On the Hardness of Approximating Shortest Integer Relations among Rational Numbers

Carsten Rőssner
Dept. of Math. Comp. Science
University of Frankfurt
P. O. Box 11 19 32
60054 Frankfurt on the Main
Germany
roessner@cs.uni-frankfurt.de

*Jean-Pierre Seifert**
Dept. of Math. Comp. Science
University of Frankfurt
P. O. Box 11 19 32
60054 Frankfurt on the Main
Germany
seifert@cs.uni-frankfurt.de

Abstract

Given $\mathbf{x} \in \mathbb{R}^n$ an integer relation for $\mathbf{x}$ is a non-trivial vector $\mathbf{m} \in \mathbb{Z}^n$ with inner product $\langle \mathbf{m}, \mathbf{x} \rangle = 0$.

In this paper we prove the following: Unless every **NP** *language is recognizable in deterministic quasi-polynomial time, i.e., in time $O(n^{\mathrm{poly}(\log n)})$, the ℓ_∞-shortest integer relation for a given vector $\mathbf{x} \in \mathbb{Q}^n$ cannot be approximated in polynomial time within a factor of $2^{\log^{0.5-\gamma} n}$, where γ is an arbitrarily small positive constant.*

This result is quasi-complementary to positive results derived from lattice basis reduction. A variant of the well-known L^3-algorithm approximates for a vector $\mathbf{x} \in \mathbb{Q}^n$ the ℓ_2-shortest integer relation within a factor of $2^{n/2}$ in polynomial time.

Our proof relies on recent advances in the theory of probabilistically checkable proofs, in particular on a reduction from 2-prover 1-round interactive proof-systems.

The same inapproximability result is valid for finding the ℓ_∞-shortest integer solution for a homogeneous linear system of equations over $\mathbb{Q}$.

Keywords Approximation algorithm, computational complexity, integer relations, label cover, **NP**-hard, probabilistically checkable proofs, 2-prover 1-round interactive proof systems.

1 Introduction

Given $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$ an integer relation for $\mathbf{x}$ is a non-trivial vector $\mathbf{m} = (m_1, \ldots, m_n) \in \mathbb{Z}^n$ satisfying $\langle \mathbf{m}, \mathbf{x} \rangle = 0$, where $\langle \cdot, \cdot \rangle$ denotes the Euclidean inner product $\langle \mathbf{m}, \mathbf{x} \rangle := \sum_{i=1}^n m_i x_i$. We investigate into the following minimization problems:

*Supported by DFG under grant DFG Leibniz Programm Schn 143/5-1

Proceedings of CATS'96 (Computing: The Australasian Theory Symposium), Melbourne, Australia, January 29–January 30 1996.

SHORTEST INTEGER RELATION in ℓ_∞-norm (SIR_∞)
INSTANCE: A rational vector $\mathbf{x} \in \mathbb{Q}^n$
SOLUTION: A non-zero vector $\mathbf{m} \in \mathbb{Z}^n$ such that $\langle \mathbf{m}, \mathbf{x} \rangle = 0$
MEASURE: The ℓ_∞-norm $\|\mathbf{m}\|_\infty := \max_{1 \le i \le n} |m_i|$ of the vector $\mathbf{m}$

SHORTEST SIMULTANEOUS INTEGER RELATION in ℓ_∞-norm (SSIR_∞)
INSTANCE: r rational non-zero vectors $\mathbf{y}_1, \ldots, \mathbf{y}_r \in \mathbb{Q}^n$
SOLUTION: A simultaneous integer relation $\mathbf{m} \in \mathbb{Z}^n$ for $\mathbf{y}_1, \ldots, \mathbf{y}_r$, i.e., a non-zero vector $\mathbf{m} \in \mathbb{Z}^n$ such that $\langle \mathbf{m}, \mathbf{y}_j \rangle = 0$, $j = 1, \ldots, r$
MEASURE: The ℓ_∞-norm $\|\mathbf{m}\|_\infty := \max_{1 \le i \le n} |m_i|$ of the vector $\mathbf{m}$

The problem of finding short and shortest integer relations is rather important because it can be applied to compute minimal polynomials of an algebraic number, (simultaneous) diophantine approximations and integer dependencies among real vectors (see [12, 13, 10]).

Obviously, for a non-zero vector $\mathbf{x} \in \mathbb{Q}^n$ there are $n - 1$ linearly independent integer relations. However, van Emde Boas [16] has shown that the decision variant of SIR_∞ is **NP**-complete. For arbitrary real non-zero $\mathbf{x} \in \mathbb{R}^n$ it cannot even be decided in a very general model of computation whether there exists an integer relation at all (see Babai, Just and Meyer auf der Heide [7]).

On the other hand, Håstad, Just, Lagarias and Schnorr [10] proposed a polynomial time algorithm which approximates for input $\mathbf{x} \in \mathbb{Q}^n$ the shortest integer relation in the Euclidean norm $\langle \cdot, \cdot \rangle^{1/2}$ within a factor $2^{n/2}$. An algorithm is said to *approximate* a positive real-valued function $opt(\cdot)$ *within a factor* f if on every input I, the value of its output is within a factor f of $opt(I)$. Thus, by the result of [10] SIR_∞ can be approximated in polynomial time within a factor $\sqrt{n}2^{n/2}$.

