldsymbol{m}(O(\sum_{s\in\mathbb{F}_q}|\boldsymbol{\Delta}^{-1}\rho(s)-1/q|^3)-1)}$.*

Proof. For any $h\geq3$ and any $\chi_1,\ldots,\chi_h\in\mathrm{supp}\chi$ we aim to calculate

$$P_h=\log\sum_{\sigma\in\mathbb{F}_q^h}\mathbb{1}\left\{\sum_{i=1}^{h}\chi_i\sigma_i=0\right\}\prod_{i=1}^{h}\frac{\rho(\sigma_i)}{\boldsymbol{\Delta}}.$$

The derivatives of this expression work out to be

$$\begin{aligned}
\frac{\partial P_h}{\partial\rho_s}&=\frac{\sum_{j=1}^{h}\sum_{\sigma\in\mathbb{F}_q^h}\mathbb{1}\{\sum_{i=1}^{h}\chi_i\sigma_i=0,\sigma_j=s\}\prod_{i\neq j}\frac{\rho(\sigma_i)}{\boldsymbol{\Delta}}}{\boldsymbol{\Delta}\mathrm{e}^{P_h}}&&(s\in\mathbb{F}_q),\\
\frac{\partial^2P_h}{\partial\rho_s\partial\rho_{s'}}&=\frac{\sum_{j,j'=1}^{h}\sum_{\sigma\in\mathbb{F}_q^h}\mathbb{1}\{\sum_{i=1}^{h}\chi_i\sigma_i=0,\sigma_j=s,\sigma_{j'}=s'\}\prod_{i\neq j,j'}\frac{\rho(\sigma_i)}{\boldsymbol{\Delta}}}{\boldsymbol{\Delta}^2\mathrm{e}^{P_h}}-\frac{\partial P_h}{\partial\rho_s}\frac{\partial P_h}{\partial\rho'_s}&&(s,s'\in\mathbb{F}_q,\ s\neq s'),\\
\frac{\partial^2P_h}{\partial\rho_s^2}&=\frac{\sum_{j\neq j'}\sum_{\sigma\in\mathbb{F}_q^h}\mathbb{1}\{\sum_{i=1}^{h}\chi_i\sigma_i=0,\sigma_j=\sigma_{j'}=s\}\prod_{i\neq j,j'}\frac{\rho(\sigma_i)}{\boldsymbol{\Delta}}}{\boldsymbol{\Delta}^2\mathrm{e}^{P_h}}-\left(\frac{\partial P_h}{\partial\rho_s}\right)^2.
\end{aligned}$$

Evaluating the derivatives at the equitable $\bar\rho=q^{-1}\boldsymbol{\Delta}\mathbb{1}$ we obtain for any $i\geq3$,

$$\begin{aligned}
\frac{\partial P_h}{\partial\rho_s}\Big|_{\bar\rho}&=\frac{hq^{-1}}{\boldsymbol{\Delta}q^{-1}}=\frac{h}{\boldsymbol{\Delta}},\\
\frac{\partial^2P_h}{\partial\rho_s\partial\rho_{s'}}\Big|_{\bar\rho}&=\frac{h(h-1)q^{-1}}{\boldsymbol{\Delta}^2q^{-1}}-\frac{h^2}{\boldsymbol{\Delta}^2}=-\frac{h}{\boldsymbol{\Delta}^2},&&(s\neq s')\\
\frac{\partial^2P_h}{\partial\rho_s^2}\Big|_{\bar\rho}&=\frac{h(h-1)q^{-1}}{\boldsymbol{\Delta}^2q^{-1}}-\frac{h^2}{\boldsymbol{\Delta}^2}=-\frac{h}{\boldsymbol{\Delta}^2}.
\end{aligned}$$

Hence, the Jacobi matrix and the Hessian work out to be

$$DP_h(\bar\rho) = \frac{h}{\boldsymbol\Delta}\mathbb{1}_q, \qquad D^2P_h(\bar\rho) = -\frac{h}{\boldsymbol\Delta^2}\mathbb{1}_{q\times q}. \tag{7.7}$$

Furthermore, the third partial derivatives are clearly bounded, i.e.,

$$\frac{\partial^3 P_h}{\partial\rho_s\partial\rho_{s'}\partial\rho_{s''}} = O_\varepsilon(1). \tag{7.8}$$

Since $\rho-\bar\rho\perp\mathbb{1}$, (7.7), (7.8) and Taylor's theorem imply the assertion. □

Claim 7.6. *W.h.p. we have* $\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{R}(\rho)\right] = \Omega_\varepsilon(n^{(1-q)/2})$.

Proof. Since the $\boldsymbol\xi_{ij}$ are mutually independent, the probability of $\mathfrak{R}(\rho)$ given $\mathfrak{A}$ is nothing but

$$\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{R}(\rho)\right] = \binom{\boldsymbol\Delta}{(\rho(s))_{s\in\mathbb{F}_q}}\prod_{s\in\mathbb{F}_q}\left(\frac{\rho(s)}{\boldsymbol\Delta}\right)^{\rho(s)}.$$

The claim therefore follows from Stirling's formula. □

Claim 7.7. *W.h.p. we have* $\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{R}(\rho)\mid\mathfrak{S}\right] = O_\varepsilon(n^{(1-q)/2})$.

Proof. The claim follows from the local limit theorem for the sums of independent random variables (e.g. [18]). To elaborate, even once we condition on the event $\mathfrak{S}$ the random *vectors* $(\boldsymbol\xi_{ij})_{j\in[\boldsymbol k_i]}$, $1\le i\le\boldsymbol m$, remain independent for different $i\in[\boldsymbol m]$ due to the independence of the $(\boldsymbol\xi_{ij})_{i,j}$. Indeed, $\mathfrak{S}$ only asks that each check be satisfied separately, without inducing dependencies among different checks. Thus, the vector

$$\left(\sum_{i=1}^{\boldsymbol m}\sum_{j=1}^{\boldsymbol k_i}\mathbb{1}\{\boldsymbol\xi_{ij}=s\}\right)_{s\in\mathbb{F}_q}\qquad\text{given }\mathfrak{S}$$

is a sum of $\boldsymbol m$ independent random vectors. The local limit theorem therefore implies that the probability of the most likely outcome of this random vector is of order $n^{(1-q)/2}$; in symbols,

$$\max_{r\in\mathfrak{P}_q(\varepsilon)}\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{R}(r)\mid\mathfrak{S}\right] = O(n^{(1-q)/2}). \tag{7.9}$$

The assertion is an immediate consequence of (7.9). □

Proof of Lemma 7.2. Fix $\rho\in\mathfrak{P}_q(\varepsilon)$ such that $\omega\sqrt{\boldsymbol\Delta}\le\sum_{s\in\mathbb{F}_q}|\rho(s)-\boldsymbol\Delta/q|\le\varepsilon\boldsymbol\Delta$. Combining Claims 7.5–7.7 with Bayes' rule, we conclude that w.h.p.

$$\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{S}\mid\mathfrak{R}(\rho)\right] = \frac{\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{S}\right]\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{R}(\rho)\mid\mathfrak{S}\right]}{\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{R}(\rho)\right]} = O(\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{S}\right]) = q^{\boldsymbol m(O(\sum_{s\in\mathbb{F}_q}|\rho(s)/\boldsymbol\Delta-1/q|^3)-1)+O(1)}. \tag{7.10}$$

Consequently, (7.6) and (7.10) imply that

$$\mathbb{P}_{\mathfrak{A}}\left[\boldsymbol\sigma\in\ker\boldsymbol A\mid\rho_{\boldsymbol\sigma}=\rho\right] = \mathbb{P}_{\mathfrak{A}}\left[\mathfrak{S}\mid\mathfrak{R}(\rho)\right] = q^{\boldsymbol m(O(\sum_{s\in\mathbb{F}_q}|\rho(s)/\boldsymbol\Delta-1/q|^3)-1)+O(1)}. \tag{7.11}$$

Hence, combining Claim 7.4 with (7.11) and using the bound $\sum_{s\in\mathbb{F}_q}|\rho(s)-\boldsymbol\Delta/q|\le\varepsilon\boldsymbol\Delta$, we obtain

$$\mathbb{P}_{\mathfrak{A}}\left[\boldsymbol\sigma\in\ker\boldsymbol A,\rho_{\boldsymbol\sigma}=\rho\right] = q^{\boldsymbol m(O(\sum_{s\in\mathbb{F}_q}|\rho(s)/\boldsymbol\Delta-1/q|^3)-(\Omega(\sum_{s\in\mathbb{F}_q}|\rho(s)/\boldsymbol\Delta-1/q|^2)-1)+O(1)} = q^{\boldsymbol m(-1-\Omega(\sum_{s\in\mathbb{F}_q}|\rho(s)/\boldsymbol\Delta-1/q|^2)+O(1)}. \tag{7.12}$$

Multiplying (7.12) with q^n and summing on $\rho\in\mathfrak{P}_q(\varepsilon)$ such that $\omega n^{-1/2}\boldsymbol\Delta\le\sum_{s\in\mathbb{F}_q}|\rho(s)-\boldsymbol\Delta/q|$, we finally obtain

$$\mathbb{E}_{\mathfrak{A}}\left[\mathcal{Z}_{\omega n^{-1/2},\varepsilon}\right] = q^{n-\boldsymbol m+O(1)}\sum_{\substack{\rho\in\mathfrak{P}\\ \omega n^{-1/2}\boldsymbol\Delta\le\sum_{s\in\mathbb{F}_q}|\rho(s)-\boldsymbol\Delta/q|<\varepsilon\boldsymbol\Delta}}\exp\left(-\Omega\left(n\sum_{s\in\mathbb{F}_q}|\rho(s)/\boldsymbol\Delta-1/q|^2\right)\right) < \varepsilon q^{n-\boldsymbol m},$$

provided $\omega=\omega(\varepsilon)>0$ is chosen large enough. □

7.3. **Proof of Lemma 7.3.** By comparison to the proof of Lemma 7.2, the main difference here is that we need to be more precise. Specifically, while in Claims 7.6 and 7.7 we got away with disregarding constant factors, here we need to be accurate up to a multiplicative $1+o(1)$. Working out the probability term turns out to be delicate. As in Section 7.2 we introduce auxiliary $\mathbb{F}_q$-valued random variables $\boldsymbol{\xi} = (\boldsymbol{\xi}_{ij})_{i,j\geq 1}$. These random variables are mutually independent as well as independent of all other randomness. But this time all $\boldsymbol{\xi}_{ij}$ are *uniform* on $\mathbb{F}_q$. Let $\mathfrak{R}(\rho)$ and $\mathfrak{S}$ be the events from (7.5).

Similarly as in Section 7.2 we will ultimately apply Bayes' rule to compute the probability of $\mathfrak{S}$ given $\mathfrak{R}(\rho)$ and hence the conditional mean of $\mathcal{Z}_\rho$. The individual probability $\mathfrak{R}(\rho)$ is easy to compute.

Claim 7.8. *For any $\rho \in \mathfrak{P}_q$ we have $\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{R}(\rho)\right] = \binom{\boldsymbol{\Delta}}{\rho} q^{-\boldsymbol{\Delta}}$.*

Proof. This is similar to the proof of Claim 7.6. As the $\boldsymbol{\xi}_{ij}$ are uniformly distributed and independent, we obtain

$$\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{R}(\rho)\right] = \binom{\boldsymbol{\Delta}}{(\rho(s))_{s\in\mathbb{F}_q}} \prod_{s\in\mathbb{F}_q} q^{-\sum_{s\in\mathbb{F}_q}\rho(s)} = \binom{\boldsymbol{\Delta}}{\rho} q^{-\boldsymbol{\Delta}},$$

as claimed. □

As a next step we calculate the conditional probability of $\mathfrak{S}$ given $\mathfrak{R}(\rho)$. Similar to (7.1), for $s \in \mathbb{F}_q$ define the empirical frequency

$$\boldsymbol{\rho}(s) = \sum_{i=1}^{\boldsymbol{m}} \sum_{j=1}^{\boldsymbol{k}_i} \mathbb{1}\{\boldsymbol{\xi}_{ij} = s\} \tag{7.13}$$

and let $\boldsymbol{\rho} = (\boldsymbol{\rho}(s))_{s\in\mathbb{F}_q}$ as well as $\hat{\boldsymbol{\rho}} = (\boldsymbol{\rho}(s))_{s\in\mathbb{F}_q^*}$. Of course, Proposition 2.3 implies that for some $\rho \in \mathfrak{P}_q$ the event $\mathfrak{S}$ may be impossible given $\mathfrak{R}(\rho)$. Hence, to characterise the distributions ρ for which $\mathfrak{S}$ can occur at all, we let

$$\mathfrak{L} = \left\{r \in \mathbb{Z}^{\mathbb{F}_q^*} : \mathbb{P}_{\mathfrak{A}}\left[\hat{\boldsymbol{\rho}} = r\right] > 0 \text{ and } \left\|r - q^{-1}\boldsymbol{\Delta}\mathbb{1}\right\|_1 \leq \omega n^{-1/2}\boldsymbol{\Delta}\right\}, \tag{7.14}$$

$$\mathfrak{L}_0 = \left\{r \in \mathfrak{L} : \mathbb{P}_{\mathfrak{A}}\left[\hat{\boldsymbol{\rho}} = r \mid \mathfrak{S}\right] > 0\right\}, \tag{7.15}$$

$$\mathfrak{L}_* = \left\{r \in \mathfrak{L} : \mathbb{P}_{\mathfrak{A}}\left[\hat{\rho}_{\boldsymbol{\sigma}} = r\right] > 0\right\}. \tag{7.16}$$

Thus, $\mathfrak{L}$ contains all conceivable outcomes of truncated frequency vectors. Moreover, $\mathfrak{L}_0$ comprises those frequency vectors that can occur given $\mathfrak{S}$, and $\mathfrak{L}_*$ those that can result from random assignments $\boldsymbol{\sigma}$ to the variables. Hence, $\mathfrak{L}_0$ is a finite subset of the $\mathbb{Z}$-module generated by those sets $\mathscr{S}_q(\chi_1,\ldots,\chi_\ell)$ from (2.13) with $\boldsymbol{m}(\chi_1,\ldots,\chi_\ell) > 0$. The following lemma shows that actually the conditional probability $\mathfrak{S}$ given $\mathfrak{R}(\rho)$ is asymptotically the same for all $\rho \in \mathfrak{L}_0$, i.e., for all conceivably satisfying ρ that are nearly equitable.

Lemma 7.9. *W.h.p. uniformly for all $r \in \mathfrak{L}_0$ we have $\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{S} \mid \hat{\boldsymbol{\rho}} = r\right] \sim q^{\mathbb{1}\{|\mathrm{supp}\boldsymbol{\chi}|=1\}-\boldsymbol{m}}$.*

We complement Lemma 7.9 by the following estimate of the probability that a uniformly random assignment $\boldsymbol{\sigma} \in \mathbb{F}_q^n$ hits the set $\mathfrak{L}_0$ in the first place.

Lemma 7.10. *W.h.p. we have $\mathbb{P}_{\mathfrak{A}}\left[\hat{\rho}_{\boldsymbol{\sigma}} \in \mathfrak{L}_0\right] \leq (1+o(1))\, q^{-\mathbb{1}\{|\mathrm{supp}\boldsymbol{\chi}|=1\}}$.*

We prove Lemmas 7.9 and 7.10 in Sections 7.4 and 7.5, respectively.

Proof of Lemma 7.3. The formula (7.6) extends to the present auxiliary probability space with uniformly distributed and independent $\boldsymbol{\xi}_{ij}$ (for precisely the same reasons given in Section 7.2). Hence, (7.6), (7.14) and (7.15) show that

$$\mathbb{E}[\mathcal{Z}_{\omega n^{-1/2}} \mid \mathfrak{A}] \leq \sum_{\sigma\in\mathbb{F}_q^n} \mathbb{1}\{\hat{\rho}_\sigma \in \mathfrak{L}\}\, \mathbb{P}_{\mathfrak{A}}\left[\mathfrak{S} \mid \hat{\boldsymbol{\rho}} = \hat{\rho}_\sigma\right] = \sum_{\sigma\in\mathbb{F}_q^n} \mathbb{1}\{\hat{\rho}_\sigma \in \mathfrak{L}_0\}\, \mathbb{P}_{\mathfrak{A}}\left[\mathfrak{S} \mid \hat{\boldsymbol{\rho}} = \hat{\rho}_\sigma\right]. \tag{7.17}$$

Finally, combining (7.17) with Lemma 7.9 and Lemma 7.10, we obtain

$$\begin{aligned}\mathbb{E}[\mathcal{Z}_{\omega n^{-1/2}} \mid \mathfrak{A}] &\leq (1+o(1))\, q^{\mathbb{1}\{|\mathrm{supp}\boldsymbol{\chi}|=1\}-\boldsymbol{m}} \sum_{\sigma\in\mathbb{F}_q^n} \mathbb{1}\{\hat{\rho}_\sigma \in \mathfrak{L}_0\} \\ &= (1+o(1))\, q^{n-\boldsymbol{m}+\mathbb{1}\{|\mathrm{supp}\boldsymbol{\chi}|=1\}}\, \mathbb{P}_{\mathfrak{A}}\left[\hat{\rho}_{\boldsymbol{\sigma}} \in \mathfrak{L}_0\right] \leq (1+o(1))\, q^{n-\boldsymbol{m}},\end{aligned}$$

as desired. □

7.4. **Proof of Lemma 7.9.** Given $\omega > 0$ (from (7.14)) we choose $\varepsilon_0 = \varepsilon_0(\omega, q)$ sufficiently small and let $0 < \varepsilon < \varepsilon_0$. Moreover, recall that we assume the existence of a constant $\eta > 0$ such that $\mathbb{E}[\boldsymbol{d}^{2+\eta}] + \mathbb{E}[\boldsymbol{k}^{2+\eta}] < \infty$. The proof hinges on a careful analysis of the conditional distribution of $\hat{\boldsymbol{\rho}}$ given $\mathfrak{S}$. We begin by observing that the vector $\hat{\boldsymbol{\rho}}$ is asymptotically normal given $\mathfrak{S}$. Let $\boldsymbol{I}_{q-1}$ the $(q-1)\times(q-1)$-identity matrix and let $\boldsymbol{N} \in \mathbb{R}^{\mathbb{F}_q^*}$ be a Gaussian vector with zero mean and covariance matrix

$$\mathscr{C} = q^{-1}\boldsymbol{I}_{q-1} - q^{-2}\mathbb{1}_{(q-1)\times(q-1)}. \tag{7.18}$$

Claim 7.11. *There exists a function $\alpha = \alpha(n,q,\eta) = o(1)$ such that for all axis-aligned cubes $U \subseteq \mathbb{R}^{\mathbb{F}_q^*}$ we have*

$$\mathbb{E}\left|\mathbb{P}_{\mathfrak{A}}\left[\boldsymbol{\Delta}^{-1/2}(\hat{\boldsymbol{\rho}} - q^{-1}\boldsymbol{\Delta}\mathbb{1}) \in U \mid \mathfrak{S}\right] - \mathbb{P}\left[\boldsymbol{N} \in U\right]\right| \le \alpha.$$

Proof. The conditional mean of $\hat{\boldsymbol{\rho}}$ given $\mathfrak{S}$ is uniform. To see this, consider any $i \in [\boldsymbol{m}]$ and $h \in [\boldsymbol{k}_i]$. We claim that for any vector $(\tau_j)_{j\in[\boldsymbol{k}_i]\setminus\{h\}}$,

$$\mathbb{P}_{\mathfrak{A}}\left[\forall j \in [\boldsymbol{k}_i]\setminus\{h\} : \boldsymbol{\xi}_{ij} = \tau_j \mid \mathfrak{S}\right] \sim q^{1-\boldsymbol{k}_i}. \tag{7.19}$$

Indeed, for any such vector $(\tau_j)_{j\in[\boldsymbol{k}_i]\setminus\{h\}}$ there is exactly one value $\boldsymbol{\xi}_{ih}$ that will satisfy the constraint, namely

$$\boldsymbol{\xi}_{ih} = -\boldsymbol{\chi}_{ih}^{-1}\sum_{j\in[\boldsymbol{k}_i]\setminus\{h\}}\boldsymbol{\chi}_{ij}\tau_j.$$

Hence, given $\mathfrak{S}$ the events $\{\forall j \in [\boldsymbol{k}_i]\setminus\{h\} : \boldsymbol{\xi}_{ij} = \tau_j\}$ are equally likely for all τ, which implies (7.19). Furthermore, together with the definition (7.13) of $\boldsymbol{\rho}$, (7.19) readily implies that $\mathbb{E}_{\mathfrak{A}}\left[\hat{\boldsymbol{\rho}}\right] = q^{-1}\boldsymbol{\Delta}\mathbb{1}$. Similarly, (7.19) also shows that $\boldsymbol{\Delta}^{-1/2}\hat{\boldsymbol{\rho}}$ has covariance matrix $\mathscr{C}$.

