Symmetries in Semidefinite and Polynomial Optimization

– Relaxations, Combinatorics, and the Degree Principle –

Dissertation zur Erlangung des Doktorgrades der Naturwissenschaften

vorgelegt beim Fachbereich 12
der Johann Wolfgang Goethe-Universität
in Frankfurt am Main

von Cordian Benedikt Riener, geboren in Memmingen.

Frankfurt 2011
(D 30)

Vom Fachbereich 12 der Johann Wolfgang Goethe-Universität angenommen.

Dekan:	Prof. Dr. Tobias Weth
Gutachter:	Prof. Dr. Thorsten Theobald Prof. Dr. Markus Schweighofer Prof. Dr. Christine Bachoc
Datum der Disputation:	10.06.2011

Symmetry is a vast subject, significant in art and nature. Mathematics lies at its root, and it would be hard to find a better one on which to demonstrate the working of the mathematical intellect

(Hermann Weyl)

Acknowledgements

At the beginning of this thesis I would like to express my deep gratitude to all the people who supported me during my work so far. Throughout this work I received the support of my family, friends, and colleagues.

I am heartily thankful to my advisor, Thorsten Theobald, for his encouragement, supervision, and support from the preliminary to the concluding level. He gave me fruitful impulses but also left me enough space to develop own ideas.

Further I also want to express my gratitude to all the academic teachers whose courses provided the basis of my research. Especially Gabriele Nebe for her excellent courses in algebra and her patient guidance during my work for the Diploma Thesis and Rainer Nagel who initiated and organized the "Rome seminars" which always provided a possibility to widen my horizons.

I am very much indebted to Christine Bachoc, Greg Blekherman, Lina Jansson, Jean Bernard Lasserre, Salma Kuhlmann, Alexander Kovačec, Markus Schweighofer for their impulses and collaboration during the work for this thesis and their interest in my work.

I want to thank Hans Mittelmann who kindly offered to calculate some of the large semidefinite programs. Without his help I would not have been able to calculate these SDPs.

I am very grateful for the help of Gabriella Óturai, Theresa Szczepanski, Hartwig Bosse, Sadik Iliman, Eddie Kim, Jörg Lehnert, Benjamin Mühlbauer, Johannes Nübler, Raman Sanyal, Henning Sulzbach, Reinhard Steffens, Max Stroh, and Louis Theran who gave valuable feedback and comments on preliminary versions of parts of this work.

Finally financial support from the German Academic Exchange Service (DAAD) for a research stay in Bordeaux is greatly acknowledged.

Zusammenfassung

In den letzten Jahren hat sich die Nutzung von Symmetrien in Anwendungen der semidefiniten Optimierung als vorteilhaft erwiesen. Die vorliegende Arbeit untersucht Möglichkeiten der Nutzung diskreter Symmetrien im Kontext dreier Problemfelder: In der polynomiellen Optimierung, beim Positivitätstest symmetrischer Polynome und in der kombinatorischen Optimierung. Die Arbeit präsentiert hierzu neue Zugänge, ermöglicht damit neue Einsichten in die zugrunde liegenden Paradigmen der Symmetrienutzung und sie studiert ein konkretes Beispiel der kombinatorischen Optimierung.

Semidefinite und polynomielle Optimierung

Seien $f, g_1, \ldots, g_m$ reelle Polynome in n Unbestimmten. Durch die Polynome $g_1, \ldots, g_m$ werde dann eine so genannte *semialgebraische Menge*

$$K := \{x \in \mathbb{R}^n \,:\, g_1(x) \geq 0, \ldots, g_m(x) \geq 0\}$$

beschrieben. Unter einem *polynomiellen Optimierungsproblem* (POP) verstehen wir nun das Problem das $x^* \in \mathbb{R}^n$ zu bestimmen, für welches (falls existent) gilt