The problem of finding the shortest integer relation in any ℓ_p-norm clearly contains the SHORTEST

VECTOR problem SV_p for integral lattices in the same ℓ_p-norm, i.e., the problem of finding for an integral basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ of an additive subgroup of the $\mathbb{Z}^n$, the ℓ_p-shortest non-zero linear integral combination of $\mathbf{b}_1, \ldots, \mathbf{b}_n$; its decision variant is known to be **NP**-complete for $p = \infty$ (see [16]).

On the other hand, Arora, Babai, Stern and Sweedyk [4] have shown that under the widely believed assumption $\mathbf{NP} \not\subseteq \mathbf{QP}$ there exists no polynomial time algorithm approximating the SHORTEST VECTOR problem in the ℓ_∞-norm within a factor of $2^{\log^{0.5-\gamma} n}$, where γ is an arbitrarily small positive constant. **QP** denotes the set of all languages which are recognizable in time $O(n^{\mathrm{poly}(\log n)})$, where n is the length of the input.

In our reduction we adapt the proof in [4] to derive the same inapproximability result for the SSIR_∞ problem. For the reduction we will use an equivalent optimization problem, stated as follows.

MIN $\mathbb{Z}$-SOLUTION OF HOMOGENEOUS LINEAR SYSTEM in ℓ_∞-norm (MIN HLS_∞)
INSTANCE: A homogeneous linear system $\boldsymbol{A}\mathbf{x} = \mathbf{0}$ of r equations in n variables, where $\boldsymbol{A}$ is a rational $r \times n$ matrix and $\mathbf{0}$ the all-zero vector in $\mathbb{R}^n$
SOLUTION: A non-zero vector $\mathbf{x} \in \mathbb{Z}^n$ satisfying $\boldsymbol{A}\mathbf{x} = \mathbf{0}$
MEASURE: The ℓ_∞-norm $\|\mathbf{x}\|_\infty := \max_{1 \le i \le n} |x_i|$ of the vector $\mathbf{x}$

The inapproximability result established here adds to the recently derived results on optimization problems arising from linear systems of equations (see [2, 1]).

From the problem MIN $\mathbb{Z}$-SOLUTION OF HOMOGENEOUS LINEAR SYSTEM in ℓ_∞-norm we give a gap-preserving reduction to the problem SHORTEST INTEGER RELATION in ℓ_∞-norm which implies the claimed inapproximability result.

2 Preliminaries

We briefly introduce some notation (see [6]):

Definition 1 An *optimization problem* Π is a set $\mathcal{I} \subseteq \{0,1\}^*$ of instances, a set $\mathcal{S} \subseteq \{0,1\}^*$ of feasible solutions on input $I \in \mathcal{I}$, and a polynomial time computable measure $m : \mathcal{I} \times \mathcal{S} \to \mathbb{R}_+$, that assigns each tuple of instance I and solution S, a positive real number $m(I,S)$, called the *value* of the solution S. The optimization problem is to find, for a given input $I \in \mathcal{I}$ a solution $S \in \mathcal{S}$ such that $m(I,S)$ is optimum over all possible $S \in \mathcal{S}$.

If the optimum is $\min_{S \in \mathcal{S}}\{m(I,S)\}$ (resp. $\max_{S \in \mathcal{S}}\{m(I,S)\}$) we refer to Π as a *minimization* (resp. *maximization*) problem.

Definition 2 For an input I of a minimization problem Π whose optimal solution has value $opt(I)$, an algorithm A is said to *approximate* $opt(I)$ *within a factor* $f(I)$ iff

$$opt(I) \le A(I) \le opt(I) f(I),$$

where $f(I) \ge 1$ and $A(I) > 0$.

For exhibiting the hardness of approximation problems we introduce the following reduction due to Arora [3].

Definition 3 Let Π and Π' be two minimization problems and $\rho, \rho' \ge 1$. A *gap-preserving reduction from* Π *to* Π' *with parameters* $((c,\rho),(c',\rho'))$ is a polynomial time transformation τ mapping every instance I of Π to an instance $I' = \tau(I)$ of Π' such that for the optima $opt_\Pi(I)$ and $opt_{\Pi'}(I')$ of I and I', respectively, the following holds:

$$\begin{aligned} opt_\Pi(I) \le c &\implies opt_{\Pi'}(I') \le c' \\ opt_\Pi(I) \ge c \cdot \rho &\implies opt_{\Pi'}(I') \ge c' \cdot \rho', \end{aligned}$$

where c, ρ and c', ρ' depend on the instance sizes $|I|$ and $|I'|$, respectively.

3 MIN PSEUDO LABEL COVER

In the following $G = (V_1, V_2, E)$ denotes a bipartite graph, $\mathcal{B}$ a set of labels for the vertices in $V_1 \cup V_2$, and for $e \in E$ there exists a partial function $\Pi_e : \mathcal{B} \to \mathcal{B}$ describing the admissible pairs of labels. Moreover, we assume that G is regular, i.e., every node of G is incident to the same number of edges. This property of G is a result of the reduction in [4] from 3-SAT to MIN PSEUDO LABEL COVER sketched below. We adapt the notation of [4].

Definition 4 A *labelling* of $G = (V_1, V_2, E)$ is a pair $(\mathcal{P}_1, \mathcal{P}_2)$ of functions $\mathcal{P}_i : V_i \to 2^{\mathcal{B}}$, $i = 1, 2$, assigning each vertex in $V_1 \cup V_2$ a possibly empty set of labels.