Finally, we are left to prove the desired uniform convergence to the normal distribution. To this end we employ the multivariate Berry-Esseen theorem (e.g., [41]). Specifically, given a small $\alpha > 0$ choose $K = K(q,\eta,\alpha) > 0$ and $m_0 = m_0(K)$, $n_0 = n_0(K, m_0)$ sufficiently large. Assuming $n > n_0$, we can ensure that w.h.p. $\boldsymbol{m} > m_0$. Also let

$$\boldsymbol{k}_i' = \mathbb{1}\{\boldsymbol{k}_i \le K\}\boldsymbol{k}_i, \qquad \boldsymbol{k}_i'' = \boldsymbol{k}_i - \boldsymbol{k}_i',$$

$$\hat{\boldsymbol{\rho}}'(s) = \sum_{1\le i\le\boldsymbol{m}:\boldsymbol{k}_i\le K}\sum_{j=1}^{\boldsymbol{k}_i}\mathbb{1}\{\boldsymbol{\xi}_{ij} = s\}, \qquad \hat{\boldsymbol{\rho}}''(s) = \sum_{1\le i\le\boldsymbol{m}:\boldsymbol{k}_i> K}\sum_{j=1}^{\boldsymbol{k}_i}\mathbb{1}\{\boldsymbol{\xi}_{ij} = s\},$$

$$\boldsymbol{\Delta}' = \sum_{i=1}^{n}\boldsymbol{k}_i', \qquad \boldsymbol{\Delta}'' = \sum_{i=1}^{n}\boldsymbol{k}_i''.$$

Then the assumtion $\mathbb{E}[\boldsymbol{k}^{2+\eta}] < \infty$ and Markov's inequality ensure that w.h.p.

$$\boldsymbol{\Delta}'' < \alpha^8\boldsymbol{\Delta}. \tag{7.20}$$

Moreover, by the same reasoning as in the previous paragraph the random vectors $\hat{\boldsymbol{\rho}}'$ and $\hat{\boldsymbol{\rho}}''$ have means $q^{-1}\boldsymbol{\Delta}'$ and $q^{-1}\boldsymbol{\Delta}''$ and covariances $\boldsymbol{\Delta}'\mathscr{C}$ and $\boldsymbol{\Delta}''\mathscr{C}$, respectively. Thus, (7.20) and Chebyshev's inequality show that w.h.p.

$$\mathbb{P}_{\mathfrak{A}}\left[\left\|\frac{\hat{\boldsymbol{\rho}}'' - q^{-1}\boldsymbol{\Delta}''\mathbb{1}}{\boldsymbol{\Delta}^{1/2}}\right\| > \alpha^2\right] < \alpha^2. \tag{7.21}$$

Further, the Berry–Esseen theorem shows that w.h.p.

$$\mathbb{P}_{\mathfrak{A}}\left[\frac{\hat{\boldsymbol{\rho}}' - q^{-1}\boldsymbol{\Delta}'\mathbb{1}}{\sqrt{\boldsymbol{\Delta}'}} \in U\right] - \mathbb{P}\left[\boldsymbol{N} \in U\right] = O(n^{-1/2}) \qquad \text{for all cubes } U. \tag{7.22}$$

Combining (7.22) and (7.21), we see that w.h.p.

$$\left|\mathbb{P}_{\mathfrak{A}}\left[\frac{\hat{\boldsymbol{\rho}} - q^{-1}\boldsymbol{\Delta}\mathbb{1}}{\sqrt{\boldsymbol{\Delta}}} \in U\right] - \mathbb{P}\left[\boldsymbol{N} \in U\right]\right| \le \alpha. \tag{7.23}$$

The assertion follows from (7.23) by taking $\alpha \to 0$ slowly as $n \to \infty$. □

The following claim states that the normal approximation from Claim 7.11 also holds for the unconditional random vector $\hat{\boldsymbol{\rho}}$.

Claim 7.12. *There exists a function $\alpha = \alpha(n,q,\eta) = o(1)$ such that w.h.p. for all convex sets $U \subseteq \mathbb{R}^{\mathbb{F}_q^*}$ we have*

$$\left|\mathbb{P}_{\mathfrak{A}}\left[\boldsymbol{\Delta}^{-1/2}(\hat{\boldsymbol{\rho}} - q^{-1}\boldsymbol{\Delta}\mathbb{1}) \in U\right] - \mathbb{P}\left[\boldsymbol{N} \in U\right]\right| \le \alpha.$$

Proof. This is an immediate consequence of Claim 7.8 and Stirling's formula. □

Let $k_0 = \min \operatorname{supp} \boldsymbol{k}$. In the case that $|\operatorname{supp}\boldsymbol{\chi}| = 1$ we set $\chi_1 = \cdots = \chi_{k_0}$ to the single element of $\operatorname{supp}\boldsymbol{\chi}$. Moreover, in the case that $|\operatorname{supp}\boldsymbol{\chi}| > 1$ we pick and fix any $\chi_1, \dots, \chi_{k_0} \in \operatorname{supp}\boldsymbol{\chi}$ such that $|\{\chi_1, \dots, \chi_{k_0}\}| > 1$. Let $\mathfrak{I}_0$ be the set of all $i \in [\boldsymbol{m}]$ such that $\boldsymbol{k}_i = k_0$ and $\boldsymbol{\chi}_{ij} = \chi_j$ for $j = 1, \dots, k_0$ and let $\mathfrak{I}_1 = [\boldsymbol{m}] \setminus \mathfrak{I}_0$. Then $|\mathfrak{I}_0|, |\mathfrak{I}_1| = \Theta(n)$ w.h.p. Further, set

$$\boldsymbol{r}_0(s) = \sum_{i \in \mathfrak{I}_0} \sum_{j \in [\boldsymbol{k}_i]} \mathbb{1}\{\boldsymbol{\xi}_{ij} = s\}, \qquad \boldsymbol{r}_1(s) = \sum_{i \in \mathfrak{I}_1} \sum_{j \in [\boldsymbol{k}_i]} \mathbb{1}\{\boldsymbol{\xi}_{ij} = s\} \qquad (s \in \mathbb{F}_q^*).$$

Then $\hat{\boldsymbol{\rho}} = \boldsymbol{r}_0 + \boldsymbol{r}_1$.

Because the vectors $\boldsymbol{\xi}_i = (\boldsymbol{\xi}_{i,1}, \dots, \boldsymbol{\xi}_{i,\boldsymbol{k}_i})$ are mutually independent, so are $\boldsymbol{r}_0 = (\boldsymbol{r}_0(s))_{s \in \mathbb{F}_q^*}$ and $\boldsymbol{r}_1 = (\boldsymbol{r}_1(s))_{s \in \mathbb{F}_q^*}$. To analyse $\boldsymbol{r}_0$ precisely, let

$$\mathscr{S}_0 = \left\{ \sigma \in \mathbb{F}_q^{k_0} : \sum_{i=1}^{k_0} \chi_i \sigma_i = 0 \right\}.$$

Moreover, for $\sigma \in \mathscr{S}_0$ let $\boldsymbol{R}_\sigma$ be the number of indices $i \in \mathfrak{I}_0$ such that $\boldsymbol{\xi}_i = \sigma$. Then conditionally on $\mathfrak{S}$, we have

$$\boldsymbol{r}_0(s) = \sum_{i \in \mathfrak{I}_0} \sum_{j \in [\boldsymbol{k}_i]} \mathbb{1}\{\boldsymbol{\xi}_{ij} = s\} = \sum_{\sigma \in \mathscr{S}_0} \sum_{j=1}^{k_0} \mathbb{1}\{\sigma_j = s\} \boldsymbol{R}_\sigma \qquad \text{given } \mathfrak{S},$$

which reduces our task to the investigation of $\boldsymbol{R} = (\boldsymbol{R}_\sigma)_{\sigma \in \mathscr{S}_0}$.

This is not too difficult because given $\mathfrak{S}$ the random vector $\boldsymbol{R}$ has a multinomial distribution with parameter $|\mathfrak{I}_0|$ and uniform probabilities $|\mathscr{S}_0|^{-1}$. In effect, the individual entries $\boldsymbol{R}(\sigma)$, $\sigma \in \mathfrak{S}_0$, will typically differ by only a few standard deviations, i.e., their typically difference will be of order $O(\sqrt{\boldsymbol{\Delta}})$. We require a precise quantitative version of this statement.

Recalling the sets from (7.14)–(7.16), for $r_* \in \mathfrak{L}_0$ and $0 < \varepsilon < \varepsilon_0$ we let

$$\mathfrak{L}_0(r_*, \varepsilon) = \left\{ r \in \mathfrak{L}_0 : \|r - r_*\|_\infty < \varepsilon \sqrt{\boldsymbol{\Delta}} \right\}.$$

Furthermore, we say that $\boldsymbol{R}$ is *t-tame* if $|\boldsymbol{R}_\sigma - |\mathscr{S}_0|^{-1}|\mathfrak{I}_0|| \le t\sqrt{\boldsymbol{\Delta}}$ for all $\sigma \in \mathscr{S}_0$. Let $\mathfrak{T}(t)$ be the event that $\boldsymbol{R}$ is t-tame.

Lemma 7.13. *W.h.p. for every $r_* \in \mathfrak{L}_0$ there exists $r^* \in \mathfrak{L}_0(r_*, \varepsilon)$ such that*

$$\mathbb{P}_{\mathfrak{A}}\left[\hat{\boldsymbol{\rho}} = r^* \mid \mathfrak{S}\right] \ge \frac{1}{2|\mathfrak{L}_0(r_*, \varepsilon)|} \qquad \textit{and} \qquad \mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(-\log\varepsilon) \mid \mathfrak{S}, \hat{\boldsymbol{\rho}} = r^*\right] \ge 1 - \varepsilon^4. \tag{7.24}$$

Proof. Recall that the event $\{\hat{\rho} = r\}$ is the same as $\mathfrak{R}(r')$ with $r'(s) = r(s)$ for $s \in \mathbb{F}_q^*$ and $r'(0) = \boldsymbol{\Delta} - \|r\|_1$. As a first step we observe that $\boldsymbol{R}$ given $\mathfrak{S}$ is reasonably tame with a reasonably high probability. More precisely, since $\boldsymbol{R}$ has a multinomial distribution given $\mathfrak{A}$ and $\mathfrak{S}$, the Chernoff bound shows that w.h.p.

$$\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(-\log\varepsilon) \mid \mathfrak{S}\right] \ge 1 - \exp(-\Omega_\varepsilon(\log^2(\varepsilon))). \tag{7.25}$$

Further, Claim 7.11 implies that $\mathbb{P}_{\mathfrak{A}}\left[\hat{\boldsymbol{\rho}} \in \mathfrak{L}_0(r_*, \varepsilon) \mid \mathfrak{S}\right] \ge \Omega_\varepsilon(\varepsilon^{q-1}) \ge \varepsilon^q$ w.h.p., provided $\varepsilon < \varepsilon_0 = \varepsilon_0(\omega)$ is small enough. Combining this estimate with (7.25) and Bayes' formula, we conclude that w.h.p. for every $r_* \in \mathfrak{L}_0$,

$$\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(-\log\varepsilon) \mid \mathfrak{S}, \hat{\boldsymbol{\rho}} \in \mathfrak{L}_0(r_*, \varepsilon)\right] \ge 1 - \varepsilon^5. \tag{7.26}$$

To complete the proof, assume that there does not exist $r^* \in \mathfrak{L}_0(r_*, \varepsilon)$ that satisfies (7.24). Then for every $r \in \mathfrak{L}_0(r_*, \varepsilon)$ we either have

$$\mathbb{P}_{\mathfrak{A}}\left[\hat{\boldsymbol{\rho}} = r \mid \mathfrak{S}\right] < \frac{1}{2|\mathfrak{L}_0(r_*, \varepsilon)|} \qquad \text{or} \tag{7.27}$$

$$\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(-\log\varepsilon) \mid \mathfrak{S}, \hat{\boldsymbol{\rho}} = r\right] < 1 - \varepsilon^4. \tag{7.28}$$

Let $\mathfrak{X}_0$ be the set of all $r \in \mathfrak{L}_0(r_*, \varepsilon)$ for which (7.27) holds, and let $\mathfrak{X}_1 = \mathfrak{L}_0(r_*, \varepsilon) \setminus \mathfrak{X}_0$. Then (7.27)–(7.28) yield

$$\begin{aligned}\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(-\log\varepsilon) \mid \mathfrak{S}, \hat{\boldsymbol{\rho}} \in \mathfrak{L}_0(r_*, \varepsilon)\right] &\le \frac{\mathbb{P}_{\mathfrak{A}}\left[\hat{\boldsymbol{\rho}} \in \mathfrak{X}_0 \mid \mathfrak{S}\right] + \sum_{r \in \mathfrak{X}_1} \mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(-\log\varepsilon) \mid \mathfrak{S}, \hat{\boldsymbol{\rho}} = r\right] \mathbb{P}_{\mathfrak{A}}\left[\hat{\boldsymbol{\rho}} = r \mid \mathfrak{S}\right]}{\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{L}_0(r_*, \varepsilon) \mid \mathfrak{S}\right]} \\ &\le \frac{\mathbb{P}_{\mathfrak{A}}\left[\hat{\boldsymbol{\rho}} \in \mathfrak{X}_0 \mid \mathfrak{S}\right] + (1 - \varepsilon^4)\mathbb{P}_{\mathfrak{A}}\left[\hat{\boldsymbol{\rho}} \in \mathfrak{X}_1 \mid \mathfrak{S}\right]}{|\mathfrak{L}_0(r_*, \varepsilon)|} < 1 - \varepsilon^4,\end{aligned}$$

provided that $1 - \varepsilon^4 > \frac{1}{2}$, in contradiction to (7.26). □

Let $\mathfrak{M} = \mathfrak{M}_q(\chi_1,\dots,\chi_{k_0})$ and let $\mathfrak{b}_1,\dots,\mathfrak{b}_{q-1}$ be the basis of $\mathfrak{M}$ supplied by Proposition 2.3. Let us fix vectors $\tau^{(1)},\dots,\tau^{(q-1)} \in \mathscr{S}_0$ whose frequency vectors as defined in (2.14) coincide with $\mathfrak{b}_,\dots,\mathfrak{b}_{q-1}$, i.e.,

$$\hat{\tau}^{(i)} = \mathfrak{b}_i \qquad \text{for } i = 1,\dots,q-1.$$

Also let $\mathfrak{T}(r,t)$ be the event that $\hat{\boldsymbol{\rho}} = r$ and that $\boldsymbol{R}$ is t-tame. The following lemma summarises the key step of the proof of Lemma 7.9.

Lemma 7.14. *W.h.p. for any $r_* \in \mathfrak{L}_0$, any $1 \le t \le \log n$ and any $r, r' \in \mathfrak{L}_0(r_*,\varepsilon)$ there exists a one-to-one map $\psi : \mathfrak{T}(r,t) \to \mathfrak{T}(r', t + O_\varepsilon(\varepsilon))$ such that for all $(R,r_1) \in \mathfrak{T}(r,t)$ we have*

$$\log \frac{\mathbb{P}_{\mathfrak{A}}\left[(\boldsymbol{R},\boldsymbol{r}_1) = (R,r_1) \mid \mathfrak{S}\right]}{\mathbb{P}_{\mathfrak{A}}\left[(\boldsymbol{R},\boldsymbol{r}_1) = \psi(R,r_1) \mid \mathfrak{S}\right]} = O_\varepsilon(\varepsilon(\omega+t)). \tag{7.29}$$

Proof. Since $r, r' \in \mathfrak{M}$, we have $r - r' \in \mathfrak{M}$ w.h.p. Indeed, if $\operatorname{supp}\boldsymbol{\chi} > 1$, then Proposition 2.3 shows that $\mathfrak{M} = \mathbb{Z}^{\mathbb{F}_q^*}$ w.h.p. Moreover, if $\operatorname{supp}\boldsymbol{\chi} = 1$, then $\mathfrak{M}$ is a proper subset of the integer lattice $\mathbb{Z}^{\mathbb{F}_q^*}$. Nonetheless, Proposition 2.3 shows that the modules

$$\mathfrak{M}_q(\underbrace{1,\dots,1}_{\ell \text{ times}})$$

coincide for all $\ell \ge 3$, and therefore $\mathfrak{M}$ coincides with the $\mathbb{Z}$-module generated by $\mathfrak{L}_0$. Hence, in either case there is a unique representation

$$r - r' = \sum_{i=1}^{q-1} \lambda_i \mathfrak{b}_i \qquad (\lambda_i \in \mathbb{Z}) \tag{7.30}$$

in terms of the basis vectors. Because $r, r' \in \mathfrak{L}_0(r_*,\varepsilon)$ and

$$\begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_{q-1} \end{pmatrix} = \begin{pmatrix} \mathfrak{b}_1 & \cdots & \mathfrak{b}_{q-1} \end{pmatrix}^{-1} (r - r'),$$

the coefficients satisfy

$$|\lambda_i| = O_\varepsilon(\varepsilon\sqrt{\boldsymbol{\Delta}}) \qquad \text{for all } i = 1,\dots,q-1. \tag{7.31}$$

Now let $\lambda_0 = -\sum_{i=1}^{q-1} \lambda_i$, obtain the vector R' from R by amending the entry R'_0 corrsponding to the zero solution $0 \in \mathscr{S}_0$ to

$$R'_0 = R_0 + \lambda_0, \qquad \text{and setting} \qquad R'_{\tau^{(i)}} = R_{\tau^{(i)}} + \lambda_i \qquad \text{for all } \sigma \notin \{0,\tau^{(1)},\dots,\tau^{(q-1)}\}.$$

Further, define $\psi(R,r) = (R',r')$. Then $\psi(R,r) \in \mathfrak{T}(r', t + O_\varepsilon(\varepsilon))$ due to (7.30) and (7.31). Moreover, Stirling's formula and the mean value theorem show that

$$\begin{aligned}
\frac{\mathbb{P}_{\mathfrak{A}}\left[(\boldsymbol{R},\boldsymbol{r}_1) = (R,r_1) \mid \mathfrak{S}\right]}{\mathbb{P}_{\mathfrak{A}}\left[(\boldsymbol{R},\boldsymbol{r}_1) = \psi(R,r_1) \mid \mathfrak{S}\right]} &= \binom{|\mathfrak{I}_0|}{R|\mathfrak{I}_0|}\binom{|\mathfrak{I}_0|}{R'|\mathfrak{I}_0|}^{-1} = \exp\left[\sum_{\sigma\in\mathscr{S}_0} O_\varepsilon\left(R_\sigma \log R_\sigma - R'_\sigma \log R'_\sigma\right)\right] \\
&= \exp\left[O_\varepsilon(|\mathfrak{I}_0|)\sum_{\sigma\in\mathscr{S}_0}\left|\int_{R'_\sigma/|\mathfrak{I}_0|}^{R_\sigma/|\mathfrak{I}_0|} \log z \mathrm{d}z\right|\right] \\
&= \exp\left[O_\varepsilon(|\mathfrak{I}_0|)\sum_{\sigma\in\mathscr{S}_0}\left(\frac{R_\sigma}{|\mathfrak{I}_0|} - \frac{R'_\sigma}{|\mathfrak{I}_0|}\right)\log\left(\frac{1}{q} + O_\varepsilon\left(\frac{(\omega+t)\sqrt{\boldsymbol{\Delta}}}{|\mathfrak{I}_0|}\right)\right)\right] \\
&= \exp\left[O_\varepsilon(|\mathfrak{I}_0|)\sum_{\sigma\in\mathscr{S}_0} O_\varepsilon\left(\frac{(\omega+t)\sqrt{\boldsymbol{\Delta}}}{|\mathfrak{I}_0|}\left(\frac{R_\sigma}{|\mathfrak{I}_0|} - \frac{R'_\sigma}{|\mathfrak{I}_0|}\right)\right)\right].
\end{aligned} \tag{7.32}$$

Since $|\mathfrak{I}_0| = \Theta_\varepsilon(\boldsymbol{\Delta}) = \Theta_\varepsilon(n)$ w.h.p., (9.17) implies (9.13). Finally, ψ is one-to-one because each vector has a unique representation with respect to the basis $(\mathfrak{b}_1,\dots,\mathfrak{b}_{q-1})$. □

Roughly speaking, Lemma 7.14 shows that any two tame $r, r' \in \mathfrak{L}_0(r_*,\varepsilon)$ close to a conceivable $r_* \in \mathfrak{L}_0$ are about equally likely. However, the map ψ produces solutions that are a little less tame than the ones we start from. The following corollary, which combines Lemmas 7.13 and 7.14, remedies this issue.

Corollary 7.15. *W.h.p. for all $r_* \in \mathfrak{L}_0$ and all $r, r' \in \mathfrak{L}_0(r_*, \varepsilon)$ we have*

$$\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(r, -3\log\varepsilon) \mid \mathfrak{S}\right] = (1 + o_\varepsilon(1))\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(r', -3\log\varepsilon) \mid \mathfrak{S}\right].$$

Proof. Let r^* be the vector supplied by Lemma 7.13. Applying Lemma 7.14 to r^* and $r \in \mathfrak{L}_0(r_*, \varepsilon)$, we see that w.h.p.

$$\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(r, -2\log\varepsilon) \mid \mathfrak{S}\right] \geq (1 + O_\varepsilon(\varepsilon\log\varepsilon))\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(r^*, -\log\varepsilon) \mid \mathfrak{S}\right] \geq \frac{1}{3|\mathfrak{L}_0(r_*, \varepsilon)|} \qquad \text{for all } r \in \mathfrak{L}_0(r_*, \varepsilon). \tag{7.33}$$

In addition, we claim that w.h.p.

$$\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(r, -4\log\varepsilon) \setminus \mathfrak{T}(r, -3\log\varepsilon) \mid \mathfrak{S}\right] \leq \varepsilon\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(r^*, -\log\varepsilon) \mid \mathfrak{S}\right] \qquad \text{for all } r \in \mathfrak{L}_0(r_*, \varepsilon). \tag{7.34}$$

Indeed, applying Lemma 7.14 twice to r and r^* and invoking (7.24), we see that w.h.p.

$$\begin{aligned}\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(r, -2\log\varepsilon) \mid \mathfrak{S}\right] &\geq \exp(O_\varepsilon(\varepsilon\log\varepsilon))\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(r^*, -3\log\varepsilon) \mid \mathfrak{S}\right] \\ &\geq \left(1 - O_\varepsilon(\varepsilon\log\varepsilon)\right)\mathbb{P}_{\mathfrak{A}}\left[\hat{\boldsymbol{\rho}} = r^* \mid \mathfrak{S}\right], \qquad (7.35)\\ \mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(r, -4\log\varepsilon) \setminus \mathfrak{T}(r, -3\log\varepsilon) \mid \mathfrak{S}\right] &\leq \exp(O_\varepsilon(\varepsilon\log\varepsilon))\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(r^*, -3\log\varepsilon) \setminus \mathfrak{T}(r^*, -2\log\varepsilon) \mid \mathfrak{S}\right] \\ &\leq O_\varepsilon(\varepsilon^4)\mathbb{P}_{\mathfrak{A}}\left[\hat{\boldsymbol{\rho}} = r^* \mid \mathfrak{S}\right]. \qquad (7.36)\end{aligned}$$

Combining (7.35) and (7.36) yields (7.34).