$$f(x^*) = \min_{x \in K} f(x).$$

Die *Momentenmethode* zur Lösung der oben beschriebenen Probleme geht auf N.Z. Shor [Sho87] aus dem Jahr 1987 zurück und überführt das polynomielle Problem in ein konvexes. Dieser Ansatz wurde in den letzten Jahren von Lasserre [Las01], sowie in dualer Form durch Parrilo [Par03] vorangetrieben. Das so entstandene Relaxierungsschema zielt darauf hin ab, polynomielle durch *semidefinite Optimierungprobleme* (SDP) zu approximieren. Vorteilhaft hierbei ist, dass sich die Optimalwerte solcher linearen Optimierungsprobleme über dem Kegel der positiv definiten Matrizen leichter bestimmen lassen.

Die Ausgangsidee dieses Zugangs besteht darin, statt des Minimums von f das größte reelle λ zu bestimmen, so dass $f - \lambda$ als eine Summe von Quadraten in $\mathbb{R}[X_1, \ldots, X_n]$ geschrieben werden kann. Da sich dieses Positivitätszertifikat als semidefinites Programm realisieren lässt, ist das gesuchte λ leichter zu bestimmen und bildet eine untere Schranke für den globalen Optimalwert f^*. Diese Approximation liefert in vielen Fällen schon eine sehr gute Näherung und wurde mittlerweile unter Zuhilfenahme tiefgehender Resultate der semi-algebraischen Geometrie (Hilberts 17. Problem der Darstellbarkeit nichtnegativer Polynome, dem Momentenproblem und den Positivstellensätzen) in vielfacher Hinsicht weiterentwickelt, so dass unter relativ allgemeingültigen Voraussetzungen eine Hierarchie von wachsenden SDPs für ein polynomielles Optimierungsproblem konstruiert werden kann, deren sukzessive Werte zum Optimalwert des Ausgangsproblems konvergieren.

Zwar lassen sich semidefinite Probleme leichter lösen als polynomielle, jedoch beinhaltet die SDP–Relaxierung der Ordnung k in der Hierarchie in der Regel $O(n^{2k})$-Variablen und lineare Matrixungleichungen (LMIs) der Größe $O(n^k)$. Dieses exponentielle Anwachsen der auftretenden Matrixgrößen macht es schwer hohe Relaxierungsstufen mit einem Computer zu konkretisieren. Es ist daher notwendig, spezifische Besonderheiten einzelner Probleme zu nutzen, um eine Vereinfachung möglich zu machen. Eine solche Besonderheit ist Symmetrie, und wir präsentieren in dieser Arbeit verschiedene Zugänge, diese vorteilhaft auszunutzen.

Ausnutzen der Symmetrie im „Lasserre–Relaxierungs–Schema“

Im Kontext des Lasserre–Relaxierungsschemas für polynomielle Optimierung zeigen wir in dieser Arbeit, wie sich Symmetrien auf zwei Ebenen vorteilhaft nutzen lassen: Einerseits auf der Seite der polynomiellen Formulierung mittels des so genannten *geometrischen Quotienten*, andererseits auf der Seite der semidefiniten Relaxierung mittels der Blockdiagonalisierung.

Der erste Ansatz bedient sich der Invariantentheorie, sowie der von Procesi und Schwarz (siehe [PS85, Brö98]) gegebenen semi-algebraischen Darstellung des so genannten *Orbitraums*. Hierbei nutzen wir die Tatsache, dass sich die von Procesi und Schwarz gegebene Beschreibung des Orbitraums als polynomielle Matrixungleichung realisieren läßt. Dies ermöglicht uns, ein Relaxierungschema im geometrischen Quotienten zu definieren (Theorem 3.11). Mit diesem Schema lässt sich die Tatsache ausnutzen, dass der Übergang zum Invariantenring $\mathbb{R}[X]^G$ in vielen Fällen eine deutliche Reduzierung des Grades der Polynome mit sich bringt.