Definition 5 Let $(\mathcal{P}_1, \mathcal{P}_2)$ be a labelling of $G = (V_1, V_2, E)$ and $e = (v_1, v_2)$, $v_1 \in V_1$, $v_2 \in V_2$, an edge of G. We call $e = (v_1, v_2)$

untouched iff $\mathcal{P}_1(v_1) = \mathcal{P}_2(v_2) = \emptyset$,

covered iff $\mathcal{P}_1(v_1) \ne \emptyset$, $\mathcal{P}_2(v_2) \ne \emptyset$ and for all labels $b_2 \in \mathcal{P}_2(v_2)$ there exists a label $b_1 \in \mathcal{P}_1(v_1)$ such that $\Pi_e(b_1) = b_2$ or

cancelled iff $\mathcal{P}_2(v_2) = \emptyset$, $\mathcal{P}_1(v_1) \ne \emptyset$ and for every label $b_1 \in \mathcal{P}_1(v_1)$ there exists a label $b_1' \in \mathcal{P}_1(v_1)$ such that for some label $b_2 \in \mathcal{B}$ we have $\Pi_e(b_1) = b_2$ and $\Pi_e(b_1') = b_2$.

A labelling $(\mathcal{P}_1, \mathcal{P}_2)$ of $G = (V_1, V_2, E)$ is called a *pseudo-cover* of G iff

(i) $\bigcup_{v_1 \in V_1, v_2 \in V_2} \mathcal{P}_1(v_1) \cup \mathcal{P}_2(v_2) \ne \emptyset$ and

(ii) every edge of G is either untouched, covered or cancelled by the labelling $(\mathcal{P}_1, \mathcal{P}_2)$.

Definition 6 The ℓ_∞-*cost* of a labelling $(\mathcal{P}_1, \mathcal{P}_2)$ for a graph $G = (V_1, V_2, E)$ is defined as

$$cost(\mathcal{P}_1, \mathcal{P}_2) \quad = \quad \max_{v_1 \in V_1} |\mathcal{P}_1(v_1)|.$$

Definition 7 MIN PSEUDO LABEL COVER (MIN PSL_∞)
INSTANCE: A regular bipartite graph $G = (V_1, V_2, E)$, a set of labels $\mathcal{B} = \{1, \ldots, \mathcal{N}\}, \mathcal{N} \in \mathbb{N}_+$, and for every edge $e \in E$ a partial function $\Pi_e : \mathcal{B} \to \mathcal{B}$ such that $\Pi_e^{-1}(1) \neq \emptyset$ for the distinguished label $1 \in \mathcal{B}$
SOLUTION: A pseudo-cover $(\mathcal{P}_1, \mathcal{P}_2)$ of G
MEASURE: The ℓ_∞-cost $cost(\mathcal{P}_1, \mathcal{P}_2)$ of the pseudo-cover $(\mathcal{P}_1, \mathcal{P}_2)$

Remark In the above definition we can always ensure the existence of a pseudo-cover with ℓ_∞-cost at most $\mathcal{N}$; we simply let $\mathcal{P}_2(v_2) = \{1\}$ for all $v_2 \in V_2$ and $\mathcal{P}_1(v_1) = \mathcal{B}$ for all $v_1 \in V_1$.

Lemma 1 ([4]) *There exists a quasi-polynomial time, i.e., $O(n^{\text{poly}(\log n)})$ transformation τ from* 3-SAT *to* MIN PSEUDO LABEL COVER *such that, for all instances I,*

$$\begin{aligned} I \in \text{3-SAT} \quad &\Longrightarrow \quad \exists \text{ pseudo-cover } (\mathcal{P}_1, \mathcal{P}_2) \text{ of } \tau(I) : \\ &\qquad cost(\mathcal{P}_1, \mathcal{P}_2) = 1 \\ I \notin \text{3-SAT} \quad &\Longrightarrow \quad \forall \text{ pseudo-cover } (\mathcal{P}_1, \mathcal{P}_2) \text{ of } \tau(I) : \\ &\qquad cost(\mathcal{P}_1, \mathcal{P}_2) \geq 2^{\log^{0.5-\gamma} N}, \end{aligned}$$

where γ is an arbitrarily small positive constant and N is the size of $\tau(I)$.

Remark In their proof Arora et al. [4] use results of [9, 5] stating that every language in **NP** (particularly 3-SAT) has a 2-prover 1-round interactive proof-system. Roughly speaking, a 2-prover 1-round interactive proof-system consists in one probabilistic polynomial time verifier communicating with two computationally unbounded provers who are not allowed to communicate with each other. The provers want to convince the verifier that a given input x belongs to a prespecified language L. The key idea of the reduction presented in [4] is the translation of the provers' strategy causing the verifier to accept into an instance of MIN PSEUDO LABEL COVER using the specific properties of the 2-prover 1-round interactive proof-system of [9]. Hereby a large gap between the acceptance probability in the case that $I \in$ 3-SAT versus the case $I \notin$ 3-SAT translates into a large gap between the ℓ_∞-cost of the corresponding MIN PSEUDO LABEL COVER instance in both cases.