Finally, (7.24), (7.33) and (7.34) show that w.h.p.

$$\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(-3\log\varepsilon) \mid \hat{\boldsymbol{\rho}} = r, \mathfrak{S}\right] \geq 1 - \sqrt{\varepsilon}, \quad \mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(-3\log\varepsilon) \mid \hat{\boldsymbol{\rho}} = r', \mathfrak{S}\right] \geq 1 - \sqrt{\varepsilon} \qquad \text{for all } r, r' \in \mathfrak{L}_0(r_*, \varepsilon), \tag{7.37}$$

and combining (7.37) with Lemma 7.14 completes the proof. □

Proof of Lemma 7.9. We are going to show that the conditional probability $\mathbb{P}_{\mathfrak{A}}\left[\hat{\boldsymbol{\rho}} = r \mid \mathfrak{S}\right]$ of hitting some particular $r \in \mathfrak{L}_0$ coincides with the unconditional probability $\mathbb{P}_{\mathfrak{A}}\left[\hat{\boldsymbol{\rho}} = r\right]$ up to a factor of $1 + o_\varepsilon(1)$. Then the assertion follows from Bayes' formula.

The unconditional probability $\mathbb{P}_{\mathfrak{A}}\left[\hat{\boldsymbol{\rho}} = r\right]$ is given precisely by Claim 7.8. Hence, recalling the $(q-1) \times (q-1)$-matrix $\Sigma = q\mathrm{id}^{-1} - q^{-2}\mathbb{1}$ and applying Stirling's formula, we obtain

$$\mathbb{P}_{\mathfrak{A}}\left[\hat{\boldsymbol{\rho}} = r\right] \sim \frac{1}{(2\pi\boldsymbol{\Delta}q^{-1}(1-q^{-1}))^{(q-1)/2}}\exp\left[-\frac{(r - q^{-1}\boldsymbol{\Delta}\mathbb{1})^\top(q^{-1}\mathbb{1} - q^{-2}\mathbb{1})^{-1}(r - q^{-1}\boldsymbol{\Delta}\mathbb{1})}{2\boldsymbol{\Delta}}\right] \tag{7.38}$$

w.h.p.

Next we will show that the conditional probability $\mathbb{P}_{\mathfrak{A}}\left[\hat{\boldsymbol{\rho}} = r \mid \mathfrak{S}\right]$ works out to be asymptotically the same. Indeed, Claim 7.11 shows that for any $r \in \mathfrak{L}_0$ the proability that $\hat{\boldsymbol{\rho}}$ hits the set $\mathfrak{L}_0(r, \varepsilon)$ is asymptotically equal to the probability of the event $\{\|\boldsymbol{N} - \boldsymbol{\Delta}^{-1/2}(r - q^{-1}\boldsymbol{\Delta}\mathbb{1})\|_\infty < \varepsilon\}$ w.h.p. Moreover, Corollary 9.4 implies that given $\hat{\boldsymbol{\rho}} \in \mathfrak{L}_0(r, \varepsilon)$, $\hat{\boldsymbol{\rho}}$ is within $o_\varepsilon(1)$ of the uniform distribution on $\mathfrak{L}_0(r, \varepsilon)$. Furthermore, Lemma 3.6 and Proposition 2.3 show that the number of points in $\mathfrak{L}_0(r, \varepsilon)$ satisfies

$$\frac{|\mathfrak{L}_0(r, \varepsilon)|}{\left|\left\{z \in \mathbb{Z}^{q-1} : \|z - r\|_\infty \leq \varepsilon\sqrt{\boldsymbol{\Delta}}\right\}\right|} \sim q^{-\mathbb{1}\{|\mathrm{supp}\boldsymbol{\chi}|=1\}}.$$

Therefore, w.h.p. for all $r \in \mathfrak{L}_0$ we have

$$\mathbb{P}_{\mathfrak{A}}\left[\hat{\boldsymbol{\rho}} = r \mid \mathfrak{S}\right] = (1 + o_\varepsilon(1))\frac{q^{\mathbb{1}\{|\mathrm{supp}\boldsymbol{\chi}|=1\}}}{(2\pi\boldsymbol{\Delta}q^{-1}(1-q^{-1}))^{(q-1)/2}}\exp\left[-\frac{(r - q^{-1}\boldsymbol{\Delta}\mathbb{1})^\top(q^{-1}\mathbb{1} - q^{-2}\mathbb{1})^{-1}(r - q^{-1}\boldsymbol{\Delta}\mathbb{1})}{2\boldsymbol{\Delta}}\right]. \tag{7.39}$$

Finally, we observe that

$$\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{S}\right] \sim q^{-\boldsymbol{m}}. \tag{7.40}$$

Indeed, since the $\boldsymbol{\xi}_{ij}$ are uniform and independent, for each $i \in [\boldsymbol{m}]$ we have $\sum_{j=1}^{\boldsymbol{k}_i}\chi_{i,j}\xi_{ij} = 0$ with probability $1/q$ indepdenently. Combining (7.38)–(7.40) completes the proof. □

7.5. **Proof of Lemma 7.10.** We continue to denote by $\boldsymbol{\sigma} \in \mathbb{F}_q^n$ a uniformly random assignment and by $\boldsymbol{I}_{q-1}$ the $(q-1)\times(q-1)$-identity matrix. Also recall ρ_σ from (7.1) and for $\rho = (\rho(s))_{s\in\mathbb{F}_q}$ obtain $\hat\rho = (\rho(s))_{s\in\mathbb{F}_q^*}$ by dropping the 0-entry. The following claim, which we prove via the local limit theorem for sums of independent random variables, determines the distribution of $\rho_{\boldsymbol{\sigma}}$. Let $\bar\rho = q^{-1}\boldsymbol{\Delta}\mathbb{1}_{q-1}$.

Claim 7.16. *Let $\mathscr{C}$ be the $(q-1)\times(q-1)$-matrix from* (9.2)*. Then w.h.p. for all $\rho\in\mathfrak{P}_q$ we have*

$$\mathbb{P}\left[\rho_{\boldsymbol{\sigma}} = \rho \mid \mathfrak{A}\right] = \frac{q^{q/2}\mathfrak{d}^{q-1}}{(2\mathbb{E}[\boldsymbol{d}^2]\pi n)^{(q-1)/2}}\exp\left(-\frac{(\hat\rho-\bar\rho)^\top\mathscr{C}^{-1}(\hat\rho-\bar\rho)}{2n\mathbb{E}[\boldsymbol{d}^2]}\right) + o(n^{(1-q)/2}).$$

The proof of Claim 7.16 is based on local limit theorem techniques similar to but simpler than the ones from Section 7.4. In fact, the proof strategy is somewhat reminiscent of that of the well-known local limit theorem for sums of independent random vectors from [18]. However, the local theorem from that paper does not imply Claim 7.16 directly because a key assumption (that increments of vectors in each direction can be realised) is not satisfied here. We therefore carry the details out in the appendix.

Claim 7.16 demonstrates that $\rho_{\boldsymbol{\sigma}}$ satisfies a local limit theorem. Hence, let $\boldsymbol{N}'\in\mathbb{R}^{q-1}$ be a mean-zero Gaussian vector with covariance matrix $q^{-1}\mathrm{id} - q^{-2}\mathbb{1}$. Moreover, fix $\varepsilon>0$ and let $U\subseteq\mathbb{R}^{q-1} = \nu + [-\varepsilon,\varepsilon]^{q-1}$ be a box of side length 2ε. Then w.h.p. we have

$$\mathbb{P}_{\mathfrak{A}}\left[\left(n\mathbb{E}[\boldsymbol{d}^2]\right)^{-1/2}(\hat\rho_{\boldsymbol{\sigma}} - q^{-1}\boldsymbol{\Delta}\mathbb{1}) \in U\right] = \mathbb{P}_{\mathfrak{A}}\left[\boldsymbol{N}'\in U\right] + o(1). \tag{7.41}$$

Indeed, Claim 7.16 implies that $\hat\rho_{\boldsymbol{\sigma}}$ is asymptotically uniformly distributed on the lattice points of the box U whose coordinates are divisible by $\mathfrak{d}$ w.h.p. Thus, w.h.p. for any $z,z'\in\boldsymbol{\Delta}U\cap\mathfrak{d}\mathbb{Z}^{\mathbb{F}_q^*}$ we have

$$\mathbb{P}_{\mathfrak{A}}\left[\hat\rho_{\boldsymbol{\sigma}} = z\right] = (1+o_\varepsilon(1))\mathbb{P}_{\mathfrak{A}}\left[\hat\rho_{\boldsymbol{\sigma}} = z'\right]. \tag{7.42}$$

Moreover, we claim that

$$\mathbb{P}_{\mathfrak{A}}\left[\hat\rho_{\boldsymbol{\sigma}}\in\mathfrak{L}_0 \mid \hat\rho_{\boldsymbol{\sigma}}\in U\right] \sim \frac{\left|U\cap\mathfrak{L}_0\cap\mathfrak{d}\mathbb{Z}^{\mathbb{F}_q^*}\right|}{\left|U\cap\mathfrak{d}\mathbb{Z}^{\mathbb{F}_q^*}\right|} \le \frac{\left|U\cap\mathfrak{M}\cap\mathfrak{d}\mathbb{Z}^{\mathbb{F}_q^*}\right|}{\left|U\cap\mathfrak{d}\mathbb{Z}^{\mathbb{F}_q^*}\right|} \le (1+o(1))q^{-\mathbb{1}\{|\mathrm{supp}\boldsymbol{\chi}|=1\}}. \tag{7.43}$$

Indeed, if $|\mathrm{supp}\boldsymbol{\chi}|>1$, then (7.43) is satisfied w.h.p. for the trivial reason that the r.h.s. equals $1+o(1)$. Hence, suppose that $|\mathrm{supp}\boldsymbol{\chi}|=1$, let $\mathfrak{M}\supset\mathfrak{L}_0$ be the module from Proposition 2.3 and let $\mathfrak{b}_1,\ldots,\mathfrak{b}_{q-1}$ be its assorted basis. Clearly, $\mathfrak{M}\cap\mathfrak{d}\mathbb{Z}^{\mathbb{F}_q^*}\supseteq\mathfrak{d}\mathfrak{M}$. Conversely, Cramer's rule shows that any $y\in\mathfrak{M}\cap\mathfrak{d}\mathbb{Z}^{\mathbb{F}_q^*}$ can be expressed as

$$(\mathfrak{b}_1\ \cdots\ \mathfrak{b}_{q-1})z, \qquad \text{with } z_i = \frac{\det(\mathfrak{b}_1\cdots\mathfrak{b}_{i-1}\ y\ \mathfrak{b}_{i+1}\cdots\mathfrak{b}_{q-1})}{q}.$$

In particular, all coordinates z_i are divisible by $\mathfrak{d}$ because $y\in\mathfrak{d}\mathbb{Z}^{\mathbb{F}_q^*}$. Hence, $y\in\mathfrak{d}\mathfrak{M}$ because $\mathfrak{d}$ and q are coprime. Lemma 3.6 therefore implies (7.43). Finally, the assertion follows from (7.41)–(7.43).

8. Proof of Proposition 4.1

We prove Proposition 4.1 by way of a coupling argument inspired by the Aizenman-Sims-Starr scheme from spin glass theory [5]. The proof is a close adaptation of the coupling argument used in [10] to prove the approximate rank formula (1.4). We will therefore be able to reuse some of the technical steps from that paper. The main difference is that we need to accommodate the extra ternary equations t_i. Their presence gives rise to the second parameter β in (4.5).

8.1. **Overview.** The basic idea behind the Aizenman-Sims-Starr scheme is to compute the expected difference $\mathbb{E}[\mathrm{nul}\,\boldsymbol{A}[n+1,\varepsilon,\delta,\Theta]] - \mathbb{E}[\mathrm{nul}\,\boldsymbol{A}[n+1,\varepsilon,\delta,\Theta]]$ of the nullity upon increasing the size of the matrix. We then obtain (4.5) by writing a telescoping sum. In order to estimate the expected change of the nullity, we set up a coupling of $\boldsymbol{A}[n,\varepsilon,\delta,\Theta]$ and $\boldsymbol{A}[n+1,\varepsilon,\delta,\Theta]$.

To this end it is helpful to work with a different description of the random matrix model. Specifically, let $\boldsymbol{M} = (\boldsymbol{M}_j)_{j\ge1}$, $\boldsymbol{\Delta} = (\boldsymbol{\Delta}_j)_{j\ge1}$, $\boldsymbol{\lambda}$ and $\boldsymbol{\eta}$ be Poisson variables with means

$$\mathbb{E}[\boldsymbol{M}_j] = (1-\varepsilon)\mathbb{P}\left[\boldsymbol{k}=j\right]dn/k, \qquad \mathbb{E}[\boldsymbol{\Delta}_j] = (1-\varepsilon)\mathbb{P}\left[\boldsymbol{k}=j\right]d/k, \qquad \mathbb{E}[\boldsymbol{\lambda}] = \delta n, \qquad \mathbb{E}\left[\boldsymbol{\eta}\right] = \delta. \tag{8.1}$$

All these random variables are mutually independent and independent of $\boldsymbol{\theta}$ and the $(\boldsymbol{d}_i)_{i\geq 1}$. Further, let

$$\boldsymbol{M}_j^+ = \boldsymbol{M}_j + \boldsymbol{\Delta}_j, \qquad \boldsymbol{m}_{\varepsilon,n} = \sum_{j\geq 1} \boldsymbol{M}_j, \qquad \boldsymbol{m}_{\varepsilon,n}^+ = \sum_{j\geq 1} \boldsymbol{M}_j^+, \qquad \boldsymbol{\lambda}^+ = \boldsymbol{\lambda} + \boldsymbol{\eta}. \tag{8.2}$$

Since $\sum_{j\geq 1} \boldsymbol{M}_j \sim \mathrm{Po}((1-\varepsilon)dn/k)$, (8.2) is consistent with (4.1).

We define a random Tanner (multi-)graph $\boldsymbol{G}[n,\boldsymbol{M},\boldsymbol{\lambda}]$ with variable nodes $x_1,\dots,x_n$ and check nodes $a_{i,j}$, $i\geq 1$, $j\in[\boldsymbol{M}_i]$, $t_1,\dots,t_{\boldsymbol{\lambda}}$ and $p_1,\dots,p_{\boldsymbol{\theta}}$. The edges between variables and the check nodes $a_{i,j}$ are induced by a random maximal matching $\boldsymbol{\Gamma}[n,\boldsymbol{M}]$ of the complete bipartite graph with vertex classes

$$\bigcup_{h=1}^{n} \{x_h\}\times[\boldsymbol{d}_h] \quad \text{and} \quad \bigcup_{i\geq 1}\bigcup_{j=1}^{\boldsymbol{M}_i} \{a_{i,j}\}\times[i].$$

Moreover, for each $j\in[\boldsymbol{\lambda}]$ we choose $\boldsymbol{i}_{j,1},\boldsymbol{i}_{j,2},\boldsymbol{i}_{j,3}$ uniformly and independently from $[n]$ and add edges between $x_{\boldsymbol{i}_{j,1}}$, $x_{\boldsymbol{i}_{j,2}}$, $x_{\boldsymbol{i}_{j,3}}$ and t_j. In addition, we insert an edge between p_i and x_i for every $i\in[\boldsymbol{\theta}]$.

To define the random matrix $\boldsymbol{A}[n,\boldsymbol{M},\boldsymbol{\lambda}]$ to go with $\boldsymbol{G}[n,\boldsymbol{M},\boldsymbol{\lambda}]$, let

$$\boldsymbol{A}[n,\boldsymbol{M},\boldsymbol{\lambda}]_{p_i,x_h} = \mathbb{1}\{i=h\} \qquad (i\in[\boldsymbol{\theta}],h\in[n]), \tag{8.3}$$

$$\boldsymbol{A}[n,\boldsymbol{M},\boldsymbol{\lambda}]_{a_{i,j},x_h} = \boldsymbol{\chi}_{i,h}\sum_{\ell=1}^{i}\sum_{s=1}^{\boldsymbol{d}_h}\mathbb{1}\{(x_h,s),(a_{i,j},\ell)\}\in\boldsymbol{\Gamma}_{n,\boldsymbol{M}}\} \qquad (i\geq 1, j\in[\boldsymbol{M}_i],h\in[n]), \tag{8.4}$$

$$\boldsymbol{A}[n,\boldsymbol{M},\boldsymbol{\lambda}]_{t_i,x_h} = \boldsymbol{\chi}_{\boldsymbol{m}_{\varepsilon,n}+i,h}\sum_{\ell=1}^{3}\mathbb{1}\{\boldsymbol{i}_{i,\ell}=h\} \qquad (i\in[\boldsymbol{\lambda}],h\in[n]). \tag{8.5}$$

The Tanner graph $\boldsymbol{G}\left[n+1,\boldsymbol{M}^+,\boldsymbol{\lambda}^+\right]$ and its associated random matrix $\boldsymbol{A}\left[n+1,\boldsymbol{M}^+,\boldsymbol{\lambda}^+\right]$ are defined analogously using $n+1$ variable nodes instead of n, $\boldsymbol{M}^+$ instead of $\boldsymbol{M}$ and $\boldsymbol{\lambda}^+$ instead of $\boldsymbol{\lambda}$.

Fact 8.1. *For any $\varepsilon,\delta>0$ we have*

$$\mathbb{E}[\mathrm{nul}\,\boldsymbol{A}[n,\varepsilon,\delta]] = \mathbb{E}[\mathrm{nul}\,\boldsymbol{A}[n,\boldsymbol{M},\boldsymbol{\lambda}]], \qquad \mathbb{E}[\mathrm{nul}\,\boldsymbol{A}[n+1,\varepsilon,\delta]] = \mathbb{E}\left[\mathrm{nul}\,\boldsymbol{A}\left[n+1,\boldsymbol{M}^+,\boldsymbol{\lambda}^+\right]\right].$$

Proof. Because the check degrees $\boldsymbol{k}_i$ of the random factor graph $\boldsymbol{G}[n,\varepsilon,\delta]$ are drawn independently, the only difference between $\boldsymbol{G}[n,\varepsilon,\delta]$ and $\boldsymbol{G}[n,\boldsymbol{M},\boldsymbol{\lambda}]$ is the bookkeeping of the number of checks of each degree. The same is true of $\boldsymbol{G}[n+1,\varepsilon,\delta]$ and $\boldsymbol{G}[n+1,\boldsymbol{M},\boldsymbol{\lambda}]$. □

To construct a coupling of $\boldsymbol{A}[n,\boldsymbol{M},\boldsymbol{\lambda}]]$ and $\boldsymbol{A}\left[n+1,\boldsymbol{M}^+,\boldsymbol{\lambda}^+\right]$ we introduce a third, intermediate random matrix. Hence, let $\boldsymbol{\gamma}_i\geq 0$ be the number of checks $a_{i,j}$, $j\in[\boldsymbol{M}_i^+]$, adjacent to the last variable node x_{n+1} in $\boldsymbol{G}\left[n+1,\boldsymbol{M}^+,\boldsymbol{\lambda}^+\right]$. Set $\boldsymbol{\gamma}=(\boldsymbol{\gamma}_i)_{i\geq 3}$. Also let

$$\lambda^- = \delta(n+1) - 3\delta\cdot\frac{n^2+n+1/3}{n^2+2n+1} \tag{8.6}$$

be the expected number of extra ternary checks of $\boldsymbol{G}\left[n+1,\boldsymbol{M}^+,\boldsymbol{\lambda}^+\right]$ in which x_{n+1} does not appear. Let

$$\boldsymbol{M}_i^- = (\boldsymbol{M}_i - \boldsymbol{\gamma}_i)\vee 0, \qquad \text{as well as} \qquad \boldsymbol{\lambda}^- \sim \mathrm{Po}(\lambda^-). \tag{8.7}$$

Consider the random Tanner graph $\boldsymbol{G}' = \boldsymbol{G}[n,\boldsymbol{M}^-,\boldsymbol{\lambda}^-]$ induced by a random maximal matching $\boldsymbol{\Gamma}' = \boldsymbol{\Gamma}[n,\boldsymbol{M}^-]$ of the complete bipartite graph with vertex classes

$$\bigcup_{h=1}^{n}\{x_h\}\times[\boldsymbol{d}_h] \quad \text{and} \quad \bigcup_{i\geq 1}\bigcup_{j=1}^{\boldsymbol{M}_i^-}\{a_{i,j}\}\times[i]. \tag{8.8}$$

Each matching edge $\{(x_h,s),(a_{i,j},\ell)\}\in\boldsymbol{\Gamma}[n,\boldsymbol{M}^-]$ induces an edge between x_h and $a_{i,j}$ in the Tanner graph. For each $j\in[\boldsymbol{\lambda}^-]$ and $\boldsymbol{i}_{j,1}^-,\boldsymbol{i}_{j,2}^-,\boldsymbol{i}_{j,3}^-$ uniform and independent in $[n]$, we add the edges between $x_{\boldsymbol{i}_{j,1}^-}$, $x_{\boldsymbol{i}_{j,2}^-}$, $x_{\boldsymbol{i}_{j,3}^-}$ and t_j. In addition, there is an edge between p_i and x_i for every $i\in[\boldsymbol{\theta}]$. Let $\boldsymbol{A}'$ denote the corresponding random matrix.