Das Studium der Blockdiagonalisierung von SDPs geht auf Arbeiten von Schrijver [Sch79, Sch05a] (im Kontext von Matrix $*$-Algebren) und Gatermann und Parillo [GP04] (im Kontext von Darstellungstheorie) zurück und hat in letzter Zeit vielfache Anwendung im SDP Bereich gefunden [KOMK01, Sch05a, Gij05, Lau07b, BV08, BV09, BNdOFV09].

In der vorliegenden Arbeit richten wir ein spezielles Augenmerk auf solche SDPs, die im Relaxierungsschema von Lasserre entstehen, bei dem sich die Symmetrie des Ausgangsproblems auf die Matrizen im Relaxierungsschema überträgt. Eine grundlegende Untersuchung von Symmetrie im Kontext des klassischen *Momentenproblems* ist mittlerweile auch von Cimpric, Kuhlmann und Scheiderer [CKS09] geleistet. Wir erarbeiten hier symmetrische Versionen des Satzes von Putinar (Theorem 3.2 und Theorem 3.4) und verwenden diese dazu, eine die Symmetrie nutzende Relaxierung für ein POP zu definieren. Diese ist direkt blockdiagonal, d.h. an die Stelle der großen Momenten- und Lokalisierungsmatrizen treten Matrizen kleinerer Dimension. Auch dieses Relaxierungsschema hat die Konvergenzeigenschaft des ursprünglichen Schemas (Theorem 3.6).

Positivität symmetrischer Polynome und das „Grad–Prinzip“

Um in polynomiellen Optimierungsproblemen, bei denen sowohl die Zielfunktion f als auch die Nebenbedingungen g_i durch symmetrische Polynome gegeben sind, die Symmetrie vielfältig ausnutzen zu können, untersuchen wir eingehend, ob und inwiefern sich die hohe Symmetrie der Problemformulierung in diesem speziellen Fall auch auf die Lösungen überträgt. Ein elementarer und allgemein bekannter Vertreter solcher Probleme ist beispielsweise die Frage, welches Rechteck mit den Seitenlängen a und b bei gegebenem Umfang $2a + 2b$ den Flächeninhalt maximiert. Die Symmetrie der Problemstellung in den Variablen a und b spiegelt sich hierbei in der Symmetrie der Lösung - des Quadrates - wider. In diesem Fall überträgt sich also die gesamte Symmetrie der Problemstellung auf die Lösung. Bereits der französische Philosoph und Mathematiker Olry Terquem betrachtete 1840 Probleme der obigen Bauart. In Verallgemeinerung des gegebenen Beispiels postulierte er dazu, es sei unter solchen Bedingungen evident, dass das Optimum stets in einem symmetrischen Punkt angenommen werde (vgl. [Ter40]). Obgleich Terquems Postulat von einem ästhetischen Standpunkt aus betrachtet durchaus wünschenswert erscheinen mag, wurden bereits einige Jahre nach der Veröffentlichung Terquems vom russischen Mathematiker Bouniakovsky [Bou54] Beispiele von symmetrischen Problemen angegeben, welche keine symmetrischen Lösungen besitzen.

In diesem Kontext von symmetrischen Polynomen beweisen wir daher ein *Grad–Prinzip*, welches genauer quantifiziert, wie viel Symmetrie eines durch symmetrische Polynome von festem Grad gegebenen Optimierungsproblems auf die Lösungen übertragen wird. Wenn man mit A_d bzw. A_d^+ diejenigen Punkte in $\mathbb{R}^n$ bzw. $\mathbb{R}^n_{\geq 0}$ bezeichnet, welche höchstens d verschiedene Komponenten bzw. d verschiedene positive Komponenten aufweisen, lautet unser Resultat zur Frage der Symmetrie der Lösungen:

Theorem
Es seien $f, g_1, \ldots, g_m \in \mathbb{R}[X_1, \ldots, X_n]$ *symmetrische Polynome und*

$$K := \{x \in \mathbb{R}^n \,:\, g_1(x) \geq 0, \ldots, g_m(x) \geq 0\}.$$

Der Grad von f *sei* d *und wir setzen* $k := \max\left\{2, \lfloor \frac{d}{2} \rfloor, \deg g_1, \ldots, \deg g_m\right\}$.
Dann gilt:

$$\inf_{x \in K} f(x) = \inf_{x \in K \cap A_k} f(x) \text{ und}$$
$$\inf_{x \in K \cap \mathbb{R}^n_+} f(x) = \inf_{x \in K \cap A_k^+} f(x).$$

Die Symmetrie der Lösung hängt also maßgeblich vom Grad der vorkommenden Polynome ab.

Den Schlüssel zum Beweis dieses Grad–Prinzips bilden jene reellen univariaten Polynome, deren Nullstellen alle auf der reellen Achse liegen. Mittels der klassischen Formel von Vieta

lassen sich die Werte der elementarsymmetrischen Polynome als Koeffizienten univariater Polynome sehen. Dadurch wird es möglich, die Beweisschritte anhand von Aussagen zu erhalten, welche sich direkt aus dem Satz von Rolle ergeben. Unter dem Blickwinkel globaler Optimierung betrachtet, liefert das obige Theorem eine Charakterisierung der Positivität symmetrischer Polynome anhand ihrer Werte auf der k-dimensionalen Menge A_k. Als direktes Korollar ergibt sich daher das so genannte *Halb–Grad–Prinzip*, welches von Vlad Timofte in [Tim03] zum ersten Mal formuliert und bewiesen wurde.

Korollar
Es sei $F \in \mathbb{R}[X]$ ein symmetrisches Polynom vom Grad d und wir setzen

$$k := \max\{2, \lfloor \frac{d}{2} \rfloor\}.$$

Dann gilt: Genau dann ist $F(x) \geq 0$ für alle $x \in \mathbb{R}^n$, wenn $F(y) \geq 0$ für alle $y \in A_k$. Des Weiteren gilt: Genau dann ist $F(x) \geq 0$ für alle $x \in \mathbb{R}^n_+$, wenn $F(y) \geq 0$ für alle $y \in A^+_k$.

Die ursprünglich von Timofte stammende Aussage, welche in [Tim03] unter Zuhilfenahme von Differentialgleichungen abgeleitet wurde, erhält durch unseren Zugang über univariate Polynome somit einen elementaren Beweis.

Darüber hinaus zeigt sich eine Beziehung unseres Zugangs zu einem Satz von Thomas Foregger [For87]:

Theorem
Sei $n \geq 2$ und ferner sei $\phi(x) = \phi(x_1, \ldots, x_n)$ eine reelle Linearkombination von elementarsymmetrischen Polynomen. Des Weiteren sei

$$C_\gamma := \left\{ x \in [0,1]^n : \sum_{i=1}^{n} x_i = \gamma \right\}.$$

Angenommen die Funktion $\phi : C_\gamma \to \mathbb{R}$ hat ein lokales Extremum $a \in \mathrm{int}(C_\gamma)$ im relativen Inneren von C_γ, dann ist entweder ϕ konstant oder a ist der symmetrische Punkt in C_γ, d.h. $a = (\frac{\gamma}{n}, \ldots, \frac{\gamma}{n})$.

Wir werden in einer genauen Analyse des ursprünglich von Foregger gelieferten Beweises zeigen, dass dieser fehlerhaft ist. Des Weiteren werden wir darlegen, dass sich ein Beweis von Foreggers Satz auch unmittelbar aus unseren Überlegungen zum Beweis des Grad–Prinzips ergibt.