4 MIN $\mathbb{Z}$-SOLUTION OF HOMOGENEOUS LINEAR SYSTEM

Theorem 2 *There exists a polynomial time transformation τ from* MIN PSEUDO LABEL COVER *to* MIN $\mathbb{Z}$-SOLUTION OF HOMOGENEOUS LINEAR SYSTEM *such that, for all instances I and for all $\rho \geq 1$,*

$$\begin{aligned} opt_{\text{MinPSL}_\infty}(I) = 1 \quad &\Longrightarrow \quad opt_{\text{MinHLS}_\infty}(\tau(I)) = 1 \\ opt_{\text{MinPSL}_\infty}(I) \geq \rho \quad &\Longrightarrow \quad opt_{\text{MinHLS}_\infty}(\tau(I)) \geq \sqrt{\rho}. \end{aligned}$$

Proof. From a given MIN PSEUDO LABEL COVER instance $I = (V_1, V_2, E, \Pi, \mathcal{B}, \mathcal{N})$ we construct a homogeneous linear system of equations $\boldsymbol{A}\mathbf{x} = \mathbf{0}$ with $\boldsymbol{A}$ an $r \times n$ matrix of entries $\{-1, 0, 1\}$, $r = |V_1|\mathcal{N} + |E|(\mathcal{N}+1)$ and $n = 2|V_1|\mathcal{N} + |V_2|\mathcal{N} + 1$.

For every pair (v, b) with $v \in V_1 \cup V_2$ and $b \in \mathcal{B}$ we define a column vector $\mathbf{a}_{v,b} \in \{-1, 0, 1\}^r$ of $\boldsymbol{A}$ as follows. The first $|E|(\mathcal{N}+1)$ coordinates of $\mathbf{a}_{v,b}$ are split into $|E|$ blocks of *e-projections* $\mathbf{u}_e(\mathbf{a}_{v,b})$ — one $(\mathcal{N}+1)$-length block for every edge $e \in E$. In particular, we define for every $(v_2, b_2) \in V_2 \times \mathcal{B}$

$$\mathbf{u}_e(\mathbf{a}_{v_2,b_2}) \quad := \quad \begin{cases} \mathbf{e}_{b_2} & \text{iff } e \text{ is incident to } v_2 \\ \mathbf{0} & \text{otherwise} \end{cases}$$

and for every $(v_1, b_1) \in V_1 \times \mathcal{B}$

$$\mathbf{u}_e(\mathbf{a}_{v_1,b_1}) \quad := \quad \begin{cases} \mathbf{1} - \mathbf{e}_{\Pi_e(b_1)} & \text{iff } e \text{ is incident to} \\ & v_1 \text{ and } \Pi_e(b_1) \neq \emptyset \\ \mathbf{0} & \text{otherwise} \end{cases}$$

where $\mathbf{e}_j$, $j = 1, \ldots, \mathcal{N}$, denotes the j^{th}-unit vector and $\mathbf{0}$, $\mathbf{1}$ the all-zero, all-one vector in $\mathbb{R}^{\mathcal{N}+1}$, respectively.

The definition of the remaining $|V_1|\mathcal{N}$ coordinates of $\mathbf{a}_{v,b}$ uses the properties of Hadamard matrices. A *Hadamard matrix of order ℓ*, denoted by $\boldsymbol{H}_\ell$, is an $\ell \times \ell$ matrix with ± 1 entries such that $\boldsymbol{H}_\ell \boldsymbol{H}_\ell^\top = \ell \boldsymbol{I}_\ell$. (Hadamard matrices can iteratively be constructed if ℓ is a power of 2, cf. [14]). The columns of $\frac{1}{\sqrt{\ell}}\boldsymbol{H}_\ell$ clearly form an orthonormal basis. Therefore $\|\frac{1}{\sqrt{\ell}}\boldsymbol{H}_\ell \mathbf{z}\|_2 = \|\mathbf{z}\|_2$ for every $\mathbf{z} \in \mathbb{Z}^\ell$. If $\mathbf{z} \in \mathbb{Z}^\ell$ has at least k non-zero entries we thus have $\|\boldsymbol{H}_\ell \mathbf{z}\|_\infty \geq \sqrt{k}$.

We may assume that for $\ell = \mathcal{N}$ there exists a Hadamard matrix $\boldsymbol{H}_\ell = [\mathbf{h}_1, \ldots, \mathbf{h}_\ell]$ with column vectors $\mathbf{h}_b$ of $\boldsymbol{H}_\ell$, each of them uniquely identified with a label $b \in \mathcal{B}$. We now split the last $|V_1|\mathcal{N}$ coordinates of $\mathbf{a}_{v,b}$ into $|V_1|$ blocks of *v_1-projections* $\mathbf{u}_{v_1}(\mathbf{a}_{v,b})$ — one $\mathcal{N}$-length block for every vertex $v_1 \in V_1$ — where the v_1-projections for every $v \in V_1 \cup V_2$ and $b \in \mathcal{B}$ are defined as follows

$$\mathbf{u}_{v_1}(\mathbf{a}_{v,b}) \quad := \quad \begin{cases} \mathbf{h}_b & \text{iff } v = v_1 \\ \mathbf{0} & \text{otherwise} \end{cases}$$

and $\mathbf{0}$ denotes the all-zero vector in $\mathbb{R}^{\mathcal{N}}$. This definition clearly implies $\mathbf{u}_{v_1}(\mathbf{a}_{v,b}) = \mathbf{0}$ for all $v \in V_2$ and all $b \in \mathcal{B}$.