For each variable x_i, $i=1,\dots,n$, let $\mathscr{C}$ be the set of clones from $\bigcup_{i\in[n]}\{x_i\}\times[\boldsymbol{d}_i]$ that $\boldsymbol{\Gamma}[n,\boldsymbol{M}^-]$ leaves unmatched. We call the elements of $\mathscr{C}$ *cavities*.

From $\boldsymbol{G}'$, we finally construct two further Tanner graphs. Obtain the Tanner graph $\boldsymbol{G}''$ from $\boldsymbol{G}'$ by adding new check nodes $a_{i,j}''$ for each $i\geq 3$, $j\in[\boldsymbol{M}_i-\boldsymbol{M}_i^-]$ and ternary check nodes t_i'' for $i\in[\boldsymbol{\lambda}'']$, where

$$\boldsymbol{\lambda}'' \sim \mathrm{Po}(\delta n - \lambda^-) = \mathrm{Po}\left(2\delta\cdot\frac{n^2+n/2}{n^2+2n+1}\right) \tag{8.9}$$

The new checks $a''_{i,j}$ are joined by a random maximal matching $\mathbf{\Gamma}''$ of the complete bipartite graph on

$$\mathscr{C} \qquad \text{and} \qquad \bigcup_{i\geq 1}\bigcup_{j\in[\boldsymbol{M}_i-\boldsymbol{M}_i^-]}\{a''_{i,j}\}\times[i].$$

Moreover, for each $j\in[\boldsymbol{\lambda}'']$ we choose $\boldsymbol{i}''_{j,1},\boldsymbol{i}''_{j,2},\boldsymbol{i}''_{j,3}\in[n]$ uniformly and independently of everything else and add the edges between $x_{\boldsymbol{i}''_{j,1}}$, $x_{\boldsymbol{i}''_{j,2}}$, $x_{\boldsymbol{i}''_{j,3}}$ and t''_j. Let $\boldsymbol{A}''$ denote the corresponding random matrix, where as before, each new edge is represented by an independent copy of $\boldsymbol{\chi}$.

Finally, let

$$\boldsymbol{\lambda}''' \sim \mathrm{Po}(\delta(n+1)-\lambda^-) = \mathrm{Po}\left(3\delta\cdot\frac{n^2+n+1/3}{n^2+2n+1}\right). \tag{8.10}$$

We analogously obtain $\boldsymbol{G}'''$ by adding one variable node x_{n+1} as well as check nodes $a'''_{i,j}$, $i\geq 1$, $j\in[\boldsymbol{\gamma}_i]$, $b'''_{i,j}$, $i\geq 1$, $j\in[\boldsymbol{M}_i^+-\boldsymbol{M}_i^--\boldsymbol{\gamma}_i]$, $t'''_i, i\in[\boldsymbol{\lambda}''']$. The new checks $a'''_{i,j}$ and $b'''_{i,j}$ are connected to $\boldsymbol{G}'$ via a random maximal matching $\mathbf{\Gamma}'''$ of the complete bipartite graph on

$$\mathscr{C} \qquad \text{and} \qquad \bigcup_{i\geq 1}\left(\bigcup_{j\in[\boldsymbol{\gamma}_i]}\{a'''_{i,j}\}\times[i-1]\cup\bigcup_{j\in[\boldsymbol{M}_i^+-\boldsymbol{M}_i^--\boldsymbol{\gamma}_i]}\{b'''_{i,j}\}\times[i]\right).$$

For each matching edge we insert the corresponding variable-check edge and in addition each of the check nodes $a'''_{i,j}$ gets connected to x_{n+1} by exactly one edge. Then we connect each t'''_i to $x_{\boldsymbol{i}'''_{i,1}}, x_{\boldsymbol{i}'''_{i,2}}$ and x_{n+1}, with $\boldsymbol{i}'''_{i,1},\boldsymbol{i}'''_{i,2}\in[n+1]$ chosen uniformly and independently. Once again each edge is represented by an independent copy of $\boldsymbol{\chi}$. Let $\boldsymbol{A}'''$ denote the resulting random matrix.

The following lemma connects $\boldsymbol{A}'',\boldsymbol{A}'''$ with the random matrices $\boldsymbol{A}[n,\boldsymbol{M},\boldsymbol{\lambda}]$, $\boldsymbol{A}\left[n+1,\boldsymbol{M}^+,\boldsymbol{\lambda}^+\right]$ and thus, in light of Fact 8.1, with $\boldsymbol{A}[n,\varepsilon,\delta]$ and $\boldsymbol{A}[n+1,\varepsilon,\delta]$.

Lemma 8.2. *We have* $\mathbb{E}[\mathrm{nul}(\boldsymbol{A}'')]=\mathbb{E}[\mathrm{nul}(\boldsymbol{A}_{n,\boldsymbol{M},\lambda})]+o(1)$ *and* $\mathbb{E}[\mathrm{nul}(\boldsymbol{A}''')]=\mathbb{E}[\mathrm{nul}(\boldsymbol{A}_{n+1,\boldsymbol{M}^+,\lambda^+})]+o(1)$.

We defer the simple proof of Lemma 8.2 to Section 8.5.

The core of the proof of Proposition 4.1 is to estimate the difference of the nullities of $\boldsymbol{A}'''$ and $\boldsymbol{A}'$ and of $\boldsymbol{A}''$ and $\boldsymbol{A}'$. The following two lemmas express these differences in terms of two random variables $\boldsymbol{\alpha},\boldsymbol{\beta}$. Specifically, let $\boldsymbol{\alpha}$ be the fraction of frozen cavities of $\boldsymbol{A}'$ and let $\boldsymbol{\beta}$ be the fraction of frozen variables of $\boldsymbol{A}'$.

Lemma 8.3. *For large enough* $\Theta(\varepsilon)>0$ *and small enough* $0<\delta<\delta_0$ *we have*

$$\mathbb{E}[\mathrm{nul}(\boldsymbol{A}''')-\mathrm{nul}(\boldsymbol{A}')]=\mathbb{E}\left[\exp\left(-3\delta\boldsymbol{\beta}^2\right)D(1-K'(\boldsymbol{\alpha})/k)\right]+\frac{d}{k}\mathbb{E}\left[K'(\boldsymbol{\alpha})+K(\boldsymbol{\alpha})\right]-\frac{d(k+1)}{k}-3\delta\mathbb{E}\left[1-\boldsymbol{\beta}^2\right]+o_\varepsilon(1).$$

Lemma 8.4. *For large enough* $\Theta(\varepsilon)>0$ *and small enough* $0<\delta<\delta_0$ *we have*

$$\mathbb{E}[\mathrm{nul}(\boldsymbol{A}'')-\mathrm{nul}(\boldsymbol{A}')]=-d+\frac{d}{k}\mathbb{E}\left[\boldsymbol{\alpha}K'(\boldsymbol{\alpha})\right]-2\delta\mathbb{E}\left[1-\boldsymbol{\beta}^3\right]+o_\varepsilon(1).$$

After some preparations in Section 8.2 we will prove Lemmas 8.3 and 8.4 in Sections 8.3 and 8.4.

Proof of Proposition 4.1. The proposition is an immediate consequence of Fact 8.1, Lemma 8.2, Lemma 8.3 and Lemma 8.4. □

8.2. **Preparations.** To facilitate the proofs of Lemmas 8.3 and 8.4 we establish a few basic statements about the coupling. Some of these are immediate consequence of statements from [10], where a similar coupling was used. Let us begin with the following lower bound on the likely number of cavities.

Lemma 8.5. *W.h.p. we have* $|\mathscr{C}|\geq\varepsilon dn/2$.

Proof. Apart from the extra ternary check nodes $t_1,\ldots t_{\boldsymbol{\lambda}'}$, the construction of $\boldsymbol{G}'$ coincides with that of the Tanner graph from [10]. Because the presence of $t_1,\ldots t_{\boldsymbol{\lambda}'}$ does not affect the number of cavities, the assertion therefore follows from [10, Lemma 5.5]. □

As a next step we show that w.h.p. the random matrix $\boldsymbol{A}'$ does not have very many short linear relations. Specifically, if we choose a bounded number of variables and a bounded number of cavities randomly, then it is quite unlikely that the chosen coordinates form a proper relation. Formally, let $\mathscr{R}(\ell_1,\ell_2)$ be the set of all sequences

$(i_1,\dots,i_{\ell_1}) \in [n]^{\ell_1}$, $(u_1,j_1),\dots,(u_{\ell_2},j_{\ell_2}) \in \mathscr{C}$ such that $(i_1,\dots,i_{\ell_1},u_1,\dots,u_{\ell_2})$ is a proper relation of $\boldsymbol{A}'$. Furthermore, let $\mathfrak{R}(\zeta,\ell)$ be the event that $|\mathscr{R}(\ell_1,\ell_2)| \le \zeta n^{\ell_1}|C|^{\ell_2}$ for all $0 \le \ell_1,\ell_2 \le \ell$.

Lemma 8.6. *For any $\zeta > 0$, $\ell > 0$ exist $\Theta_0 = \Theta_0(\varepsilon,\zeta,\ell) > 0$ and $n_0 > 0$ such that for all $n \ge n_0$, $\Theta \ge \Theta_0$ we have $\mathbb{P}[\mathfrak{R}(\zeta,\ell)] > 1-\zeta$.*

Proof. Fix any $\ell_1,\ell_2 \le \ell$ such that $\ell_1+\ell_2 > 0$ and let $\mathfrak{R}(\zeta,\ell_1,\ell_2)$ be the event that $|\mathscr{R}(\ell_1,\ell_2)| < \zeta n^{\ell_1}|C|^{\ell_2}$. Then it suffices to show that $\mathbb{P}[\mathfrak{R}(\zeta,\ell_1,\ell_2)] > 1-\zeta$ as we can just replace ζ by $\zeta/(\ell+1)^2$ and apply the union bound. To this end we may assume that $\zeta < \zeta_0(\varepsilon,\ell)$ for a small enough $\zeta_0(\varepsilon,\ell) > 0$.

We will actually estimate $|\mathscr{R}(\ell_1,\ell_2)|$ on a certain likely event. Specifically, due to Lemma 8.5 we have $|\mathscr{C}| \ge \varepsilon n/2$ w.h.p. In addition, let $\mathscr{A}$ be the event that $\boldsymbol{A}'$ is $(\zeta^4/L^\ell,\ell)$-free. Then Lemma 3.4 shows that $\mathbb{P}[\mathscr{A}] > 1-\zeta/3$, provided that $n \ge n_0$ for a large enough $n_0 = n_0(\zeta,\ell)$. To see this, consider the matrix $\boldsymbol{B}$ obtained from $\boldsymbol{A}'$ by deleting the rows representing the unary checks p_i. Then Lemma 3.4 shows that the matrix $\boldsymbol{B}[\boldsymbol{\theta}]$ obtained from $\boldsymbol{B}$ via the pinning operation is (ζ^4,L^ℓ)-free with probability $1-\zeta/3$, provided that Θ is chosen sufficiently large. The only difference between $\boldsymbol{B}[\boldsymbol{\theta}]$ and $\boldsymbol{A}'$ is that in the former random matrix we apply the pinning operation to $\boldsymbol{\theta}$ random coordinates, while in $\boldsymbol{A}'$ the unary checks p_i pin the first $\boldsymbol{\theta}$ coordinates. However, the distribution of $\boldsymbol{A}'$ is actually invariant under permutations of the columns. Therefore, the matrices $\boldsymbol{A}'$ and $\boldsymbol{B}[\boldsymbol{\theta}]$ are (ζ^4,L^ℓ)-free with precisely the same probability. Hence, Lemma 3.4 implies that $\mathbb{P}[\mathscr{A}] > 1-\zeta/3$.

Further, Markov's inequality shows that for any $L > 0$,

$$\mathbb{P}\left[\sum_{i=1}^n \boldsymbol{d}_i \mathbb{1}\{\boldsymbol{d}_i > L\} \ge \frac{\varepsilon\zeta^2 n}{16\ell}\right] \le \frac{16\ell\mathbb{E}[\boldsymbol{d}\mathbb{1}\{\boldsymbol{d} > L\}]}{\varepsilon\zeta^2}.$$

Therefore, since $\mathbb{E}[\boldsymbol{d}] = O_\varepsilon(1)$ we can choose $L = L(\varepsilon,\zeta,\ell) > 0$ big enough such that the event

$$\mathscr{L} = \left\{\sum_{i=1}^n \boldsymbol{d}_i \mathbb{1}\{\boldsymbol{d}_i > L\} < \frac{\varepsilon\zeta^2 n}{16\ell}\right\}$$

has probability at least $1-\zeta/3$. Thus, the event $\mathscr{E} = \mathscr{A} \cap \mathscr{L} \cap \{|\mathscr{C}| \ge \varepsilon n/2\}$ satisfies $\mathbb{P}[\mathscr{E}] > 1-\zeta$. Hence, suffices to show that

$$|\mathscr{R}(\ell_1,\ell_2)| < \zeta n^{\ell_1}|\mathscr{C}|^{\ell_2} \qquad \text{if the event } \mathscr{E} \text{ occurs.} \tag{8.11}$$

To bound $\mathscr{R}(\ell_1,\ell_2)$ on $\mathscr{E}$ we need to take into consideration that the cavities are degree-weighted. Hence, let $\mathscr{R}'(\ell_1,\ell_2)$ be the set of all sequences $(i_1,\dots,i_{\ell_1},(u_1,j_1),\dots,(u_{\ell_2},j_{\ell_2})) \in \mathscr{R}(\ell_1,\ell_2)$ such that the degree of some variable node u_i exceeds L. Assuming $\ell_2 > 0$, on $\mathscr{E}$ we have

$$|\mathscr{R}'(\ell_1,\ell_2)| \le n^{\ell_1+1}|\mathscr{C}|^{\ell_2-1} \cdot \frac{2}{\varepsilon}\sum_{i=1}^n \boldsymbol{d}_i\mathbb{1}\{\boldsymbol{d}_i > L\} \le n^{\ell_1}|\mathscr{C}|^{\ell_2} \cdot \frac{2}{\varepsilon} \cdot \frac{\zeta^2 n}{16\ell_2} < \frac{\zeta}{2}, \tag{8.12}$$

provided that $\zeta > 0$ is small enough.

Finally, we bound the size of $\mathscr{R}''(\ell_1,\ell_2) = \mathscr{R}(\ell_1,\ell_2) \setminus \mathscr{R}'(\ell_1,\ell_2)$. Since for any $(i_1,\dots,i_{\ell_1},(u_1,j_1),\dots,(u_{\ell_2},j_{\ell_2})) \in \mathscr{R}''(\ell_1,\ell_2)$ the sequence $(i_1,\dots,i_{\ell_1},u_1,\dots,u_{\ell_2})$ is a proper relation and since there are no more than L^{ℓ_2} ways of choosing the indices $j_1,\dots,j_{\ell_2}$, on the event $\mathscr{E}$ we have

$$\begin{aligned}
|\mathscr{R}''(\ell_1,\ell_2)| &\le \frac{\zeta^4}{L^\ell} \cdot L^{\ell_2} n^\ell && \text{[because } \boldsymbol{A}' \text{ is } \zeta^4/L^\ell,\ell\text{)-free]} \\
&\le \zeta^4 \left(\frac{2}{\varepsilon}\right)^{\ell_2} \cdot n^{\ell_1}|\mathscr{C}|^{\ell_2} && \text{[because } |\mathscr{C}| > \varepsilon n/2\text{]} \\
&< \frac{\zeta}{2} n^{\ell_1}|\mathscr{C}|^{\ell_2}, && (8.13)
\end{aligned}$$

provided that $\zeta < \zeta_0(\varepsilon,\ell)$ is sufficiently small. Thus, (8.11) follows from (8.12) and (8.13). □

Let $(\hat{\boldsymbol{k}}_i)_{i\ge1}$ be a sequence of copies of $\hat{\boldsymbol{k}}$, mutually independent and independent of everything else. Also let

$$\hat{\boldsymbol{\gamma}}_j = \sum_{i=1}^{\boldsymbol{d}_{n+2}} \mathbb{1}\{\hat{\boldsymbol{k}}_i = j\}, \qquad \hat{\boldsymbol{\gamma}} = (\hat{\boldsymbol{\gamma}}_j)_{j\ge1}.$$

Additionally, let $(\hat{\boldsymbol{\Delta}}_j)_{j\geq 3}$ be a family of independent random variables with distribution

$$\hat{\boldsymbol{\Delta}}_j = \mathrm{Po}\big((1-\varepsilon)\mathbb{P}\big[\boldsymbol{k}=j\big]\,d/k\big). \tag{8.14}$$

Further, let Σ' be the σ-algebra generated by $\boldsymbol{G}', \boldsymbol{A}', \boldsymbol{\theta}, \boldsymbol{\lambda}^-, \boldsymbol{M}^-, \boldsymbol{\Gamma}_{n,M^-}, (\boldsymbol{\chi}'_{i,j,h})_{i,j,h\geq 1}$ and $(\boldsymbol{d}_i)_{i\in[n]}$. In particular, $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are Σ'-measurable.

Lemma 8.7. *With probability* $1-\exp(-\Omega_\varepsilon(1/\varepsilon))$*, we have*

$$d_{\mathrm{TV}}\big(\mathbb{P}\big[\{\boldsymbol{\gamma}\in\cdot\}\,|\Sigma'\big],\hat{\boldsymbol{\gamma}}\big) + d_{\mathrm{TV}}\big(\mathbb{P}\big[\{\boldsymbol{\Delta}\in\cdot\}\,|\Sigma'\big],\hat{\boldsymbol{\Delta}}\big) = O_\varepsilon(\sqrt{\varepsilon}).$$

Proof. Because $\boldsymbol{G}'$ is distributed the same as the Tanner graph from [10], apart from the extra ternary checks t_i, which do not affect the random vector $\boldsymbol{\gamma}$, the assertion follows from [10, Lemma 5.8]. □

Let $\ell_* = \lceil \exp(1/\varepsilon^4)\rceil$ and $\delta_* = \exp(-1/\varepsilon^4)$ and consider the event

$$\mathscr{E} = \mathfrak{R}(\delta_*, \ell_*). \tag{8.15}$$

Further, consider the event

$$\mathscr{E}' = \left\{|\mathscr{C}| \geq \varepsilon d n/2 \wedge \max_{i\leq n} \boldsymbol{d}_i \leq n^{1/2}\right\}. \tag{8.16}$$

Corollary 8.8. *For sufficiently large* $\Theta = \Theta(\varepsilon) > 0$ *we have* $\mathbb{P}\big[\boldsymbol{A}'\in\mathscr{E}\big] > \exp(-1/\varepsilon^4)$*. Moreover,* $\mathbb{P}\big[\mathscr{E}'\big] = 1-o(1)$.

Proof. The first statement follows from Lemma 8.6. The second statement follows from the choice of the parameters in (8.1), Lemma 3.8 and Lemma 8.5. □

With these preparations in place we are ready to proceed to the proofs of Lemmas 8.3 and 8.4.

8.3. **Proof of Lemma 8.3.** Let

$$\boldsymbol{X} = \sum_{i\geq 1} \boldsymbol{\Delta}_i, \qquad \boldsymbol{Y} = \sum_{i\geq 1} i\boldsymbol{\Delta}_i, \qquad \boldsymbol{Y}' = \sum_{i\geq 1} i\boldsymbol{\gamma}_i.$$

Then the total number of new non-zero entries upon going from $\boldsymbol{A}'$ to $\boldsymbol{A}'''$ is bounded by $\boldsymbol{Y}+\boldsymbol{Y}'+3\boldsymbol{\lambda}'''$. Let

$$\mathscr{E}'' = \big\{\boldsymbol{X}\vee\boldsymbol{Y}\vee\boldsymbol{Y}'\vee\boldsymbol{\lambda}'''\leq 1/\varepsilon\big\}.$$

Claim 8.9. *We have* $\mathbb{P}\big[\mathscr{E}''\big] = 1-O_\varepsilon(\varepsilon)$.

Proof. Apart from the additional ternary checks the argument is similar to [10, Proof of Claim 5.9]. The construction (8.1) ensures that $\mathbb{E}[\boldsymbol{X}], \mathbb{E}[\boldsymbol{Y}] = O_\varepsilon(1)$. Therefore, $\mathbb{P}[\boldsymbol{X} > 1/\varepsilon] = O_\varepsilon(\varepsilon)$, $\mathbb{P}[\boldsymbol{Y} > 1/\varepsilon] = O_\varepsilon(\varepsilon)$ by Markov's inequality. Further, a given check node of degree i is adjacent to x_{n+1} with probability at most $i\boldsymbol{d}_{n+1}/\sum_{i=1}^n \boldsymbol{d}_i \geq n \leq i\boldsymbol{d}_{n+1}/n$. Consequently,

$$\mathbb{E}\big[\boldsymbol{Y}'\big] = \mathbb{E}\sum_{i\geq 1} i\boldsymbol{\gamma}_i \leq \mathbb{E}\sum_{i\in[\boldsymbol{m}^+_{\varepsilon,n}]} \boldsymbol{k}_i^2\boldsymbol{d}_{n+1}/n = O_\varepsilon(1).$$

Moreover, (8.10) shows that $\mathbb{E}[\boldsymbol{\lambda}'''] = O_\varepsilon(1)$. Thus, the assertion follows from Markov's inequality. □

We obtain $\boldsymbol{G}'''$ from $\boldsymbol{G}'$ by adding checks $a'''_{i,j}$, $i\geq 1$, $j\in[\boldsymbol{\gamma}_i]$, $b'''_{i,j}$, $i\geq 1$, $j\in[\boldsymbol{M}^+_i - \boldsymbol{M}^-_i - \boldsymbol{\gamma}_i]$ and t'''_i, $i\in[\boldsymbol{\lambda}''']$. Let

$$\mathscr{X}''' = \left(\bigcup_{i\geq 1}\bigcup_{j=1}^{\boldsymbol{\gamma}_i} \partial a'''_{i,j}\setminus\{x_{n+1}\}\right) \cup \left(\bigcup_{i\geq 1}\bigcup_{j\in[\boldsymbol{M}^+_i-\boldsymbol{M}^-_i-\boldsymbol{\gamma}_i]} \partial b'''_{i,j}\right) \cup \bigcup_{i=1}^{\boldsymbol{\lambda}'''} \partial t'''_i \setminus\{x_{n+1}\}$$

be the set of variable neighbours of these new checks among $x_1,\ldots,x_n$. Further, let

$$\mathscr{E}''' = \left\{|\mathscr{X}| = Y + \sum_{i\geq 1}(i-1)\boldsymbol{\gamma}_i + \boldsymbol{\lambda}'''\right\}$$

be the event that the variables of $\boldsymbol{G}'$ where the new checks connect are pairwise distinct.