Optimierung mit symmetrischen Polynomen

Unter den diskreten Gruppen nimmt die symmetrische Gruppe $\mathcal{S}_n$ durch ihre reichhaltige Kombinatorik eine herausragende Stellung ein. Daher erarbeiten wir alle im Folgenden

dargestellten Möglichkeiten zur Symmetrienutzung ausführlich am Beispiel der Gruppe $\mathcal{S}_n$.

Wir benutzen dazu die klassische Konstruktion der irreduziblen Darstellungen der Gruppe $\mathcal{S}_n$ von Wilhelm Specht [Spe37], die wir für unsere Bedürfnisse verallgemeinern. Mit diesen so erhaltenen *Spechtpolynomen* zeigt sich, dass die symmetrie–angepasste Momentenrelaxierung sehr explizit angegeben werden kann (Theorem 5.5). Unsere hierbei erarbeiteten Techniken geben Antworten auf die von Gatermann und Parrilo ([GP04] S. 124) explizit als offen bezeichnete Frage nach einer kombinatorischen Charakterisierung der isotypischen Komponenten in diesem Fall. Mittels der Kombinatorik der *irreduziblen Darstellungen* der Gruppe $\mathcal{S}_n$, den so genannten Specht-Moduln, können wir nämlich auch ein Grad-Prinzip für die symmetrie–angepasste Momentenrelaxierung im Fall der Gruppe $\mathcal{S}_n$ zeigen: Die Größe der zu betrachtenden Matrizen und somit auch die Komplexität der zu führenden Berechnungen hängt in diesem Fall nur vom Grad der Relaxierungsstufe ab (Theorem 5.7).

Als eine direkte Folgerung der symmetrie–angepassten Momentenrelaxierung können wir in der hierzu dualen Sichtweise konkrete Darstellungssätze für symmetrische Summen von Quadraten angeben (Theorem 5.10). Insbesondere lassen sich dadurch positive $\mathcal{S}_n$–invariante Formen in den drei Hilbert–Fällen ($n = 1, d = 2$ und $(n, d) = (3, 4)$) charakterisieren (Korollare 5.11, 5.12, 5.13).

Weiterhin werden wir zeigen, dass sich auch das Grad–Prinzip bei SDP-Relaxierungen gewinnbringend anwenden lässt. Dazu studieren wir, wie sich mit Hilfe dieses Prinzips ein Relaxierungsschema definieren lässt, welches das symmetrische polynomielle Optimierungsproblem in n Variablen vom Grad d durch eine Familie von Lasserre–Relaxierungen in d Variablen annähert. Wir zeigen, dass unter den allgemeinen Voraussetzungen an das polynomielle Optimierungsproblem (Putinar–Bedingung) auch dieses Schema eine zum Optimum konvergierende Folge von Näherungen liefert (Theorem 5.14). Darüber hinaus können wir in einigen Fällen die endliche Konvergenz dieses Schemas zeigen (Theorem 5.16). Obwohl im allgemeinen Fall positive symmetrische Polynome vom Grad 4 nicht unbedingt als Summe von Quadraten darstellbar sind, folgern wir in Theorem 5.17, dass sich die Frage der Positivität in diesem Fall auf eine Frage nach einer Darstellung als Summe von Quadraten überführen lässt.

Des Weiteren zeigen wir, wie der Ansatz über den Orbitraum in einer Beispielklasse von Potenzsummenproblemen gewinnbringend genutzt werden kann. Die von uns studierte Klasse verallgemeinert hierbei ein Problem, welches von Brandenberg und Theobald [BT06] untersucht wurde. Wir zeigen dabei, wie der von uns definierte Ansatz der Relaxierung im Orbitraum dazu verwendet werden kann, sowohl obere als auch untere Schranken für Probleme dieser Bauart anzugeben, welche sich einfach berechnen lassen (Theoreme 5.21 und 5.22).