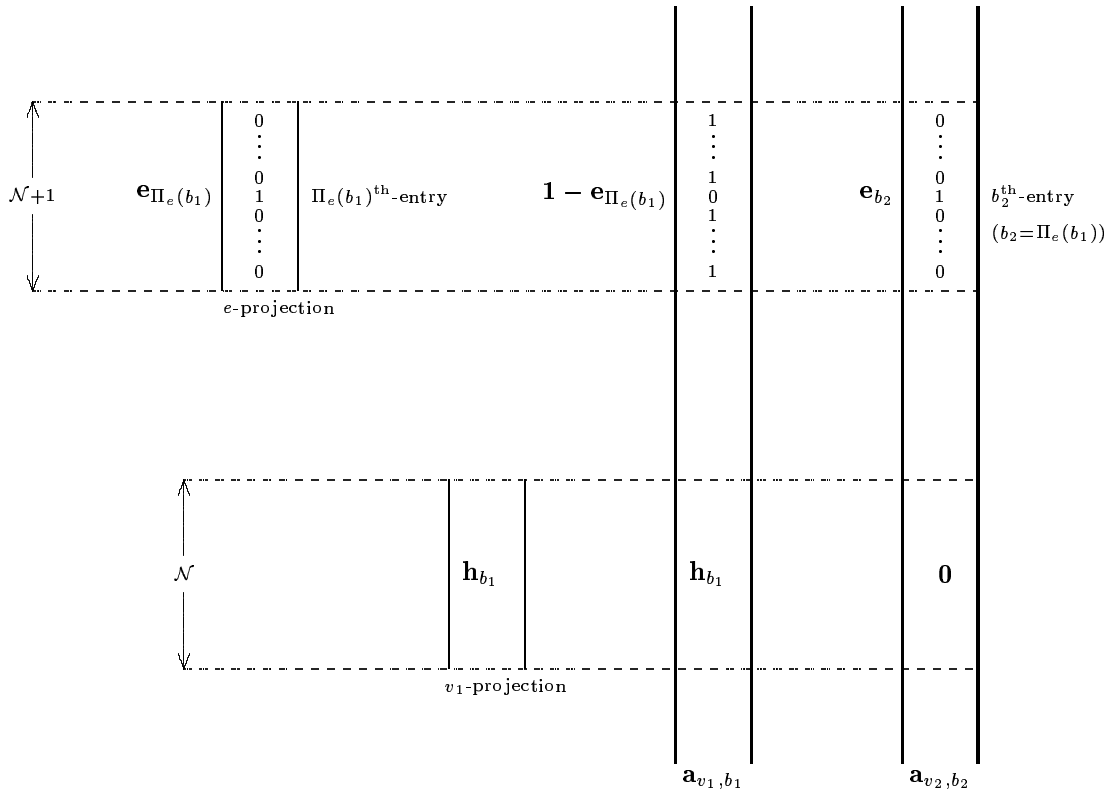

Figure 1: The resulting column vectors due to [4]

$$\begin{array}{l} \\ |E|(\mathcal{N}+1) \text{ rows} \\ |V_1|\mathcal{N} \text{ rows} \end{array} \begin{array}{c} \overset{|V_1|\mathcal{N} \text{ columns}}{\left[\mathbf{u}_e(\mathbf{a}_{v,b_1}),\ldots,\mathbf{u}_e(\mathbf{a}_{v,b_\mathcal{N}})\right]_{\substack{e\in E\\ v\in V_1}}} \\ \left[\mathbf{u}_{v_1}(\mathbf{a}_{v,b_1}),\ldots,\mathbf{u}_{v_1}(\mathbf{a}_{v,b_\mathcal{N}})\right]_{\substack{v_1\in V_1\\ v\in V_1}} \end{array} \begin{array}{c} \overset{|V_2|\mathcal{N} \text{ columns}}{\left[\mathbf{u}_e(\mathbf{a}_{v,b})\right]_{\substack{e\in E\\ (v,b)\in V_2\times\mathcal{B}}}} \\ \mathbf{0} \end{array} \begin{array}{c} \overset{1 \text{ column}}{\mathbf{1}} \\ \mathbf{0} \end{array} \begin{array}{c} \overset{|V_1|\mathcal{N} \text{ columns}}{\mathbf{0}} \\ \boldsymbol{I}_{|V_1|\mathcal{N}} \end{array}$$

Figure 2: The matrix $\boldsymbol{A}$
(owing lack of space we abbreviated $\left[\mathbf{u}_e(\mathbf{a}_{v,b_1}),\ldots,\mathbf{u}_e(\mathbf{a}_{v,b_\mathcal{N}})\right]_{\substack{e\in E\\ v\in V_2}} =: \left[\mathbf{u}_e(\mathbf{a}_{v,b})\right]_{\substack{e\in E\\ (v,b)\in V_2\times\mathcal{B}}}$)

Moreover, we define the $(|V_1|\mathcal{N}+|V_2|\mathcal{N}+1)^{\text{th}}$-column vector $\mathbf{a}_0$ as the vector having 1 in each of the first $|E|(\mathcal{N}+1)$ coordinates and 0 in the remaining ones.

The remaining $|V_1|\mathcal{N}$ column vectors are $\mathbf{e}_{|E|(\mathcal{N}+1)+i}$, $i=1,\ldots,|V_1|\mathcal{N}$ where $\mathbf{e}_j$ denotes the j^{th}-unit vector in $\mathbb{R}^{|V_1|\mathcal{N}+|E|(\mathcal{N}+1)}$.

The resulting matrix $\boldsymbol{A}$ is shown in the above Figure 2.