Claim 8.10. *We have* $\mathbb{P}\big[\mathscr{E}''' \mid \mathscr{E}'\cap\mathscr{E}''\big] = 1-o(1)$.

Proof. By the same token as in [10, proof of Claim 5.10], given that $\mathscr{E}'$ occurs the total number of cavities comes to $\Omega(n)$. At the same time, the maximum variable node degree is of order $O(\sqrt{n})$. Moreover, given the event $\mathscr{E}''$ no more than $Y + Y' = O_\varepsilon(1/\varepsilon)$ random cavities are chosen as neighbours of the new checks $a'''_{i,j}, b'''_{i,j}$. Thus, by the birthday paradox the probability that the checks $a'''_{i,j}, b'''_{i,j}$ occupy more than one cavity of any variable node is $o(1)$. Furthermore, the additional ternary nodes t'''_i choose their two neighbours among $x_1, \ldots, x_n$ mutually independently and independently of the $a'''_{i,j}, b'''_{i,j}$. Since $\boldsymbol{\lambda}'''$ is bounded given $1/\varepsilon$, the overall probability of choosing the same variable twice is $o(1)$. □

The following claim shows that the unlikely event that $\mathscr{E} \cap \mathscr{E}' \cap \mathscr{E}'' \cap \mathscr{E}'''$ does not occur does not contributed significantly to the expected change in nullity.

Claim 8.11. *We have* $\mathbb{E}\left[\left|\mathrm{nul}(\boldsymbol{A}''') - \mathrm{nul}(\boldsymbol{A}')\right| (1 - \mathbb{1}\mathscr{E} \cap \mathscr{E}' \cap \mathscr{E}'' \cap \mathscr{E}''')\right] = o_\varepsilon(1)$.

Proof. We modify the proof of [10, Claim 5.11] to accommodate the extra ternary nodes. Since $\boldsymbol{A}'''$ results from $\boldsymbol{A}'$ by adding one column and no more than $\boldsymbol{X} + \boldsymbol{d}_{n+1} + \boldsymbol{\lambda}'''$ rows, we have $\left|\mathrm{nul}(\boldsymbol{A}''') - \mathrm{nul}(\boldsymbol{A}')\right| \le X + \boldsymbol{d}_{n+1} + \boldsymbol{\lambda}''' + 1$. Because $\boldsymbol{X}, \boldsymbol{d}^2_{n+1}, \boldsymbol{\lambda}'''$ have bounded second moments, the Cauchy-Schwarz inequality therefore yields the estimate

$$\mathbb{E}\left[\left|\mathrm{nul}(\boldsymbol{A}''') - \mathrm{nul}(\boldsymbol{A}')\right| (1 - \mathbb{1}\mathscr{E}'')\right] \le \mathbb{E}\left[(X + \boldsymbol{d}_{n+1} + \boldsymbol{\lambda}''' + 1)^2\right]^{1/2} \left(1 - \mathbb{P}\left[\mathscr{E}''\right]\right)^{1/2} = o_\varepsilon(1). \tag{8.17}$$

Moreover, combining Corollary 8.8 and Claims 8.9–8.10, we obtain

$$\mathbb{E}\left[\left|\mathrm{nul}(\boldsymbol{A}''') - \mathrm{nul}(\boldsymbol{A}')\right| \mathbb{1}\mathscr{E}'' \setminus \mathscr{E}\right] \le O_\varepsilon(\varepsilon^{-1}) \exp(-1/\varepsilon^4) = o_\varepsilon(1), \tag{8.18}$$

$$\mathbb{E}\left[\left|\mathrm{nul}(\boldsymbol{A}''') - \mathrm{nul}(\boldsymbol{A}')\right| \mathbb{1}\mathscr{E}'' \setminus \mathscr{E}'\right], \mathbb{E}\left[\left|\mathrm{nul}(\boldsymbol{A}''') - \mathrm{nul}(\boldsymbol{A}')\right| \mathbb{1}\mathscr{E}'' \cap \mathscr{E}' \setminus \mathscr{E}'''\right] = o(1). \tag{8.19}$$

The assertion follows from (8.17)–(8.19). □

Recall that $\boldsymbol{\alpha}$ denotes the fraction of frozen cavities and $\boldsymbol{\beta}$ the fraction of frozen variables of $\boldsymbol{A}'$. Further, let $\Sigma'' \supset \Sigma'$ be the σ-algebra generated by $\boldsymbol{\theta}$, $\boldsymbol{G}'$, $\boldsymbol{A}'$, $\boldsymbol{M}_-$, $(\boldsymbol{d}_i)_{i \in [n+1]}$, $\boldsymbol{\gamma}$, $\boldsymbol{M}$, $\boldsymbol{\Delta}$, $\boldsymbol{\lambda}^-, \boldsymbol{\lambda}'''$. Then $\boldsymbol{\alpha}, \boldsymbol{\beta}$ as well as $\mathscr{E}, \mathscr{E}', \mathscr{E}''$ are Σ''-measurable but $\mathscr{E}'''$ is not.

Claim 8.12. *On the event* $\mathscr{E} \cap \mathscr{E}' \cap \mathscr{E}''$ *we have*

$$\begin{aligned}\mathbb{E}\left[\left(\mathrm{nul}(\boldsymbol{A}''') - \mathrm{nul}(\boldsymbol{A}')\right) \mathbb{1}\mathscr{E}''' \mid \Sigma''\right] = o_\varepsilon(1) + (1 - \boldsymbol{\beta}^2)^{\boldsymbol{\lambda}'''} \prod_{i \ge 1} (1 - \boldsymbol{\alpha}^{i-1})^{\boldsymbol{\gamma}_i} - \sum_{i \ge 1} (1 - \boldsymbol{\alpha}^{i-1}) \boldsymbol{\gamma}_i - \boldsymbol{\lambda}'''(1 - \boldsymbol{\beta}^2) \\ - \sum_{i \ge 1} (1 - \boldsymbol{\alpha}^i)(\boldsymbol{M}^+_i - \boldsymbol{M}^-_i - \boldsymbol{\gamma}_i).\end{aligned}$$

Proof. We modify the proof of [10, Claim 5.12] by taking the additional ternary checks into consideration. Let

$$\mathscr{A} = \left\{a'''_{i,j} : i \ge 1,\ j \in [\boldsymbol{\gamma}_i]\right\}, \qquad \mathscr{B} = \left\{b'''_{i,j} : i \ge 1,\ j \in [\boldsymbol{M}^+_i - \boldsymbol{M}^-_i - \boldsymbol{\gamma}_i]\right\}, \qquad \mathscr{T} = \left\{t_i : i \in [\boldsymbol{\lambda}''']\right\}.$$

We set up a random matrix $\boldsymbol{B}$ with rows indexed by $\mathscr{A} \cup \mathscr{B} \cup \mathscr{T}$ and columns indexed by $V_n = \{x_1, \ldots, x_n\}$. For a check $a \in \mathscr{A} \cup \mathscr{B} \cup \mathscr{T}$ and a variable $x \in V_n$ the (a, x)-entry of $\boldsymbol{B}$ equals zero unless $x \in \partial_{\boldsymbol{G}'''} a$. Further, the non-zero entries of $\boldsymbol{B}$ are independent copies of $\boldsymbol{\chi}$. Additionally, obtain $\boldsymbol{B}_*$ from $\boldsymbol{B}$ by zeroing out the x-column for every variable $x \in \mathfrak{F}(\boldsymbol{A}')$. Finally, let $\boldsymbol{C} \in \mathbb{F}^{\mathscr{A} \cup \mathscr{B} \cup \mathscr{T}}$ be a random vector whose entries $\boldsymbol{C}_a$, $a \in \mathscr{A} \cup \mathscr{T}$, are independent copies of $\boldsymbol{\chi}$, while $\boldsymbol{C}_b = 0$ for all $b \in \mathscr{B}$.

If $\mathscr{E}'''$ occurs, $\boldsymbol{B}$ has row full rank because there is at most one non-zero entry in every column and at least one non-zero entry in every row. Hence,

$$\mathrm{rk}(\boldsymbol{B}) = |\mathscr{A} \cup \mathscr{B} \cup \mathscr{T}| = \sum_{i \ge 1} \boldsymbol{M}^+_i - \boldsymbol{M}^-_i + \boldsymbol{\lambda}'''.$$

Furthermore, since the rank is invariant under row and column permutations, given $\mathscr{E} \cap \mathscr{E}' \cap \mathscr{E}'' \cap \mathscr{E}'''$ we have

$$\mathrm{nul}\, \boldsymbol{A}''' = \mathrm{nul} \begin{pmatrix} \boldsymbol{A}' & 0 \\ \boldsymbol{B} & \boldsymbol{C} \end{pmatrix}.$$

Moreover, given $\mathscr{E}'$ the set $\mathscr{X}'''$ of all non-zero columns of $\boldsymbol{B}$ satisfies $|\mathscr{X}'''| \le Y + Y' + \boldsymbol{\lambda}''' \le 3/\varepsilon$ while $|\mathscr{C}| \ge \varepsilon d n/2$. Therefore, the set of cavities that $\boldsymbol{\Gamma}'''$ occupies is within total variation distance $o(1)$ of a commensurate number of cavities drawn independently, i.e., with replacement. Furthermore, the variables where the checks from $\mathscr{T}$ attach are chosen uniformly at random from $x_1, \ldots, x_n$. Therefore, on $\mathscr{E} \cap \mathscr{E}' \cap \mathscr{E}''$ the conditional probability given $\mathscr{E}'''$ that

$\mathscr{X}'''$ forms a proper relation is bounded by $O_\varepsilon(\exp(-1/\varepsilon^4))$. Consequently, Lemma 3.2 implies that on the event $\mathscr{E}\cap\mathscr{E}'\cap\mathscr{E}''$,

$$\mathbb{E}\left[\left(\mathrm{nul}(\boldsymbol{A}''')-\mathrm{nul}(\boldsymbol{A}')\right)\mathbb{1}_{\mathscr{E}'''}\mid\Sigma''\right]=1-\mathbb{E}\left[\mathrm{rk}\left(\boldsymbol{B}_*\ \boldsymbol{C}\right)\mid\Sigma''\right]+o_\varepsilon(1). \tag{8.20}$$

We are thus left to calculate the rank of $\boldsymbol{Q}=(\boldsymbol{B}_*\ \boldsymbol{C})$. Given $\mathscr{E}'''$ this block matrix decomposes into the $\mathscr{A}\cup\mathscr{T}$-rows $\boldsymbol{Q}_{\mathscr{A}\cup\mathscr{T}}$ and the $\mathscr{B}$-rows $\boldsymbol{Q}_{\mathscr{B}}$ such that $\mathrm{rk}(\boldsymbol{Q})=\mathrm{rk}(\boldsymbol{Q}_{\mathscr{A}\cup\mathscr{T}})+\mathrm{rk}(\boldsymbol{Q}_{\mathscr{B}})$. Therefore, it suffices to prove that

$$\mathbb{E}\left[\mathrm{rk}\left(\boldsymbol{Q}_{\mathscr{B}}\right)\mid\Sigma''\right]=\sum_{i\geq1}\left(1-\boldsymbol{\alpha}^i\right)(\boldsymbol{M}_i^+-\boldsymbol{M}_i^--\boldsymbol{\gamma}_i)+o(1), \tag{8.21}$$

$$\mathbb{E}\left[\mathrm{rk}(\boldsymbol{Q}_{\mathscr{A}\cup\mathscr{T}})\mid\Sigma''\right]=\lambda'''(1-\boldsymbol{\beta}^2)+\sum_{i\geq1}\left(1-\boldsymbol{\alpha}^{i-1}\right)\boldsymbol{\gamma}_i+1-(1-\boldsymbol{\beta}^2)^{\boldsymbol{\lambda}'''}\prod_{i\geq1}\left(1-\boldsymbol{\alpha}^{i-1}\right)^{\boldsymbol{\gamma}_i}+o(1). \tag{8.22}$$

Towards (8.21) consider a check $b\in\mathscr{B}$ whose corresponding row sports i non-zero entries. Since we may pretend (up to $o(1)$ in total variation) that these entries are drawn uniformly and independently from the set of cavities, the probability that they are all frozen comes to $\boldsymbol{\alpha}^i+o(1)$. Since there are $\boldsymbol{M}_i^+-\boldsymbol{M}_i^--\boldsymbol{\gamma}_i$ such checks $b\in\mathscr{B}$, we obtain (8.21).

Moving on to (8.22), consider $a\in\mathscr{A}$ whose corresponding row has $i-1$ non-zero entries. By the same token as in the previous paragraph, the probability that all entries in the a-row correspond to frozen cavities comes to $\boldsymbol{\alpha}^{i-1}+o(1)$. Hence, the expected rank of the $\mathscr{A}\times V_n$-minor works out to be $\sum_{i\geq1}\left(1-\boldsymbol{\alpha}^{i-1}\right)\boldsymbol{\gamma}_i+o(1)$, which is the second summand in (8.22). Similarly, a $t\in\mathscr{T}$-row adds to the rank unless both the variables in the corresponding check are frozen. The latter event occurs with probability $\boldsymbol{\beta}^2$. Hence the first summand. Finally, the $\boldsymbol{C}$-column adds to the rank if none of the $\mathscr{A}\cup\mathscr{T}$-rows become all-zero, which occurs with probability $(1-\boldsymbol{\beta}^2)^{\boldsymbol{\lambda}'''}\prod_{i\geq1}\left(1-\boldsymbol{\alpha}^{i-1}\right)^{\boldsymbol{\gamma}_i}+o(1)$. □

Proof of Lemma 8.3. Letting $\mathfrak{E}=\mathscr{E}\cap\mathscr{E}'\cap\mathscr{E}''\cap\mathscr{E}'''$ and combining Claims 8.9–8.12, we obtain

$$\begin{aligned}\mathbb{E}\Big|\mathbb{E}\left[\mathrm{nul}(\boldsymbol{A}''')-\mathrm{nul}(\boldsymbol{A}')\mid\Sigma''\right]-\Big((1-\boldsymbol{\beta}^2)^{\boldsymbol{\lambda}'''}\prod_{i\geq1}(1-\boldsymbol{\alpha}^{i-1})^{\boldsymbol{\gamma}_i}-\sum_{i\geq1}(1-\boldsymbol{\alpha}^{i-1})\boldsymbol{\gamma}_i\\-\sum_{i\geq1}(1-\boldsymbol{\alpha}^i)(\boldsymbol{M}_i^+-\boldsymbol{M}_i^--\boldsymbol{\gamma}_i)-\boldsymbol{\lambda}'''(1-\boldsymbol{\beta}^2)\Big)\mathbb{1}_{\mathfrak{E}}\Big|=o_\varepsilon(1).\end{aligned} \tag{8.23}$$

On $\mathfrak{E}$ all i with $\boldsymbol{M}_i^+-\boldsymbol{M}_i^--\boldsymbol{\gamma}_i>0$ are bounded. Moreover, w.h.p. we have $\boldsymbol{M}_i\sim\mathbb{E}[\boldsymbol{M}_i]=\Omega(n)$ for all bounded i by Chebyshev's inequality. Hence, (8.7) implies that $\boldsymbol{M}_i^-=\boldsymbol{M}_i-\boldsymbol{\gamma}_i$ w.h.p. Consequently, (8.23) becomes

$$\begin{aligned}\mathbb{E}\Big|\mathbb{E}\left[\mathrm{nul}(\boldsymbol{A}''')-\mathrm{nul}(\boldsymbol{A}')\mid\Sigma''\right]-\Big((1-\boldsymbol{\beta}^2)^{\boldsymbol{\lambda}'''}\prod_{i\geq1}(1-\boldsymbol{\alpha}^{i-1})^{\boldsymbol{\gamma}_i}-\sum_{i\geq1}(1-\boldsymbol{\alpha}^{i-1})\boldsymbol{\gamma}_i\\-\sum_{i\geq1}(1-\boldsymbol{\alpha}^i)\boldsymbol{\Delta}_i-\boldsymbol{\lambda}'''(1-\boldsymbol{\beta}^2)\Big)\mathbb{1}_{\mathfrak{E}}\Big|=o_\varepsilon(1).\end{aligned} \tag{8.24}$$

We proceed to estimate the various terms on the r.h.s. of (8.24) separately. Since $\mathbb{P}[\mathfrak{E}]=1-o_\varepsilon(1)$ by Corollary 8.8 and Claims 8.9 and 8.10, Lemma 8.7 yield

$$\begin{aligned}\mathbb{E}\left[\mathbb{1}_{\mathfrak{E}}\cdot(1-\boldsymbol{\beta}^2)^{\boldsymbol{\lambda}'''}\prod_{i\geq1}(1-\boldsymbol{\alpha}^{i-1})^{\boldsymbol{\gamma}_i}\mid\Sigma''\right]&=\mathbb{E}\left[(1-\boldsymbol{\beta}^2)^{\boldsymbol{\lambda}'''}\prod_{i\geq1}(1-\boldsymbol{\alpha}^{i-1})^{\hat{\boldsymbol{\gamma}}_i}\mid\Sigma''\right]+o_\varepsilon(1)\\&=\exp(-3\delta\boldsymbol{\beta}^2)D(1-K'(\boldsymbol{\alpha})/k)\qquad\text{[by (3.2) and (8.10)].}\end{aligned} \tag{8.25}$$

Moreover, since $\sum_{i\geq1}\boldsymbol{\gamma}_i\leq\boldsymbol{d}_{n+1}$ and $\boldsymbol{d}_{n+1}$ has a bounded second moment, Lemma 8.7 implies that

$$\mathbb{E}\left[\mathbb{1}_{\mathfrak{E}}\cdot\sum_{i\geq1}(1-\boldsymbol{\alpha}^{i-1})\boldsymbol{\gamma}_i\mid\Sigma''\right]=\mathbb{E}\left[\sum_{i\geq1}(1-\boldsymbol{\alpha}^{i-1})\hat{\boldsymbol{\gamma}}_i\mid\Sigma''\right]+o_\varepsilon(1)=d-\frac{d}{k}K'(\boldsymbol{\alpha})+o_\varepsilon(1). \tag{8.26}$$

Further, by Claim 8.9, Lemma 8.7 and (8.14),

$$\mathbb{E}\left[\mathbb{1}_{\mathfrak{E}}\cdot\sum_{i\geq1}(1-\boldsymbol{\alpha}^i)\boldsymbol{\Delta}_i\mid\Sigma''\right]=\mathbb{E}\left[\sum_{i\geq1}(1-\boldsymbol{\alpha}^i)\boldsymbol{\Delta}_i\mid\Sigma''\right]+o_\varepsilon(1)=o_\varepsilon(1)+\frac{d}{k}-\frac{d}{k}\mathbb{E}[K(\boldsymbol{\alpha})]. \tag{8.27}$$

Finally, (8.10) yields

$$\mathbb{E}\left[\mathbb{1}_{\mathfrak{E}}\cdot\boldsymbol{\lambda}'''(1-\boldsymbol{\beta}^2)\mid\Sigma''\right]=3\delta(1-\boldsymbol{\beta}^2)+o_\varepsilon(1). \tag{8.28}$$

Thus, the assertion follows from (8.24)–(8.28). □

8.4. **Proof of Lemma 8.4.** We proceed similarly as in the proof of Lemma 8.3; actually matters are a bit simpler because we only add checks, while in the proof of Lemma 8.3 we also had to deal with the extra variable node x_{n+1}. Let $\mathscr{E},\mathscr{E}'$ be the events from (8.15) and (8.16) and let $\mathscr{E}'' = \{\boldsymbol{d}_{n+1} + \boldsymbol{\lambda}'' \le 1/\varepsilon\}$. As a direct consequence of the assumption $\mathbb{E}[\boldsymbol{d}_{n+1}^2] = O_{\varepsilon,n}(1)$ and of (8.9), we obtain the following.

Fact 8.13. *We have* $\mathbb{P}\left[\mathscr{E}''\right] = 1 - O_\varepsilon(\varepsilon^2)$.