Schranken für kombinatorische Probleme der Codierungstheorie

Die ursprünglichen Anwendungen von semidefiniter Optimierung liegen zu einem großen Teil in der kombinatorischen Optimierung (z.B. [Lov79]). Daher zeigen wir am Beispiel einer Frage aus der Kombinatorik von Codes, wie sich die reichhaltige Symmetrie des Problems gewinnbringend nutzen lässt.

Klassisch wird in der Theorie binärer Codes der so genannte *Hamming–Abstand* $d_H(x, y)$ verwendet. Dieser ist für zwei Elemente $x, y \in \mathbb{F}_2^n$ definiert als

$$d_H(x, y) := \#\{x_i \neq y_i\}.$$

In den 1970er Jahren konnte Delsarte [Del73] einen vielbeachteten Ansatz zur Abschätzung der Größe von Codes mit gegebenem Minimalabstand vorstellen, welcher auf der Lösung linearer Programme beruht. Schrijver [Sch79] sowie unabhängig davon McEliece, Rode, und and Rumsey [MRR78] stellten einige Jahre später einen Zusammenhang zwischen Delsartes LP–Methode und einer Symmetrisierung des von Lovász definierten Graph–Parameters ϑ her, welcher als Lösung eines SDPs definiert ist. Dieser Zusammenhang hat in den letzten Jahren zu neuen SDP basierten Schranken für Codes mit gegebenem Hamming–Abstand geführt [Sch05a, Lau07b, Gij05, GMS10].

In dieser Arbeit liefern wir SDP–basierte Abschätzungen für die Größen von Codes, welche von so genannten Pseudodistanzen abhängen. Im Gegensatz zum Hamming–Abstand, der für Paare von Punkten definiert ist, sind solche Pseudodistanzen für allgemeine k-Tupel von Punkten definiert. Ein Beispiel für eine solche Pseudodistanz, zu welcher wir auch numerische Resultate für unsere Methode liefen, ist der *verallgemeinerte Hamming–Abstand*. Dieser wurde von Cohen, Litsyn und Zémor [CLZ94] erstmalig definiert und geht auf Arbeiten von Ozarow und Wyner [OW84] im Umfeld der praktischen Anwendung zurück.

Unsere Methode zur Konstruktion von SDP–basierten Schranken in diesem Fall folgt der von Schrijver in [Sch05a] für Tripel benutzte Idee, den für Graphen definierten Parameter ϑ' auf Hypergraphen zu verallgemeinern. Ein entscheidender Wesenszug unseres Zugangs ist, dass wir die hohe Symmetrie des *Hamming–Würfels* geschickt ausnutzen können, um die entstandenen SDPs zu vereinfachen. Nur so ist es möglich die resultierenden Programme numerisch zu lösen.

Gliederung dieser Dissertation

Diese Arbeit ist wie folgt gegliedert: Das erste Kapitel führt in die semidefinite und polynomielle Optimierung ein. Zuerst stellen wir hierzu eine kurze Einführung in die Theorie der semidefiniten Programme zur Verfügung, wobei wir uns auf die für die Arbeit relevanten Aspekte begrenzen. In diesem Zusammenhang führen wir auch den Parameter ϑ ein.

Danach führen wir aus, wie sich ausgehend von Hilberts Charakterisierung von positiven Polynomen als Summen von Quadraten die SDP–basierten Ansätze zur polynomiellen Optimierung entwickelten.

Im zweiten Kapitel stellen wir eine kurze Einführung in die moderne mathematische Sichtweise auf Symmetrie bereit. Namentlich beschäftigen wir uns mit Darstellungs– und Invariantentheorie, wobei wir uns beide Male auf den Fall von endlichen Gruppen beschränken. Wir beginnen mit Grundzügen linearer Darstellungstheorie, wobei insbesondere das Lemma von Schur für das weitere Vorgehen wichtig ist. Insbesondere führen wir aus, wie sich Darstellungstheorie im Kontext von semidefiniter Programmierung als wichtiges Hilfsmittel zur Reduktion der Rechenkomplexität erweist. Danach stellen wir den kombinatorischen Zugang zur Darstellungetheorie der symmetrischen Gruppe $\mathcal{S}_n$ bereit. Der Überblick auf die mathematische Verwendung von Symmetrie wird durch eine kurze Darstellung der Invariantentheorie abgerundet.