Given a vector $\mathbf{y}\in\mathbb{R}^{|V_1|\mathcal{N}+|E|(\mathcal{N}+1)}$, let $\mathbf{u}_E(\mathbf{y})$ denote the vector $\mathbf{y}$ *restricted to* its first $|E|(\mathcal{N}+1)$ coordinates. Let $\mathbf{x}=\sum x_{v,b}\mathbf{u}_E(\mathbf{a}_{v,b})$ be a non-trivial linear integral combination of the 'restricted' column vectors $\mathbf{u}_E(\mathbf{a}_{v,b})$. Then, assigning every vertex v a label b iff $x_{v,b}\neq 0$ defines a labelling $(\mathcal{P}_1^{\mathbf{x}},\mathcal{P}_2^{\mathbf{x}})$ *induced by the vector* $\mathbf{x}$. From [4, Corollary 10] it follows that any such $\mathbf{x}$ with $\mathbf{x}=\alpha\mathbf{u}_E(\mathbf{a}_0)$, $\alpha\in\mathbb{Z}$, induces a pseudo-cover of (V_1,V_2,E).

Thus, any non-trivial integral solution $\mathbf{x}$ of the homogeneous linear system $\boldsymbol{A}\mathbf{x}=\mathbf{0}$ induces by its first $|V_1|\mathcal{N}+|V_2|\mathcal{N}$ coordinates a pseudo-cover of (V_1,V_2,E) (note that the last $|V_1|\mathcal{N}$ column vectors of the matrix $\boldsymbol{A}$ have 0-entries in its first $|E|(\mathcal{N}+1)$ coordinates).

Thus, for the induced pseudo-cover $(\mathcal{P}_1^{\mathbf{x}},\mathcal{P}_2^{\mathbf{x}})$ there exists a vertex $v_1\in V_1$ with at least $opt_{\text{MinPSL}_\infty}(I)$ labels assigned. This in turn means that $\mathbf{x}$ has at least $opt_{\text{MinPSL}_\infty}(I)$ non-zero entries. By the above properties of the Hadamard matrices we see that there exists an index $i^*\in\{|E|(\mathcal{N}+1)+1,\ldots,|E|(\mathcal{N}+1)+|V_1|\mathcal{N}\}$ such that

$$\left|\sum_{j=1}^{|V_1|\mathcal{N}} a_{i^*,j}x_j\right| \geq \sqrt{opt_{\text{MinPSL}_\infty}(I)}.$$

As $\mathbf{x}$ is a solution of $\boldsymbol{A}\mathbf{x}=\mathbf{0}$ its remaining $|V_1|\mathcal{N}$ coordinates are forced to cancel out each of the

sums

$$\sum_{j=1}^{|V_1|\mathcal{N}} a_{i,j}x_j,$$

where $i = |E|(\mathcal{N}+1)+1,\ldots,|E|(\mathcal{N}+1)+|V_1|\mathcal{N}$. Hence, any non-trivial integral solution $\mathbf{x}$ of $\boldsymbol{A}\mathbf{x}=\mathbf{0}$ has one entry, say $x_{|V_1|\mathcal{N}+|V_2|\mathcal{N}+1+j^*}$, $j^* \in \{1,\ldots,|V_1|\mathcal{N}\}$ satisfying

$$\|\mathbf{x}\|_\infty \geq |x_{|V_1|\mathcal{N}+|V_2|\mathcal{N}+1+j^*}| \geq \sqrt{opt_{\mathrm{MinPSL}_\infty}(I)}.$$

Now assume $opt_{\mathrm{MinPSL}_\infty}(I)=1$. Let $(\mathcal{P}_1,\mathcal{P}_2)$ denote the corresponding labelling. Then the $(2|V_1|\mathcal{N}+|V_2|\mathcal{N}+1)$-length vector $\mathbf{x}$ given by

$$\begin{array}{rcll} x_{v_i,\mathcal{P}_i(v_i)} & := & 1 & \forall v_i \in V_i,\ i=1,2 \\ x_{v_i,b} & := & 0 & \forall v_i \in V_i, \\ & & & \forall b \in \mathcal{B}\setminus\mathcal{P}_i(v_i), \\ & & & i=1,2 \\ x_{|V_1|\mathcal{N}+|V_2|\mathcal{N}+1} & := & -1 & \\ x_{|V_1|\mathcal{N}+|V_2|\mathcal{N}+1+i} & := & -x_i & i=1,\ldots,|V_1|\mathcal{N} \end{array}$$

obviously is a feasible solution of the homogeneous linear system $\boldsymbol{A}\mathbf{x}=\mathbf{0}$ satisfying $\|\mathbf{x}\|_\infty = 1$.

The reduction from the given instance I of MIN PSEUDO LABEL COVER to the above constructed matrix $\boldsymbol{A}$ is feasible in time polynomial in the dimension of $\boldsymbol{A}$ which in turn is polynomial in $|I|$. Clearly, the above reduction τ is gap-reserving with parameters $((1,\rho),(1,\sqrt{\rho}))$. □

Combining Lemma 1 and the above Theorem 2 yields the following.

Corollary 1 *Approximating* MIN $\mathbb{Z}$-SOLUTION OF HOMOGENEOUS LINEAR SYSTEM *in* ℓ_∞*-norm within a factor of* $2^{\log^{0.5-\gamma} n}$ *is almost-***NP***-hard for any* $\gamma > 0$.