Let

$$\mathscr{X}'' = \bigcup_{i\ge 1}\bigcup_{j\in[\boldsymbol{M}_i - \boldsymbol{M}_i^-]} \partial_{\boldsymbol{G}''} a''_{i,j} \cup \bigcup_{i=1}^{\boldsymbol{\lambda}''} \partial t''_i$$

be the set of variable nodes where the new checks that we add upon going from $\boldsymbol{A}'$ to $\boldsymbol{A}''$ attach. Let $\mathscr{E}'''$ be the event that in $\boldsymbol{G}''$ no variable from $\mathscr{X}''$ is connected with the checks $\{a''_{i,j} : i \ge 1, j \in [\boldsymbol{M}_i - \boldsymbol{M}_i^-]\} \cup \{t''_i : i \in [\boldsymbol{\lambda}'']\}$ by more than one edge.

Claim 8.14. *We have* $\mathbb{P}\left[\mathscr{E}''' \mid \mathscr{E}' \cap \mathscr{E}''\right] = 1 - o(1)$.

Proof. This follows from the "birthday paradox" (see the proof of Claim 8.10). □

Claim 8.15. *We have* $\mathbb{E}\left[\left|\mathrm{nul}(\boldsymbol{A}'') - \mathrm{nul}(\boldsymbol{A}')\right|(1 - \mathbb{1}\mathscr{E} \cap \mathscr{E}' \cap \mathscr{E}'' \cap \mathscr{E}''')\right] = o_\varepsilon(1)$.

Proof. We have $\left|\mathrm{nul}(\boldsymbol{A}'') - \mathrm{nul}(\boldsymbol{A}')\right| \le \boldsymbol{d}_{n+1} + \boldsymbol{\lambda}''$ as we add at most $\boldsymbol{d}_{n+1} + \boldsymbol{\lambda}''$ rows. Because $\mathbb{E}[(\boldsymbol{d}_{n+1} + \boldsymbol{\lambda}'')^2] = O_\varepsilon(1)$ by (8.9), Claim 8.13 and the Cauchy-Schwarz inequality yield

$$\mathbb{E}\left[\left|\mathrm{nul}(\boldsymbol{A}'') - \mathrm{nul}(\boldsymbol{A}')\right|(1 - \mathbb{1}\mathscr{E}'')\right] \le \mathbb{E}\left[(\boldsymbol{d}_{n+1} + \boldsymbol{\lambda}'')^2\right]^{1/2}(1 - \mathbb{P}[\mathscr{E}])^{1/2} = o_\varepsilon(1). \tag{8.29}$$

Moreover, Corollary 8.8 and Claim 8.14 show that

$$\mathbb{E}\left[\left|\mathrm{nul}(\boldsymbol{A}'') - \mathrm{nul}(\boldsymbol{A}')\right|\mathbb{1}\mathscr{E}'' \setminus \mathscr{E}\right], \mathbb{E}\left[\left|\mathrm{nul}(\boldsymbol{A}'') - \mathrm{nul}(\boldsymbol{A}')\right|\mathbb{1}\mathscr{E}'' \setminus \mathscr{E}'\right], \mathbb{E}\left[\left|\mathrm{nul}(\boldsymbol{A}'') - \mathrm{nul}(\boldsymbol{A}')\right|\mathbb{1}\mathscr{E}'' \setminus \mathscr{E}'''\right] = o_\varepsilon(1). \tag{8.30}$$

The assertion follows from (8.29) and(8.30). □

The matrix $\boldsymbol{A}''$ results from $\boldsymbol{A}'$ by adding checks $a''_{i,j}$, $i \ge 1$, $j \in [\boldsymbol{M}_i - \boldsymbol{M}_i^-]$ that are connected to random cavities of $\boldsymbol{A}'$.

Moreover, as before let $\Sigma'' \supset \Sigma'$ be the σ-algebra generated by $\boldsymbol{\theta}$, $\boldsymbol{G}'$, $\boldsymbol{A}'$, $\boldsymbol{M}_-$, $(\boldsymbol{d}_i)_{i\in[n+1]}$, $\boldsymbol{\gamma}$, $\boldsymbol{M}$, $\boldsymbol{\Delta}$, $\boldsymbol{\lambda}^-$, $\boldsymbol{\lambda}'''$. Then $\mathscr{E},\mathscr{E}',\mathscr{E}''$ are Σ''-measurable, but $\mathscr{E}'''$ is not.

Claim 8.16. *On* $\mathscr{E} \cap \mathscr{E}' \cap \mathscr{E}''$ *we have*

$$\mathbb{E}\left[(\mathrm{nul}(\boldsymbol{A}'') - \mathrm{nul}(\boldsymbol{A}'))\mathbb{1}\mathscr{E}''' \mid \Sigma''\right] = o_\varepsilon(1) - \sum_{i\ge 1}(1 - \boldsymbol{\alpha}^i)(\boldsymbol{M}_i - \boldsymbol{M}_i^-) - \boldsymbol{\lambda}''(1 - \boldsymbol{\beta}^3).$$

Proof. Let $\mathscr{A} = \{a''_{i,j} : i \ge 1,\ j \in [\boldsymbol{M}_i - \boldsymbol{M}_i^-]\}$. Moreover, let $\mathscr{T}$ be the set of new ternary checks t''_i, $i \in [\boldsymbol{\lambda}'']$. Let $\boldsymbol{B}$ be the $\mathbb{F}_q$-matrix whose rows are indexed by $\mathscr{A} \cup \mathscr{T}$ and whose columns are indexed by $V_n = \{x_1, \ldots, x_n\}$. The (a,x)-entry of $\boldsymbol{B}$ is zero unless a,x are adjacent in $\boldsymbol{G}''$, in which case the entry is an independent copy of $\boldsymbol{\chi}$. Given $\mathscr{E}'''$ the matrix $\boldsymbol{B}$ has full row rank $\mathrm{rk}(\boldsymbol{B}) = |\mathscr{A}| = \boldsymbol{\lambda}'' + \sum_{i\ge 1}\boldsymbol{M}_i^+ - \boldsymbol{M}_i$, because no column contains two non-zero entries and each row has at least one non-zero entry. Further, obtain $\boldsymbol{B}_*$ from $\boldsymbol{B}$ by zeroing out the x-column of every $x \in \mathfrak{F}(\boldsymbol{A}')$.

On $\mathscr{E} \cap \mathscr{E}' \cap \mathscr{E}'' \cap \mathscr{E}'''$ we see that

$$\mathrm{nul}\,\boldsymbol{A}'' = \mathrm{nul}\begin{pmatrix}\boldsymbol{A}'\\ \boldsymbol{B}\end{pmatrix}. \tag{8.31}$$

Moreover, let $\mathscr{I}$ be the set of non-zero columns of $\boldsymbol{B}$. Then on $\mathscr{E}' \cap \mathscr{E}''$ we have $|\mathscr{I}| \le \boldsymbol{d}_{n+1} + \boldsymbol{\lambda}'' \le 1/\varepsilon$. Hence, on $\mathscr{E} \cap \mathscr{E}' \cap \mathscr{E}'' \cap \mathscr{E}'''$ the probability that $\mathscr{I}$ forms a proper relation is bounded by $\exp(-1/\varepsilon^4)$. Hence, Lemma 3.2 shows

$$\mathbb{E}\left[\left(\mathrm{nul}(\boldsymbol{A}'') - \mathrm{nul}(\boldsymbol{A}')\right)\mathbb{1}\mathscr{E}''' \mid \Sigma''\right] = o_\varepsilon(1) - \mathbb{E}\left[\mathrm{rk}(\boldsymbol{B}_*) \mid \Sigma''\right]. \tag{8.32}$$

We are thus left to calculate the rank of $\boldsymbol{B}_*$. Recalling that $\boldsymbol{\alpha}$ stands for the fraction of frozen cavities, we see that for $a \in \mathscr{A}$ of degree i the a-row is all-zero in $\boldsymbol{B}_*$ with probability $\boldsymbol{\alpha}^i + o(1)$. Similarly, for $a \in \mathscr{T}$ the a-row of $\boldsymbol{B}$ gets zeroed out with probability $\boldsymbol{\beta}^3$. Hence, we conclude that

$$\mathbb{E}\left[\mathrm{rk}(\boldsymbol{B}_*) \mid \Sigma''\right] = o_\varepsilon(1) + \boldsymbol{\lambda}''(1 - \boldsymbol{\beta}^3) + \sum_{i\ge 1}\left(1 - \boldsymbol{\alpha}^i\right)(\boldsymbol{M}_i - \boldsymbol{M}_i^-). \tag{8.33}$$

Combining (8.32) and (8.33) completes the proof. □

Proof of Lemma 8.4. Let $\mathfrak{E} = \mathscr{E} \cap \mathscr{E}' \cap \mathscr{E}'' \cap \mathscr{E}'''$. Combining Claims 8.15–8.16, we see that

$$\mathbb{E}\left|\mathbb{E}[\mathrm{nul}(\boldsymbol{A}'') - \mathrm{nul}(\boldsymbol{A}') \mid \Sigma''] + \left(\boldsymbol{\lambda}''(1-\boldsymbol{\beta}^3) + \sum_{i\geq 1}(1-\boldsymbol{\alpha}^i)(\boldsymbol{M}_i - \boldsymbol{M}_i^-)\right)\mathbb{1}\mathfrak{E}\right| = o_\varepsilon(1). \tag{8.34}$$

On $\mathfrak{E}$ all degrees i with $\boldsymbol{M}_i^+ - \boldsymbol{M}_i^- > 0$ are bounded. Moreover, $\boldsymbol{M}_i^- = \Omega(n)$ w.h.p. for every bounded i by Chebyshev's inequality. Therefore, (8.7) shows that $\boldsymbol{M}_i - \boldsymbol{M}_i^- = \boldsymbol{\gamma}_i$ for all i with $\boldsymbol{M}_i^+ - \boldsymbol{M}_i^- > 0$ w.h.p. Hence, (8.34) turns into

$$\mathbb{E}\left|\mathbb{E}[\mathrm{nul}(\boldsymbol{A}'') - \mathrm{nul}(\boldsymbol{A}') \mid \Sigma''] + \left(\boldsymbol{\lambda}''(1-\boldsymbol{\beta}^3) + \sum_{i\geq 1}(1-\boldsymbol{\alpha}^i)\boldsymbol{\gamma}_i\right)\mathbb{1}\mathfrak{E}\right| = o_\varepsilon(1). \tag{8.35}$$

We now estimate the two parts of the last expression separately. Since $\mathbb{P}[\mathfrak{E}] = 1 - o_\varepsilon(1)$ by Corollary 8.8, Fact 8.13 and Claim 8.14, the definition (8.9) of $\boldsymbol{\lambda}''$ yields

$$\mathbb{E}\left|\boldsymbol{\lambda}''(1-\boldsymbol{\beta}^3)\mathbb{1}\mathfrak{E}\right| = 2\delta(1-\mathbb{E}[\boldsymbol{\beta}^3]) + o_\varepsilon(1). \tag{8.36}$$

Moreover, because $\sum_{i\geq 1}\boldsymbol{\gamma}_i \leq \boldsymbol{d}_{n+1}$, $\mathbb{E}[\boldsymbol{d}_{n+1}] = O_\varepsilon(1)$,

$$\begin{aligned}
\mathbb{E}\left[\sum_{i\geq 1}(1-\boldsymbol{\alpha}^i)\boldsymbol{\gamma}_i\mathbb{1}\mathfrak{E}\right] &= \mathbb{E}\left[\sum_{i\geq 1}(1-\boldsymbol{\alpha}^i)\hat{\boldsymbol{\gamma}}_i\mathbb{1}\left\{\boldsymbol{\lambda}'' + \sum_{i\geq 1}\hat{\boldsymbol{\gamma}}_i \leq \varepsilon^{-1/4}\right\}\right] + o_\varepsilon(1) && \text{[by Lemma 8.7 and Claim 8.13]}\\
&= d\mathbb{E}[1-\boldsymbol{\alpha}^{\hat{\boldsymbol{k}}}] + o_\varepsilon(1) = d - d\mathbb{E}[\boldsymbol{\alpha}K'(\boldsymbol{\alpha})]/k + o_\varepsilon(1) && \text{[by (3.2)]}.
\end{aligned} \tag{8.37}$$

Combining (8.36) and (8.37) completes the proof. □

8.5. **Proof of Lemma 8.2.** The proof is relatively straightforward, not least because once again we can reuse some technical statements from [10]. Let us deal with $\boldsymbol{A}''$ and $\boldsymbol{A}'''$ separately.

Claim 8.17. *We have* $\mathbb{E}[\mathrm{nul}(\boldsymbol{A}'')] = \mathbb{E}[\mathrm{nul}(\boldsymbol{A}_{n,\boldsymbol{M},\lambda})] + o(1)$.

Proof. The matrix models $\boldsymbol{A}_{n,\boldsymbol{M},\lambda}$ and $\boldsymbol{A}''$ coincide with the corresponding models from [10, Claim 5.17], except that here we add extra ternary checks. Because these extra checks are added independently, the coupling from [10, Claim 5.17] directly induces a coupling of the enhanced models by attaching the same number $\boldsymbol{\lambda}''$ of ternary equations to the same neighbors. □

Claim 8.18. *We have* $\mathbb{E}[\mathrm{nul}(\boldsymbol{A}''')] = \mathbb{E}[\mathrm{nul}(\boldsymbol{A}_{n+1,\boldsymbol{M}^+,\lambda^+})] + o(1)$.

Proof. The matrix models $\boldsymbol{A}_{n+1,\boldsymbol{M}^+,\lambda^+}$ and $\boldsymbol{A}''''$ coincide with the corresponding models from [10, Section 5.5] plus the extra independent ternary equations. Hence, the coupling from [10, Claim 5.17] yields a coupling of the enhanced models just as in Claim 8.17. □

Proof of Lemma 8.2. The lemma is an immediate consequence of Claims 8.17 and 8.18. □

References

[1] D. Achlioptas, F. McSherry: Fast computation of low-rank matrix approximations. Journal of the ACM **54** (2007) #9.
[2] D. Achlioptas, M. Molloy: The solution space geometry of random linear equations. Random Structures and Algorithms **46** (2015) 197–231.
[3] D. Achlioptas, C. Moore: Random k-SAT: two moments suffice to cross a sharp threshold. SIAM Journal on Computing **36** (2006) 740–762.
[4] D. Achlioptas, A. Naor, Y. Peres: Rigorous location of phase transitions in hard optimization problems. Nature **435** 759–764.
[5] M. Aizenman, R. Sims, S. Starr: An extended variational principle for the SK spin-glass model. Phys. Rev. B **68** (2003) 214403.
[6] P. Ayre, A. Coja-Oghlan, P. Gao, N. Müller: The satisfiability threshold for random linear equations. Combinatorica **40** (2020) 179–235.
[7] G. Balakin: The distribution of random matrices over a finite field. Theory Probab. Appl. **13** (1968) 631–641.
[8] J. Blömer, R. Karp, E. Welzl: The rank of sparse random matrices over finite fields. Random Structures and Algorithms **10** (1997) 407–419.
[9] C. Bordenave, M. Lelarge, J. Salez: The rank of diluted random graphs. Ann. Probab. **39** (2011) 1097–1121.
[10] A. Coja-Oghlan, A. Ergür, P. Gao, S. Hetterich, M. Rolvien: The rank of sparse random matrices. Proc. 31st SODA (2020) 579–591.
[11] A. Coja-Oghlan, F. Krzakala, W. Perkins, L. Zdeborova: Information-theoretic thresholds from the cavity method. Advances in Mathematics **333** (2018) 694–795.
[12] A. Coja-Oghlan, K. Panagiotou: The asymptotic k-SAT threshold. Advances in Mathematics **288** (2016) 985–1068.
[13] A. Coja-Oghlan, K. Panagiotou: Catching the k-NAESAT threshold. Proc. 44th STOC (2012) 899–908.
[14] A. Coja-Oghlan, N. Müller, J. Ravelomanana: Belief Propagation on the random k-SAT model. Annals of Applied Probability, in press.
[15] C. Cooper, A. Frieze, W. Pegden: On the rank of a random binary matrix. Electron. J. Comb. **26** (2019) P4.12.
[16] K. Costello, V. Vu: The rank of random graphs. Random Structures and Algorithms **33** (2008) 269–285.
[17] K. Costello, V. Vu: On the rank of random sparse matrices. Combinatorics, Probability and Computing **19** (2010) 321–342.
[18] B. Davis, D. McDonald: An elementary proof of the local limit theorem. Journal of Theoretical Probability **8** (1995) 693–701.

[19] M. Dietzfelbinger, A. Goerdt, M. Mitzenmacher, A. Montanari, R. Pagh, M. Rink: Tight thresholds for cuckoo hashing via XORSAT. Proc. 37th ICALP (2010) 213–225.
[20] J. Ding, A. Sly, N. Sun: Proof of the satisfiability conjecture for large k. Proc. 47th STOC (2015) 59–68.
[21] O. Dubois, J. Mandler: The 3-XORSAT threshold. Proc. 43rd FOCS (2002) 769–778.
[22] A. Ferber, M. Kwan, A. Sah, M. Sawhney: Singularity of the k-core of a random graph. arXiv:2106.05719
[23] A. Goerdt, L. Falke: Satisfiability thresholds beyond k-XORSAT. Proc. 7th International Computer Science Symposium in Russia (2012) 148–159.
[24] J. Huang: Invertibility of adjacency matrices for random d-regular graphs. arXiv:1807.06465.
[25] M. Ibrahimi, Y. Kanoria, M. Kraning, A. Montanari: The set of solutions of random XORSAT formulae. Annals of Applied Probability **25** (2015) 2743–2808.
[26] J. Kahn; J. Komloś, E. Szemerédi: On the probability that a random ±1-matrix is singular. Journal of the AMS **8** (1995) 223–240.
[27] V. Kolchin: Random graphs and systems of linear equations in finite fields. Random Structures and Algorithms **5** (1995) 425–436.
[28] V. Kolchin, V. Khokhlov: On the number of cycles in a random non-equiprobable graph. Discrete Math. Appl. **2** (1992) 109–118.
[29] V. Kolchin: Consistency of a system of random congruences. Discrete Math. Appl. **3** (1993) 103–113.
[30] J. Komlós: On the determinant of (0,1) matrices. Studia Sci. Math. Hungar. **2** (1967) 7–21.
[31] I. Kovalenko: On the limit distribution of the number of solutions of a random system of linear equations in the class of Boolean functions. Theory Probab. Appl. **12** (1967) 51–61.
[32] I. Kovalenko, A. Levitskaya, M. Savchuk: Selected problems of probabilistic combinatorics. Naukova Dumka, Kiev (1986).
[33] H. Lenstra: Lattices. In J. Buhler, P. Stevenhagen (eds.): Algorithmic number theory: lattices, number fields, curves and cryptography. Cambridge University Press (2008) 127–181.
[34] A. Levitskaya: Theorems on invariance for the systems of random linear equations over an arbitrary finite ring. Soviet Math. Dokl. **263** (1982) 289–291.
[35] A. Levitskaya: The probability of consistency of a system of random linear equations over a finite ring. Theory Probab. Appl. **30** (1985) 339–350.
[36] M. Mézard, A. Montanari: Information, physics and computation. Oxford University Press 2009.
[37] M. Mézard, F. Ricci-Tersenghi, R. Zecchina: Two solutions to diluted p-spin models and XORSAT problems. Journal of Statistical Physics **111** (2003) 505–533.
[38] G. Miller, G. Cohen: The rate of regular LDPC codes. IEEE Transactions on Information Theory **49** (2003) 2989–2992.
[39] A. Montanari: Estimating random variables from random sparse observations. European Transactions on Telecommunications **19**(4) (2008) 385–403.
[40] B. Pittel, G. Sorkin: The satisfiability threshold for k-XORSAT. Combinatorics, Probability and Computing **25** (2016) 236–268.
[41] M. Raič: A multivariate Berry–Esseen theorem with explicit constants. Bernoulli **25** (2019) 2824–2853.
[42] P. Raghavendra, N. Tan: Approximating CSPs with global cardinality constraints using SDP hierarchies. Proc. 23rd SODA (2012) 373–387.
[43] T. Richardson, R. Urbanke: Modern coding theory. Cambridge University Press (2008).
[44] T. Tao, V. Vu: On the singularity probability of random Bernoulli matrices. Journal of the AMS **20** (2007) 603–628.
[45] K. Tikhomirov: Singularity of random Bernoulli matrices. Annals of Mathematics **191** (2020) 593–634.
[46] V. Vu: Combinatorial problems in random matrix theory. Proc. International Congress of Mathematicians IV (2014) 489–508.
[47] V. Vu: Recent progress in combinatorial random matrix theory. arXiv:2005.02797.
[48] M. Wainwright, E. Maneva, E. Martinian: Lossy source compression using low-density generator matrix codes: analysis and algorithms. IEEE Trans. Inf. Theory **56** (2010) 1351–1368.

9. Appendix

In this appendix we give a self-contained proof of Lemma 7.16, the local limit theorem for sums of independent vectors. We employ a simplified version of the strategy of the proof of Lemma 7.9. Recall that we assume the existence of a constant $\eta > 0$ such that $\mathbb{E}[\boldsymbol{d}^{2+\eta}] + \mathbb{E}[\boldsymbol{k}^{2+\eta}] < \infty$.

Given $\omega > 0$, we choose $\varepsilon_0 = \varepsilon_0(\omega, q)$ sufficiently small and let $0 < \varepsilon < \varepsilon_0$. With these parameters, we set

$$s_n := \sqrt{\sum_{i=1}^{n} \boldsymbol{d}_i^2}. \tag{9.1}$$

As in the proof of Lemma 7.16, given $\omega > 0$, we choose $\varepsilon_0 = \varepsilon_0(\omega, q)$ sufficiently small and let $0 < \varepsilon < \varepsilon_0$. With these parameters, we set

$$\mathfrak{L}_0 = \left\{ r \in \mathbb{Z}^{\mathbb{F}_q^*} : \mathbb{P}_{\mathfrak{A}}\left(\hat{\rho}_{\boldsymbol{\sigma}} = r\right) > 0 \text{ and } \left\| r - \frac{\boldsymbol{\Delta}}{q}\mathbb{1} \right\|_1 < \omega n^{-1/2}\boldsymbol{\Delta} \right\} \quad \text{and}$$
$$\mathfrak{L}_0(r_*, \varepsilon) = \{ r \in \mathfrak{L}_0 : \|r - r_*\|_\infty < \varepsilon s_n \}.$$

Then

$$\mathfrak{L}_0 \subseteq \mathfrak{d}\mathbb{Z}^{\mathbb{F}_q^*}.$$

We begin by observing that the vector $\hat{\rho}_{\boldsymbol{\sigma}}$ is asymptotically normal given $\mathfrak{A}$. As before we let $\boldsymbol{I}_{q-1}$ the $(q-1)\times(q-1)$-identity matrix and let $\boldsymbol{N}\in\mathbb{R}^{\mathbb{F}_q^*}$ be a Gaussian vector with zero mean and covariance matrix

$$\mathscr{C} = q^{-1}\boldsymbol{I}_{q-1} - q^{-2}\mathbb{1}_{(q-1)\times(q-1)}. \tag{9.2}$$

Claim 9.1. *There exists a function $\iota = \iota_{\eta,q}(n) = o(1)$ such that for all axis-aligned cubes $U\subseteq\mathbb{R}^{\mathbb{F}_q^*}$ we have*

$$\mathbb{E}\left|\mathbb{P}_{\mathfrak{A}}\left[\frac{\hat{\rho}_{\boldsymbol{\sigma}} - q^{-1}\boldsymbol{\Delta}\mathbb{1}}{s_n}\in U\right] - \mathbb{P}\left[\boldsymbol{N}\in U\right]\right| \le \iota.$$

Proof. The mean of each entry $\hat{\rho}_{\boldsymbol{\sigma}}(\tau)$ clearly equals $\boldsymbol{\Delta}/q$ for every $\tau\in\mathbb{F}_q^*$. Concerning the covariance matrix, for distinct $s\neq t$ we obtain

$$\mathbb{E}_{\mathfrak{A}}[\hat{\rho}_{\boldsymbol{\sigma}}^2(s)] = \sum_{i,j\in[n]:i\neq j}\frac{\boldsymbol{d}_i\boldsymbol{d}_j}{q^2} + \sum_{i=1}^n\frac{\boldsymbol{d}_i^2}{q} = \sum_{i,j=1}^n\frac{\boldsymbol{d}_i\boldsymbol{d}_j}{q^2} + \sum_{i=1}^n\frac{\boldsymbol{d}_i^2}{q}\left(1-\frac{1}{q}\right),$$
$$\mathbb{E}_{\mathfrak{A}}[\hat{\rho}_{\boldsymbol{\sigma}}(s)\hat{\rho}_{\boldsymbol{\sigma}}(t)] = \sum_{i,j\in[n]:i\neq j}\frac{\boldsymbol{d}_i\boldsymbol{d}_j}{q^2} = \sum_{i,j=1}^n\frac{\boldsymbol{d}_i\boldsymbol{d}_j}{q^2} - \sum_{i=1}^n\frac{\boldsymbol{d}_i^2}{q^2}.$$

Hence, the means and covariances of $(\hat{\rho}_{\boldsymbol{\sigma}} - q^{-1}\boldsymbol{\Delta}\mathbb{1})/s_n$ and $\boldsymbol{N}$ match.

We are thus left to prove that $(\hat{\rho}_{\boldsymbol{\sigma}} - q^{-1}\boldsymbol{\Delta}\mathbb{1})/s_n$ is asymptotically normal, with the required uniformity. Thus, given a small $\xi>0$ we pick $\mathfrak{D} = \mathfrak{D}(q,\eta,\xi) > 0$ and $n_0 = n_0(\mathfrak{D})$ sufficiently large. Suppose $n > n_0$ and let

$$\boldsymbol{d}_i' = \mathbb{1}\{\boldsymbol{d}_i\le\mathfrak{D}\}\boldsymbol{d}_i, \qquad \boldsymbol{d}_i'' = \boldsymbol{d}_i - \boldsymbol{d}_i',$$
$$\hat{\rho}_{\boldsymbol{\sigma}}'(s) = \sum_{i=1}^n\mathbb{1}\{\boldsymbol{\sigma}_i = s\}\boldsymbol{d}_i', \qquad \hat{\rho}_{\boldsymbol{\sigma}}''(s) = \sum_{i=1}^n\mathbb{1}\{\boldsymbol{\sigma}_i = s\}\boldsymbol{d}_i'',$$
$$s_n'^2 = \sum_{i=1}^n\boldsymbol{d}_i'^2, \qquad s_n''^2 = \sum_{i=1}^n\boldsymbol{d}_i''^2,$$
$$\boldsymbol{\Delta}' = \sum_{i=1}^n\boldsymbol{d}_i', \qquad \boldsymbol{\Delta}'' = \sum_{i=1}^n\boldsymbol{d}_i''.$$

Since $\mathbb{E}[\boldsymbol{d}^{2+\eta}]<\infty$, by Markov's inequality and by construction we have w.h.p.

$$\boldsymbol{\Delta}'' < \xi^8 n, \qquad \boldsymbol{\Delta} = \boldsymbol{\Delta}' + \boldsymbol{\Delta}'', \qquad s_n''^2 < \xi^8 n, \qquad s_n'^2 < \mathfrak{D}^2 n, \qquad s_n^2 = s_n'^2 + s_n''^2, \tag{9.3}$$

providing $\mathfrak{D}$ is large enough. Hence, the multivariate Berry–Esseen theorem (e.g., [41]) shows that w.h.p. for all U,

$$\mathbb{P}_{\mathfrak{A}}\left[\frac{\hat{\rho}_{\boldsymbol{\sigma}}' - q^{-1}\boldsymbol{\Delta}'\mathbb{1}}{s_n'}\in U\right] - \mathbb{P}\left[\boldsymbol{N}\in U\right] = O(n^{-1/2}). \tag{9.4}$$

Furthermore, combining (9.3) with Chebyshev's inequality, we see that w.h.p.

$$\mathbb{P}_{\mathfrak{A}}\left[\left|\frac{\hat{\rho}_{\boldsymbol{\sigma}}'' - q^{-1}\boldsymbol{\Delta}''\mathbb{1}}{s_n}\right| > \xi^2\right] < \xi^2. \tag{9.5}$$

Thus, combining (9.4) and (9.5), we conclude that w.h.p.

$$\left|\mathbb{P}_{\mathfrak{A}}\left[\frac{\hat{\rho}_{\boldsymbol{\sigma}} - q^{-1}\boldsymbol{\Delta}\mathbb{1}}{s_n}\in U\right] - \mathbb{P}\left[\boldsymbol{N}\in U\right]\right| \le \xi. \tag{9.6}$$

Finally, the assertion follows from (9.6) by taking the limit $\xi\to 0$ slowly enough as $n\to\infty$. □

There exist $g\in\mathbb{N}$, $a_1,\dots,a_g\in\mathbb{Z}$ and $\delta_1,\dots,\delta_g$ in the support of $\boldsymbol{d}$ such that the greatest common divisor of the support can be linearly combined as

$$\mathfrak{d} = \sum_{i=1}^g a_i\delta_i. \tag{9.7}$$

We next count how many variables there are with degree δ_i. For $i\in[g]$, let $\mathfrak{I}_i$ denote the set of all $j\in[n]$ with $\boldsymbol{d}_j = \delta_i$ (the set of all variables that appear in δ_i equations). Set $\mathfrak{I}_0 = [n]\setminus\left(\mathfrak{I}_1\cup\ldots\cup\mathfrak{I}_g\right)$. Then

$$\mathfrak{I}_0\cup\ldots\cup\mathfrak{I}_g = [n]$$

and $|\mathfrak{I}_0|, |\mathfrak{I}_1|, \ldots, |\mathfrak{I}_g| = \Theta(n)$ w.h.p. (if $\mathfrak{I}_0$ is non-empty). We further count how many entries of value $s \in \mathbb{F}_q^*$ all variables of degree δ_i generate under the assignment $\boldsymbol{\sigma}$, and the contribution from the rest, yielding

$$\boldsymbol{r}_0(s) = \sum_{j \in \mathfrak{I}_0} \boldsymbol{d}_j \mathbb{1}\{\boldsymbol{\sigma}_j = s\}, \qquad \boldsymbol{r}_i(s) = \sum_{j \in \mathfrak{I}_i} \mathbb{1}\{\boldsymbol{\sigma}_j = s\}. \qquad (i \in [g], s \in \mathbb{F}_q^*)$$

Then summing the contributions, we get back $\hat{\rho}_{\boldsymbol{\sigma}} = \boldsymbol{r}_0 + \sum_{i=1}^g \delta_i \boldsymbol{r}_i$, where $\boldsymbol{r}_i = (\boldsymbol{r}_i(s))_{s \in \mathbb{F}_q^*}$.

Because $\boldsymbol{\sigma}_1, \ldots, \boldsymbol{\sigma}_n$ are mutually independent given $\mathfrak{A}$, so are $\boldsymbol{r}_0, \boldsymbol{r}_1, \ldots, \boldsymbol{r}_g$. Moreover, given $\mathfrak{A}$, for $i \in [g]$, $\boldsymbol{r}_i$ has a multinomial distribution with parameter $|\mathfrak{I}_i|$ and uniform probabilities q^{-1}. In effect, the individual entries $\boldsymbol{r}_i(s)$, $s \in \mathbb{F}_q^*$, will typically differ by only a few standard deviations, i.e., their typical difference will be of order $O(\sqrt{|\mathfrak{I}_i|})$. We require a precise quantitative version of this statement.

Furthermore, we say that $\boldsymbol{r}_i$ is *t-tame* if $|\boldsymbol{r}_i(s) - q^{-1}|\mathfrak{I}_i|| \le t\sqrt{|\mathfrak{I}_i|}$ for all $s \in \mathbb{F}_q^*$. Let $\mathfrak{T}(t)$ be the event that $\boldsymbol{r}_1, \ldots, \boldsymbol{r}_g$ are t-tame.

Lemma 9.2. *W.h.p. for every $r_* \in \mathfrak{L}_0$ there exists $r^* \in \mathfrak{L}_0(r_*, \varepsilon)$ such that*

$$\mathbb{P}_{\mathfrak{A}}\left[\hat{\rho}_{\boldsymbol{\sigma}} = r^*\right] \ge \frac{1}{2|\mathfrak{L}_0(r_*, \varepsilon)|} \qquad \textit{and} \qquad \mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(-\log\varepsilon) \mid \hat{\rho}_{\boldsymbol{\sigma}} = r^*\right] \ge 1 - \varepsilon^4. \tag{9.8}$$

Proof. Since $\boldsymbol{r}_i$ has a multinomial distribution given $\mathfrak{A}$ the Chernoff bound shows that for a large enough $c = c(q)$ w.h.p.

$$\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(-\log\varepsilon)\right] \ge 1 - \exp(-\Omega_\varepsilon(\log^2(\varepsilon))). \tag{9.9}$$

Further, Claim 9.1 implies that w.h.p. $\mathbb{P}_{\mathfrak{A}}\left[\hat{\rho}_{\boldsymbol{\sigma}} \in \mathfrak{L}_0(r_*, \varepsilon)\right] \ge \Omega_\varepsilon(\varepsilon^{q-1}) \ge \varepsilon^q$, provided $\varepsilon < \varepsilon_0 = \varepsilon_0(\omega)$ is small enough. Combining this estimate with (9.9) and Bayes' formula, we conclude that w.h.p. for every $r_* \in \mathfrak{L}_0$,

$$\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(-\log\varepsilon),\ \hat{\rho}_{\boldsymbol{\sigma}} \in \mathfrak{L}_0(r_*, \varepsilon)\right] \ge 1 - \varepsilon^5. \tag{9.10}$$

To complete the proof, assume that there does not exist $r^* \in \mathfrak{L}_0(r_*, \varepsilon)$ that satisfies (9.8). Then for every $r \in \mathfrak{L}_0(r_*, \varepsilon)$ we either have

$$\mathbb{P}_{\mathfrak{A}}\left[\hat{\rho}_{\boldsymbol{\sigma}} = r\right] < \frac{1}{2|\mathfrak{L}_0(r_*, \varepsilon)|} \qquad \text{or} \tag{9.11}$$

$$\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(-\log\varepsilon) | \hat{\rho}_{\boldsymbol{\sigma}} = r\right] < 1 - \varepsilon^4. \tag{9.12}$$

Let $\mathfrak{X}_0$ be the set of all $r \in \mathfrak{L}_0(r_*, \varepsilon)$ for which (9.11) holds, and let $\mathfrak{X}_1 = \mathfrak{L}_0(r_*, \varepsilon) \setminus \mathfrak{X}_0$. Then (9.11)–(9.12) yield

$$\begin{aligned}\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(-\log\varepsilon) \mid \hat{\rho}_{\boldsymbol{\sigma}} \in \mathfrak{L}_0(r_*, \varepsilon)\right] &\le \frac{\mathbb{P}_{\mathfrak{A}}\left[\hat{\rho}_{\boldsymbol{\sigma}} \in \mathfrak{X}_0\right] + \sum_{r \in \mathfrak{X}_1} \mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(-\log\varepsilon) | \hat{\rho}_{\boldsymbol{\sigma}} = r\right] \mathbb{P}_{\mathfrak{A}}\left[\hat{\rho}_{\boldsymbol{\sigma}} = r\right]}{\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{L}_0(r_*, \varepsilon)\right]} \\ &\le \frac{\mathbb{P}_{\mathfrak{A}}\left[\hat{\rho}_{\boldsymbol{\sigma}} \in \mathfrak{X}_0\right] + (1 - \varepsilon^4)\mathbb{P}_{\mathfrak{A}}\left[\hat{\rho}_{\boldsymbol{\sigma}} \in \mathfrak{X}_1\right]}{|\mathfrak{L}_0(r_*, \varepsilon)|} < 1 - \varepsilon^4,\end{aligned}$$

provided that $1 - \varepsilon^4 > \frac{1}{2}$, in contradiction to (9.10). □

Also let $\mathfrak{T}(r, t)$ be the event that $\hat{\rho}_{\boldsymbol{\sigma}} = r$ and that $\boldsymbol{r}_1, \ldots, \boldsymbol{r}_g$ are t-tame. We write $(r_0, \ldots, r_g) \in \mathfrak{T}(r, t)$ if $r_0 + \sum_{i=1}^g \delta_i r_i = r$ and $|r_i(s) - q^{-1}|\mathfrak{I}_i|| \le t\sqrt{|\mathfrak{I}_i|}$ for all $s \in \mathbb{F}_q^*$. The following lemma summarises the key step of the proof of Lemma 7.9.

Lemma 9.3. *W.h.p. for any $r_* \in \mathfrak{L}_0$, any $1 \le t \le \log n$ and any $r, r' \in \mathfrak{L}_0(r_*, \varepsilon)$ there exists a one-to-one map $\psi : \mathfrak{T}(r, t) \to \mathfrak{T}(r', t + O_\varepsilon(\varepsilon))$ such that for all $(r_0, \ldots, r_g) \in \mathfrak{T}(r, t)$ we have*

$$\log \frac{\mathbb{P}_{\mathfrak{A}}\left[(\boldsymbol{r}_0, \ldots, \boldsymbol{r}_g) = (r_0, \ldots, r_g)\right]}{\mathbb{P}_{\mathfrak{A}}\left[(\boldsymbol{r}_0, , \ldots, \boldsymbol{r}_r) = \psi(r_0, \ldots, r_g)\right]} = O_\varepsilon(\varepsilon(\omega + t)). \tag{9.13}$$

Proof. Since $r, r' \in \mathfrak{L}_0(r_*, \varepsilon)$, we have $r - r' \in \mathfrak{d}\mathbb{Z}^{\mathbb{F}_q^*}$. Hence, with $e_1, \ldots, e_{q-1}$ denoting the standard basis of $\mathbb{R}^{\mathbb{F}_q^*}$, there is a unique representation

$$r' - r = \sum_{i=1}^{q-1} \lambda_i \mathfrak{d} e_i \tag{9.14}$$

with $\lambda_1,\dots,\lambda_{q-1}\in\mathbb{Z}$. Because $r,r'\in\mathfrak{L}_0(r_*,\varepsilon)$ and

$$\lambda:=\begin{pmatrix}\lambda_1\\ \vdots\\ \lambda_{q-1}\end{pmatrix}=\mathfrak{d}^{-1}(r'-r),$$

the coefficients satisfy

$$|\lambda_i|=O_\varepsilon(\varepsilon s_n)\qquad\text{for all } i=1,\dots,q-1. \tag{9.15}$$

Now recall $g\in\mathbb{N}$, $a_1,\dots,a_g\in\mathbb{Z}$ and $\delta_1,\dots,\delta_g$ in the support of $\boldsymbol{d}$ with

$$\mathfrak{d}=\sum_{i=1}^g a_i\delta_i.$$

Fir $i\in[g]$, we set

$$r_i'=r_i+\frac{a_i}{\mathfrak{d}}\lambda$$

as well as $r_0'=r_0$. Further, define $\psi(r_0,\dots,r_g)=(r_0',\dots,r_g')$. Then clearly

$$r_0+\sum_{i=1}^g\delta_i r_i'=r+\sum_{i=1}^g\frac{a_i\delta_i}{\mathfrak{d}}\lambda=r+r'-r=r'. \tag{9.16}$$

and due to (9.15), we have $\psi(r_0,\dots,r_g)\in\mathfrak{T}(r',t+O_\varepsilon(\varepsilon))$. Finally, for $i\in[g]$ set

$$r_i(0)=|\mathfrak{I}_i|-\sum_{s\in\mathbb{F}_q^*}r_i(s),\qquad r_i'(0)=|\mathfrak{I}_i|-\sum_{s\in\mathbb{F}_q^*}r_i'(s).$$

Moreover, Stirling's formula and the mean value theorem show that

$$\begin{aligned}\frac{\mathbb{P}_{\mathfrak{A}}\left[(\boldsymbol{r}_0,\dots,\boldsymbol{r}_g)=(r_0,\dots,r_g)\right]}{\mathbb{P}_{\mathfrak{A}}\left[(\boldsymbol{r}_0,\dots,\boldsymbol{r}_g)=\psi(r_0,\dots,r_g)\right]}&=\frac{\binom{|\mathfrak{I}_1|}{(r_1(0),r_1)}\cdot\ldots\cdot\binom{|\mathfrak{I}_g|}{(r_g(0),r_g)}}{\binom{|\mathfrak{I}_1|}{(r_1'(0),r_1')}\cdot\ldots\cdot\binom{|\mathfrak{I}_g|}{(r_g'(0),r_g')}}=\exp\left[\sum_{i=1}^g\sum_{s\in\mathbb{F}_q}O_\varepsilon\left(r_i'(s)\log r_i'(s)-r_i(s)\log r_i(s)\right)\right]\\&=\exp\left[\sum_{i=1}^g O_\varepsilon(|\mathfrak{I}_i|)\sum_{s\in\mathbb{F}_q}\left|\int_{r_i(s)/|\mathfrak{I}_i|}^{r_i'(s)/|\mathfrak{I}_i|}\log z\mathrm{d}z\right|\right]\\&=\exp\left[\sum_{i=1}^g O_\varepsilon(|\mathfrak{I}_i|)\sum_{s\in\mathbb{F}_q}\left(\frac{r_i'(s)}{|\mathfrak{I}_i|}-\frac{r_i(s)}{|\mathfrak{I}_i|}\right)\log\left(\frac{1}{q}+O_\varepsilon\left(\frac{(\omega+t)s_n}{|\mathfrak{I}_i|}\right)\right)\right]\\&=\exp\left[\sum_{i=1}^g O_\varepsilon(|\mathfrak{I}_i|)\sum_{s\in\mathbb{F}_q}O_\varepsilon\left(\frac{(\omega+t)s_n}{|\mathfrak{I}_i|}\left(\frac{r_i'(s)}{|\mathfrak{I}_i|}-\frac{r_i(s)}{|\mathfrak{I}_i|}\right)\right)\right].\end{aligned} \tag{9.17}$$

Since $|\mathfrak{I}_1|,\dots,|\mathfrak{I}_g|=\Theta_\varepsilon(n)$ w.h.p., (9.17) implies (9.13). Finally, ψ is one-to-one because each vector has a unique representation with respect to the basis $(e_1,\dots,e_{q-1})$. □

Roughly speaking, Lemma7.14 shows that any two tame $r,r'\in\mathfrak{L}_0(r_*,\varepsilon)$ close to a conceivable $r_*\in\mathfrak{L}_0$ are about equally likely. However, the map ψ produces solutions that are a little less tame than the ones we start from. The following corollary, which combines Lemmas 7.13 and 7.14, remedies this issue.