5 The Final Reduction

5.1 Aggregation

The following lemma implicitely proven by Kannan [11] establishes a polynomial time reduction from a system of homogeneous linear equations to a single equation with identical solution set, provided that the solutions are bounded.

Lemma 3 *Let* $\boldsymbol{A}$ *be an integral* $r\times n$ *matrix,* $\|\boldsymbol{A}\|_\infty$ *the maximum absolut value of its entries* a_{ij}, $1 \leq i \leq r$, $1 \leq j \leq n$ *and* $\mathbf{0}$ *be the* r*-dimensional all-zero vector. Then*

$$\begin{aligned} & B_\mu \cap \{\mathbf{x}\in\mathbb{Z}^n \mid \boldsymbol{A}\mathbf{x}=\mathbf{0}\} \\ = \ & B_\mu \cap \left\{\mathbf{x}\in\mathbb{Z}^n \;\middle|\; \sum_{i=1}^{r}\sum_{j=1}^{n} k^i a_{ij}x_j = 0\right\} \end{aligned}$$

where B_μ *denotes the* n*-dimensional ball of* ℓ_∞*-radius* μ *centered at the origin and* $k = n\|\boldsymbol{A}\|_\infty\mu + 1$.

Proof. Denote the two sets by S_r and S_1, respectively. Clearly, $S_r \subseteq S_1$. For proving the reverse inclusion, suppose that there exists an element $\mathbf{x}\in S_1$ not satisfying at least one equation of $\boldsymbol{A}\mathbf{x}=\mathbf{0}$. Let $i_{\max}$ denote the largest index for which $\langle \mathbf{a}_i,\mathbf{x}\rangle \neq 0$. As $\|\mathbf{x}\|_\infty \leq \mu$ we have

$$|\langle \mathbf{a}_i,\mathbf{x}\rangle| \leq n\|\boldsymbol{A}\|_\infty\mu = k-1$$

and since $\mathbf{x}\in S_1$ we must have

$$\sum_{i=1}^{r} k^i\langle \mathbf{a}_i,\mathbf{x}\rangle = 0.$$

By definition of $i_{\max}$ this yields

$$\sum_{i=1}^{i_{\max}-1} k^i\langle \mathbf{a}_i,\mathbf{x}\rangle = -k^{i_{\max}}\langle \mathbf{a}_{i_{\max}},\mathbf{x}\rangle$$

with a non-zero right-hand side implying that the left-hand side is also non-zero. Now the left-hand side is both a multiple of $k^{i_{\max}}$ and in absolute value bounded by $k^{i_{\max}}-k \leq k^{i_{\max}}-1$, a contradiction of course proving the lemma. □

5.2 Hardness of Approximating Optima for Integer Relations

By piecing the above results together we now prove the following.

Theorem 4 *Unless* **NP** $\subseteq$ **QP**, *there exists no polynomial time algorithm approximating the* SHORTEST INTEGER RELATION *problem in* ℓ_∞*-norm within a factor of* $2^{\log^{0.5-\gamma} n}$, *where* γ *is an arbitrarily small positive constant.*

Proof. We may assume that we are given an instance $I_1 = (V_1,V_2,E,\Pi,\mathcal{B},\mathcal{N})$ of MIN PSEUDO LABEL COVER with the properties shown in Lemma 1. In applying the reduction given in the proof of Theorem 2 we obtain an instance I_2 of MIN $\mathbb{Z}$-SOLUTION OF HOMOGENEOUS LINEAR SYSTEM. I_2 consists of an integral $(|V_1|\mathcal{N}+|E|(\mathcal{N}+1))\times(2|V_1|\mathcal{N}+|V_2|\mathcal{N}+1)$ matrix $\boldsymbol{A}$. For the proof of the Theorem it thus suffices to have a gap-preserving reduction from MIN $\mathbb{Z}$-SOLUTION OF HOMOGENEOUS LINEAR SYSTEM to SHORTEST INTEGER RELATION.

Fixing $\rho \geq 1$ and applying Lemma 3 to the matrix $\boldsymbol{A}$ with $\mu=\sqrt{\rho}$ and $k=(2|V_1|\mathcal{N}+|V_2|\mathcal{N}+1)\sqrt{\rho}+1$ (note that $\|\boldsymbol{A}\|_\infty = 1$) will do the work. We obtain an instance, say I_3, of SHORTEST INTEGER RELATION, consisting in a single equation

$$\sum_{i=1}^{r}\sum_{j=1}^{n} k^i a_{ij}x_j = 0, \qquad (*)$$

where $r = |V_1|\mathcal{N}+|E|(\mathcal{N}+1)$ and $n = 2|V_1|\mathcal{N}+|V_2|\mathcal{N}+1$.

Assume $opt_{\mathrm{MinHLS}_\infty}(I_2) \geq \sqrt{\rho}$. By Lemma 3 a solution $\mathbf{x}$ of $(*)$ with $\|\mathbf{x}\|_\infty < \sqrt{\rho}$ is also a solution of $\boldsymbol{A}\mathbf{x} = \mathbf{0}$, contradicting Theorem 2. Hence, for every solution $\mathbf{x}$ of $(*)$ we must have

$$opt_{\mathrm{SIR}_\infty}(I_3) \geq \sqrt{\rho}.$$

If $opt_{\mathrm{MinHLS}_\infty}(I_2) = 1$, again by Lemma 3, every optimum solution for I_2 is a witness of $opt_{\mathrm{SIR}_\infty}(I_3) = 1$.