Corollary 9.4. *W.h.p. for all $r_*\in\mathfrak{L}_0$ and all $r,r'\in\mathfrak{L}_0(r_*,\varepsilon)$ we have*

$$\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(r,-3\log\varepsilon)\right]=(1+o_\varepsilon(1))\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(r',-3\log\varepsilon)\right].$$

Proof. Let r^* be the vector supplied by Lemma 9.2. Applying Lemma 9.3 to r^* and $r\in\mathfrak{L}_0(r_*,\varepsilon)$, we see that w.h.p.

$$\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(r,-2\log\varepsilon)\right]\geq(1+O_\varepsilon(\varepsilon\log\varepsilon))\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(r^*,-\log\varepsilon)\right]\geq\frac{1}{3|\mathfrak{L}_0(r_*,\varepsilon)|}\qquad\text{for all } r\in\mathfrak{L}_0(r_*,\varepsilon). \tag{9.18}$$

In addition, we claim that w.h.p.

$$\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(r,-4\log\varepsilon)\setminus\mathfrak{T}(r,-3\log\varepsilon)\right]\leq\varepsilon\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(r^*,-\log\varepsilon)\right]\qquad\text{for all } r\in\mathfrak{L}_0(r_*,\varepsilon). \tag{9.19}$$

Indeed, applying Lemma 7.14 twice to r and r^* and invoking (7.24), we see that w.h.p.

$$\begin{aligned}\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(r,-2\log\varepsilon)\right] &\geq \exp(O_\varepsilon(\varepsilon\log\varepsilon))\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(r^*,-3\log\varepsilon)\right]\\ &\geq \left(1-O_\varepsilon(\varepsilon\log\varepsilon)\right)\mathbb{P}_{\mathfrak{A}}\left[\hat{\rho}_{\boldsymbol{\sigma}}=r^*\right], \qquad (9.20)\\ \mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(r,-4\log\varepsilon)\setminus\mathfrak{T}(r,-3\log\varepsilon)\right] &\leq \exp(O_\varepsilon(\varepsilon\log\varepsilon))\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(r^*,-3\log\varepsilon)\setminus\mathfrak{T}(r^*,-2\log\varepsilon)\right]\\ &\leq O_\varepsilon(\varepsilon^4)\mathbb{P}_{\mathfrak{A}}\left[\hat{\rho}_{\boldsymbol{\sigma}}=r^*\right]. \qquad (9.21)\end{aligned}$$

Combining (9.20) and (9.21) yields (9.19).

Finally, (7.24), (9.18) and (9.19) show that w.h.p.

$$\mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(-3\log\varepsilon)\mid\hat{\rho}_{\boldsymbol{\sigma}}=r\right]\geq 1-\sqrt{\varepsilon},\quad \mathbb{P}_{\mathfrak{A}}\left[\mathfrak{T}(-3\log\varepsilon)\mid\hat{\rho}_{\boldsymbol{\sigma}}=r'\right]\geq 1-\sqrt{\varepsilon}\qquad\text{for all } r,r'\in\mathfrak{L}_0(r_*,\varepsilon), \qquad (9.22)$$

and combining (9.22) with Lemma 9.3 completes the proof. □

Proof of Lemma 7.16. Claim 9.1 shows that for any $r\in\mathfrak{L}_0$ and $\boldsymbol{N}\sim\mathscr{N}(0,\mathscr{C})$

$$\mathbb{P}_{\mathfrak{A}}\left(\hat{\rho}_{\boldsymbol{\sigma}}\in\mathfrak{L}_0(r,\varepsilon)\right)=\mathbb{P}_{\mathfrak{A}}\left(\left\|\boldsymbol{N}-\frac{r-\boldsymbol{\Delta}\mathbb{1}/q}{s_n}\right\|_\infty<\varepsilon\right)+o(1).$$

Moreover, Corollary 9.4 implies that given $\hat{\rho}_{\boldsymbol{\sigma}}\in\mathfrak{L}_0(r,\varepsilon)$, $\hat{\rho}_{\boldsymbol{\sigma}}$ is within $o_\varepsilon(1)$ of the uniform distribution on $\mathfrak{L}_0(r,\varepsilon)$. Furthermore, Lemma 3.6 shows that the number of points in $\mathfrak{L}_0(r,\varepsilon)$ satisfies

$$\frac{|\mathfrak{L}_0(r,\varepsilon)|}{\left|\left\{z\in\mathbb{Z}^{q-1}:\|z-r\|_\infty\leq\varepsilon s_n\right\}\right|}\sim\mathfrak{d}^{1-q}.$$

Finally, the eigenvalues of the matrix $\mathscr{C}$ are q^{-2} (once) and q^{-1} ($(q-2)$ times). Hence, $\det\mathscr{C}=q^{-q}$. Therefore, w.h.p. for all $r\in\mathfrak{L}_0$ we have

$$\mathbb{P}_{\mathfrak{A}}\left[\hat{\rho}_{\boldsymbol{\sigma}}=r\right]=(1+o_\varepsilon(1))\frac{q^{q/2}\mathfrak{d}^{q-1}}{(2\pi\sum_{i=1}^n\boldsymbol{d}_i^2)^{(q-1)/2}}\exp\left[-\frac{(r-q^{-1}\boldsymbol{\Delta}\mathbb{1})^T\mathscr{C}^{-1}(r-q^{-1}\boldsymbol{\Delta}\mathbb{1})}{2\sum_{i=1}^n\boldsymbol{d}_i^2}\right]. \qquad (9.23)$$

Finally, since $\mathbb{E}\left[\boldsymbol{d}^2\right]<\infty$, $\sum_{i=1}\boldsymbol{d}_i^2\sim n\mathbb{E}\left[\boldsymbol{d}^2\right]$ and the claim follows. □

AMIN COJA-OGHLAN, amin.coja-oghlan@tu-dortmund.de, TU DORTMUND, FACULTY OF COMPUTER SCIENCE, 12 OTTO-HAHN-ST, DORTMUND 44227, GERMANY.

PU GAO, p3gao@uwaterloo.ca, DEPARTMENT OF COMBINATORICS AND OPTIMIZATION, UNIVERSITY OF WATERLOO, CANADA.

MAX HAHN-KLIMROTH, maximilian.hahnklimroth@tu-dortmund.de , TU DORTMUND, FACULTY OF COMPUTER SCIENCE, 12 OTTO-HAHN-ST, DORTMUND 44227, GERMANY.

JOON LEE, joon.lee@tu-dortmund.de, TU DORTMUND, FACULTY OF COMPUTER SCIENCE, 12 OTTO-HAHN-ST, DORTMUND 44227, GERMANY.

NOELA MÜLLER, n.s.muller@tue.nl, EINDHOVEN UNIVERSITY OF TECHNOLOGY, DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, METAFORUM MF 4.084, 5600 MB EINDHOVEN, THE NETHERLANDS.

MAURICE ROLVIEN, maurice.rolvien@tu-dortmund.de, TU DORTMUND, FACULTY OF COMPUTER SCIENCE, 12 OTTO-HAHN-ST, DORTMUND 44227, GERMANY.

Bibliography

[1] Dimitris Achlioptas. Lower bounds for random 3-sat via differential equations. *Theoretical Computer Science*, 265(1-2):159–185, 2001.

[2] Dimitris Achlioptas, Amin Coja-Oghlan, Max Hahn-Klimroth, Joon Lee, Noela Müller, Manuel Penschuck, and Guangyan Zhou. The random 2-sat partition function. *arXiv preprint arXiv:2002.03690*, 2020.

[3] Dimitris Achlioptas, Amin Coja-Oghlan, Max Hahn-Klimroth, Joon Lee, Noëla Müller, Manuel Penschuck, and Guangyan Zhou. The number of satisfying assignments of random 2-sat formulas. *Random Structures & Algorithms*, 58(4):609–647, 2021.

[4] Dimitris Achlioptas and Frank McSherry. Fast computation of low-rank matrix approximations. *Journal of the ACM (JACM)*, 54(2):9–es, 2007.

[5] Dimitris Achlioptas and Michael Molloy. The solution space geometry of random linear equations. *Random Structures & Algorithms*, 46(2):197–231, 2015.

[6] Dimitris Achlioptas and Cristopher Moore. Random k-sat: Two moments suffice to cross a sharp threshold. *SIAM Journal on Computing*, 36(3):740–762, 2006.

[7] Dimitris Achlioptas, Assaf Naor, and Yuval Peres. Rigorous location of phase transitions in hard optimization problems. *Nature*, 435(7043):759–764, 2005.

[8] Michael Aizenman, Robert Sims, and Shannon L Starr. Extended variational principle for the sherrington-kirkpatrick spin-glass model. *Physical Review B*, 68(21):214403, 2003.

[9] Noga Alon and Joel H Spencer. *The probabilistic method*. John Wiley & Sons, 2016.

[10] Montanari Andrea. Estimating random variables from random sparse observations. *European Transactions on Telecommunications*, 19(4):385–403, 2008.

[11] Peter Ayre, Amin Coja-Oghlan, Pu Gao, and Noëla Müller. The satisfiability threshold for random linear equations. *Combinatorica*, 40(2):179–235, 2020.

[12] Antar Bandyopadhyay and David Gamarnik. Counting without sampling: Asymptotics of the log-partition function for certain statistical physics models. *Random Structures & Algorithms*, 33(4):452–479, 2008.

[13] Jean Barbier and Dmitry Panchenko. Strong replica symmetry in high-dimensional optimal bayesian inference. *Communications in Mathematical Physics*, pages 1–41, 2022.

[14] Alexander Barvinok. *Combinatorics and complexity of partition functions*, volume 9. Springer, 2016.

[15] Mohsen Bayati, Devavrat Shah, and Mayank Sharma. Maximum weight matching via max-product belief propagation. In *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005.*, pages 1763–1767. IEEE, 2005.

[16] Hans A Bethe. Statistical theory of superlattices. *Proceedings of the Royal Society of London. Series A-Mathematical and Physical Sciences*, 150(871):552–575, 1935.

[17] Christopher M Bishop. Pattern recognition and machine learning-springer 2006. *Reference Source*, 2006.

[18] Béla Bollobás. A probabilistic proof of an asymptotic formula for the number of labelled regular graphs. *European Journal of Combinatorics*, 1(4):311–316, 1980.

[19] Béla Bollobás. The evolution of sparse graphs, graph theory and combinatorics (cambridge, 1983), 1984.

[20] Béla Bollobás, Christian Borgs, Jennifer T Chayes, Jeong Han Kim, and David B Wilson. The scaling window of the 2-sat transition. *Random Structures & Algorithms*, 18(3):201–256, 2001.

[21] Charles Bordenave, Marc Lelarge, and Justin Salez. Matchings on infinite graphs. *Probability Theory and Related Fields*, 157(1):183–208, 2013.

[22] Joe P Buhler and Peter Stevenhagen. *Algorithmic number theory*. Cambridge University Press Cambridge, 2008.

[23] Peter C Cheeseman, Bob Kanefsky, William M Taylor, et al. Where the really hard problems are. In *Ijcai*, volume 91, pages 331–337, 1991.

[24] Amin Coja-Oghlan, Oliver Cooley, Mihyun Kang, Joon Lee, and Jean Bernoulli Ravelomanana. The sparse parity matrix. In *Proceedings of the 2022 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 822–833. SIAM, 2022.

[25] Amin Coja-Oghlan, Oliver Cooley, Mihyun Kang, and Kathrin Skubch. Core forging and local limit theorems for the k-core of random graphs. *Journal of Combinatorial Theory, Series B*, 137:178–231, 2019.

[26] Amin Coja-Oghlan, Alperen A Ergür, Pu Gao, Samuel Hetterich, and Maurice Rolvien. The rank of sparse random matrices. In *Proceedings of the Fourteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 579–591. SIAM, 2020.

[27] Amin Coja-Oghlan, Pu Gao, Max Hahn-Klimroth, Joon Lee, Noela Müller, and Maurice Rolvien. The full rank condition for sparse random matrices. *arXiv preprint arXiv:2112.14090*, 2021.

[28] Amin Coja-Oghlan, Florent Krzakala, Will Perkins, and Lenka Zdeborová. Information-theoretic thresholds from the cavity method. *Advances in Mathematics*, 333:694–795, 2018.

[29] Amin Coja-Oghlan, Noëla Müller, and Jean B Ravelomanana. Belief propagation on the random k-sat model. *arXiv preprint arXiv:2011.02303*, 2020.

[30] Amin Coja-Oghlan and Konstantinos Panagiotou. The asymptotic k-sat threshold. *Advances in Mathematics*, 288:985–1068, 2016.

[31] Amin Coja-Oghlan and Will Perkins. Belief propagation on replica symmetric random factor graph models. *Annales de l'institut Henri Poincare D*, 5(2):211–249, 2018.

[32] Oliver Cooley, Joon Lee, and Jean B Ravelomanana. Warning propagation: stability and subcriticality. *arXiv preprint arXiv:2111.15577*, 2021.

[33] Colin Cooper, Alan Frieze, and Gregory B Sorkin. Random 2-sat with prescribed literal degrees. *Algorithmica*, 48(3):249–265, 2007.

[34] Don Coppersmith, David Gamarnik, MohammadTaghi Hajiaghayi, and Gregory B Sorkin. Random max sat, random max cut, and their phase transitions. *Random Structures & Algorithms*, 24(4):502–545, 2004.

[35] Burgess Davis and David McDonald. An elementary proof of the local central limit theorem. *Journal of Theoretical Probability*, 8(3):693–702, 1995.

[36] Martin Dietzfelbinger, Andreas Goerdt, Michael Mitzenmacher, Andrea Montanari, Rasmus Pagh, and Michael Rink. Tight thresholds for cuckoo hashing via xorsat. In *International Colloquium on Automata, Languages, and Programming*, pages 213–225. Springer, 2010.

[37] Jian Ding, Allan Sly, and Nike Sun. Proof of the satisfiability conjecture for large k. In *Proceedings of the forty-seventh annual ACM symposium on Theory of computing*, pages 59–68, 2015.

[38] Olivier Dubois and Jacques Mandler. The 3-xorsat threshold. *Comptes Rendus Mathematique*, 335(11):963–966, 2002.

[39] Samuel Frederick Edwards and Phil W Anderson. Theory of spin glasses. *Journal of Physics F: Metal Physics*, 5(5):965, 1975.

[40] P ErdHos. Rényi, a.:" on random graphs. *I". Publicationes Mathematicae (Debre*, 1959.

[41] Paul ErdHos and Alfréd Rényi. On the strength of connectedness of a random graph. *Acta Mathematica Hungarica*, 12(1):261–267, 1961.

[42] Paul ErdHos, Alfréd Rényi, et al. On the evolution of random graphs. *Publ. Math. Inst. Hung. Acad. Sci*, 5(1):17–60, 1960.

[43] John Franco and Marvin Paull. Probabilistic analysis of the davis putnam procedure for solving the satisfiability problem. *Discrete Applied Mathematics*, 5(1):77–87, 1983.

[44] Silvio Franz and Michele Leone. Replica bounds for optimization problems and diluted spin systems. *Journal of Statistical Physics*, 111(3):535–564, 2003.

[45] Alan Frieze and Stephen Suen. Analysis of two simple heuristics on a random instance ofk-sat. *Journal of Algorithms*, 20(2):312–355, 1996.

[46] Andreas Goerdt. A threshold for unsatisfiability. *Journal of Computer and System Sciences*, 53(3):469–486, 1996.

[47] Francesco Guerra. Broken replica symmetry bounds in the mean field spin glass model. *Communications in mathematical physics*, 233(1):1–12, 2003.

[48] Jiaoyang Huang. Invertibility of adjacency matrices for random d-regular graphs. *Duke Mathematical Journal*, 170(18):3977–4032, 2021.

[49] Morteza Ibrahimi, Yashodhan Kanoria, Matt Kraning, and Andrea Montanari. The set of solutions of random xorsat formulae. In *Proceedings of the twenty-third annual ACM-SIAM symposium on Discrete Algorithms*, pages 760–779. SIAM, 2012.

[50] Svante Janson and Malwina J Luczak. A simple solution to the k-core problem. *Random Structures & Algorithms*, 30(1-2):50–62, 2007.

[51] Svante Janson and Malwina J Luczak. Asymptotic normality of the k-core in random graphs. *The annals of applied probability*, 18(3):1085–1137, 2008.

[52] Nathalie Japkowicz and Jerzy Stefanowski. *Big Data Analysis: New Algorithms for a New Society*, volume 16. Springer, 2016.

[53] Florent Krzakała, Andrea Montanari, Federico Ricci-Tersenghi, Guilhem Semerjian, and Lenka Zdeborová. Gibbs states and the set of solutions of random constraint satisfaction problems. *Proceedings of the National Academy of Sciences*, 104(25):10318–10323, 2007.

[54] Frank R Kschischang, Brendan J Frey, and H-A Loeliger. Factor graphs and the sum-product algorithm. *IEEE Transactions on information theory*, 47(2):498–519, 2001.

[55] Marc Lelarge. Bypassing correlation decay for matchings with an application to xorsat. In *2013 IEEE Information Theory Workshop (ITW)*, pages 1–5. IEEE, 2013.

[56] Tomasz Luczak. Component behavior near the critical point of the random graph process. *Random Structures & Algorithms*, 1(3):287–310, 1990.

[57] Madan Lal Mehta. *Random matrices*. Elsevier, 2004.

[58] Stephan Mertens, Marc Mézard, and Riccardo Zecchina. Threshold values of random k-sat from the cavity method. *Random Structures & Algorithms*, 28(3):340–373, 2006.

[59] Marc Mézard. Spin glasses and optimization in complex systems. *Europhysics News*, 53(1):15–17, 2022.

[60] Marc Mezard and Andrea Montanari. *Information, physics, and computation*. Oxford University Press, 2009.

[61] Marc Mézard, Giorgio Parisi, and Miguel Angel Virasoro. *Spin glass theory and beyond: An Introduction to the Replica Method and Its Applications*, volume 9. World Scientific Publishing Company, 1987.

[62] Marc Mézard, Giorgio Parisi, and Riccardo Zecchina. Analytic and algorithmic solution of random satisfiability problems. *Science*, 297(5582):812–815, 2002.

[63] David Mitchell, Bart Selman, Hector Levesque, et al. Hard and easy distributions of sat problems. In *Aaai*, volume 92, pages 459–465. Citeseer, 1992.

[64] Michael Molloy. Cores in random hypergraphs and boolean formulas. *Random Structures & Algorithms*, 27(1):124–135, 2005.

[65] Michael Molloy and Bruce Reed. A critical point for random graphs with a given degree sequence. *Random structures & algorithms*, 6(2-3):161–180, 1995.

[66] Remi Monasson and Riccardo Zecchina. Entropy of the k-satisfiability problem. *Physical review letters*, 76(21):3881, 1996.

[67] Andrea Montanari, Giorgio Parisi, and Federico Ricci-Tersenghi. Instability of one-step replica-symmetry-broken phase in satisfiability problems. *Journal of Physics A: Mathematical and General*, 37(6):2073, 2004.

[68] Andrea Montanari and Devavrat Shah. Counting good truth assignments of random k-sat formulae. *arXiv preprint cs/0607073*, 2006.

[69] Hidetoshi Nishimori. *Statistical physics of spin glasses and information processing: an introduction*. Number 111. Clarendon Press, 2001.

[70] Dmitry Panchenko. On the replica symmetric solution of the k-sat model. *Electronic Journal of Probability*, 19:1–17, 2014.

[71] Dmitry Panchenko and Michel Talagrand. Bounds for diluted mean-fields spin glass models. *Probability Theory and Related Fields*, 130(3):319–336, 2004.

[72] Boris Pittel and Gregory B Sorkin. The satisfiability threshold for k-xorsat. *Combinatorics, Probability and Computing*, 25(2):236–268, 2016.

[73] Boris Pittel, Joel Spencer, and Nicholas Wormald. Sudden emergence of a giantk-core in a random graph. *Journal of Combinatorial Theory, Series B*, 67(1):111–151, 1996.

[74] Prasad Raghavendra and Ning Tan. Approximating csps with global cardinality constraints using sdp hierarchies. In *Proceedings of the twenty-third annual ACM-SIAM symposium on Discrete Algorithms*, pages 373–387. SIAM, 2012.

[75] B Reed. Mick gets some (the odds are on his side). In *Proceedings of the 32nd IEEE Symposium on Foundationsof Computer Science*, pages 620–626.

[76] Tom Richardson and Ruediger Urbanke. *Modern coding theory*. Cambridge university press, 2008.

[77] Oliver Riordan. The k-core and branching processes. *Combinatorics, Probability and Computing*, 17(1):111–136, 2008.

[78] Michel Talagrand. The parisi formula. *Annals of mathematics*, pages 221–263, 2006.

[79] Michel Talagrand et al. *Spin glasses: a challenge for mathematicians: cavity and mean field models*, volume 46. Springer Science & Business Media, 2003.

[80] Terence Tao. What's new: 275a, notes 5. variants of the central limit theorem, 2015.

[81] Leslie G Valiant. The complexity of enumeration and reliability problems. *SIAM Journal on Computing*, 8(3):410–421, 1979.

[82] L Viana and Allan J Bray. Phase diagrams for dilute spin glasses. *Journal of Physics C: Solid State Physics*, 18(15):3037, 1985.

[83] Van H Vu. Combinatorial problems in random matrix theory. In *Proceedings ICM*, volume 4, pages 489–508, 2014.

[84] Van H Vu. Recent progress in combinatorial random matrix theory. *Probability Surveys*, 18:179–200, 2021.

[85] Martin J Wainwright, Elitza Maneva, and Emin Martinian. Lossy source compression using low-density generator matrix codes: Analysis and algorithms. *IEEE Transactions on Information theory*, 56(3):1351–1368, 2010.

[86] Nicholas C Wormald. Differential equations for random processes and random graphs. *The annals of applied probability*, pages 1217–1235, 1995.

[87] Nicholas C Wormald et al. Models of random regular graphs. *London Mathematical Society Lecture Note Series*, pages 239–298, 1999.

[88] Jonathan S Yedidia, William T Freeman, Yair Weiss, et al. Understanding belief propagation and its generalizations. *Exploring artificial intelligence in the new millennium*, 8(236-239):0018–9448, 2003.

[89] Jonathan S Yedidia, William T Freeman, Yair Weiss, et al. Understanding belief propagation and its generalizations. *Exploring artificial intelligence in the new millennium*, 8(236-239):0018–9448, 2003.

[90] Lenka Zdeborová and Florent Krzakala. Statistical physics of inference: Thresholds and algorithms. *Advances in Physics*, 65(5):453–552, 2016.