Thus, we obtain a quasi-polynomial time transformation τ such that, for all instances I and for all $\gamma > 0$,

$$I \in \text{3-SAT} \implies opt_{\mathrm{SIR}_\infty}(\tau(I)) = 1$$
$$I \notin \text{3-SAT} \implies opt_{\mathrm{SIR}_\infty}(\tau(I)) \geq \sqrt{2^{\log^{0.5-\gamma}|\tau(I)|}}.$$

Therefore, given a polynomial time algorithm approximating the SHORTEST INTEGER RELATION problem in ℓ_∞-norm within a factor of $2^{\log^{0.5-\gamma} n}$ for some $\gamma > 0$ would enable us to decide 3-SAT in quasi-polynomial time. □

From Theorem 4 we easily conclude the following.

Corollary 2 *Approximating* SHORTEST INTEGER RELATION *in ℓ_∞-norm within a factor of $2^{\log^{0.5-\gamma} n}$ is almost-***NP***-hard for any $\gamma > 0$.*

6 Conclusion

We have shown that under the assumption **NP** $\not\subseteq$ **QP** there exists no polynomial time algorithm approximating SIR_∞ within a factor of $2^{\log^{0.5-\gamma} n}$, where $\gamma > 0$.

Improving the inapproximability gap to n^δ for some $\delta > 0$ is a still open problem. It is also desirable to prove the **NP**-hardness of approximating SIR_∞ rather than the almost-**NP**-hardness.

Arora et al. [4] showed also the almost-**NP**-hardness of approximating the NEAREST VECTOR for any ℓ_p-norm, the NEAREST CODEWORD and related problems within a factor of $2^{\log^{0.5-\gamma} n}$ for $\gamma > 0$. The proof relies on a quasi-polynomial time reduction from the LABEL COVER problem (see [4, 3]). Using a recent result of Raz [15] the inapproximability gap can be amplified to $2^{\log^{1-\gamma} n}$ for $\gamma > 0$. Unfortunately, the underlying technique ('parallel repetition') cannot be applied to the MIN PSEUDO LABEL COVER problem since the latter has specific geometric properties inherently given by the 2-prover 1-round interactive proof-system of [9] (see also [8]).

Thus, in order to resolve the above open problems a more direct reduction to SIR_∞ avoiding MIN PSEUDO LABEL COVER seems promising. This point requires further study.

Acknowledgment

We would like to thank Claus Schnorr for several valuable discussions.

References

[1] E. Amaldi and V. Kann. The complexity and approximability of finding maximum feasible subsystems of linear relations. *Theoretical Computer Science*, Volume 147, pages 181–210, 1995.

[2] E. Amaldi and V. Kann. On the approximability of removing the smallest number of relations from linear systems to achieve feasibility. Technical Report ORWP-6-94, Department of Mathematics, Swiss Federal Institute of Technology, Lausanne, 1995.

[3] S. Arora. *Probabilistic Checking of Proofs and Hardness of Approximation Problems.* Ph.D. thesis, University of California at Berkeley, 1994.

[4] S. Arora, L. Babai, J. Stern and Z Sweedyk. The hardness of approximate optima in lattices, codes and systems of linear equations. In *Proc. 34th IEEE Symp. on Foundations of Computer Science*, pages 724–730, 1993.

[5] S. Arora, C. Lund, R. Motwani, M. Sudan and M. Szegedy. Proof verification and hardness of approximation problems. In *Proc. 33rd IEEE Symp. on Foundations of Computer Science*, pages 14–23, 1992.

[6] G. Ausiello, P. Crescenzi and M. Protasi. Approximate solutions of NP optimization problems. *Theoretical Computer Science*, Volume 150, pages 1–55, 1995.

[7] L. Babai, B. Just and F. Meyer auf der Heide. On the limits of computations with the floor function. *Information and Computation*, Volume 78, pages 99–107, 1988.

[8] U. Feige and J. Kilian. Impossibility results for recycling random bits in two-prover proof systems. In *Proc. 27th ACM Symp. Theory of Computing*, pages 457–468, 1995.

[9] U. Feige and L. Lovász. Two-prover one-round proof systems: Their power and their problems. In *Proc. 24th ACM Symp. Theory of Computing*, pages 643–654, 1992.

[10] J. Håstad, B. Just, J. C. Lagarias and C. P. Schnorr. Polynomial time algorithms for finding integer relations among real numbers. *SIAM J. Computation*, Volume 18, pages 859–881, 1989.

[11] R. Kannan. Polynomial-time aggregation of integer programming problems. *J. ACM*, Volume 30, pages 133–145, 1983.

[12] R. Kannan, A. K. Lenstra and L. Lovász. Polynomial factorization and nonrandomness of bits of algebraic and some transcendental numbers. *Math. Comp.*, Volume 50, pages 235–250, 1988.

[13] J. C. Lagarias. The computational complexity of simultaneous diophantine approximation problems. *SIAM J. Comput.*, Volume 14, pages 196–209, 1985.

[14] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes.* North Holland, Amsterdam, 1977.

[15] R. Raz. A parallel repetition theorem. In *Proc. 27th ACM Symp. Theory of Computing*, pages 447–456, 1995.

[16] P. van Emde Boas. Another NP-complete partition problem and the complexity of computing short vectors in a lattice. Technical Report 81-04, Math. Inst., University of Amsterdam, 1981.