Im dritten Kapitel der Arbeit untersuchen wir, wie sich die Invarianz eines polynomiellen Optimierungsproblems unter einer endlichen Gruppe im Kontext von SDP–Relaxierungen ausnutzen lässt und stellen dazu zwei Vorgehensweisen bereit: Einerseits diskutieren wir, wie sich Symmetrie im Kontext des Momentenproblems mittels linearer Darstellungstheorie ausnutzen lässt. Hierbei entwickeln wir ein symmetrie–angepasstes Relaxierungs-Schema. Andererseits zeigen wir auch auf, wie Invariantentheorie direkt auf der Ebene des polynomiellen Optimierungsproblems vorteilhaft genutzt werden kann.

Im vierten Kapitel beschäftigen wir uns mit der Frage der Positivität symmetrischer Polynome. Wir betrachten dazu eine Verallgemeinerung eines Resultats von Vlad Timofte. Wir zeigen auf, wie sich diese Verallgemeinerung auf eine Frage über Nullstellen von reellen univariaten Polynomen überführen lässt und können somit einen neuen elementaren Beweis sowohl für das Grad- als auch das Halbgradprinzip angeben.

Das fünfte Kapitel dient dazu, die eingeführten Techniken zur Symmetrieausnutzung am Beispiel der Symmetrischen Gruppe $\mathcal{S}_n$ genauer zu studieren. Zur genauen Beschreibung der symmetrie–angepassten Relaxierung eines (POP) gehen wir daher im ersten Abschnitt daran, die klassische Darstellungstheorie der Gruppe $\mathcal{S}_n$ in diesen Kontext zu überführen. Dadurch sind wir in der Lage, die Situation im Fall von $\mathcal{S}_n$-invarianten POPs genauer zu beleuchten und erhalten zusätzlich Darstellungssätze für positive symmetrische Formen in den so genannten Hilbert–Fällen. Anschließend zeigen wir auf, wie sich mittels des Grad–Prinzips ein Relaxierungs–Schema definieren lässt. Zum Abschluss studieren wir anhand einer Klasse von Potenzsummen den Orbitraum–Zugang.

Im sechsten Kapitel erarbeiten wir SDP–basierte Schranken für ein kombinatorisches Problem aus der Codierungstheorie. Wir erläutern dazu kurz den Zusammenhang zwischen der Delsarte–Methode und dem SDP–Parameter ϑ. Daran anschließend zeigen wir auf, wie eine Verallgemeinerung dieses Parameters zu Schranken für das betrachtete Code–Problem führt. Um die bei diesem Vorgehen entstehenden SDPs für interessante Wahlen der Eingabeparameter in numerisch behandelbare SDPs kleinerer Größe zu verwandeln,

zeigen wir danach, wie sich die Symmetrie des Hamming–Würfels nutzen lässt. Abschließend geben wir kurz Beziehungen unseres Zugangs zu einer allgemeinen Methode an und stellen die numerischen Resultate vor.

Abstract

In recent years using symmetry has proven to be a very useful tool to simplify computations in semidefinite programming. In this dissertation we examine the possibilities of exploiting discrete symmetries in three contexts: In SDP–based relaxations for polynomial optimization, in testing positivity of symmetric polynomials, and combinatorial optimization. In these contexts the thesis provides new ways for exploiting symmetries and thus deeper insight in the paradigms behind the techniques and studies a concrete combinatorial optimization question.

Semidefinite and polynomial optimization

Let $f, g_1, \ldots, g_m$ be real polynomials in the n unknowns $x_1, \ldots, x_n$. The polynomials $g_1, \ldots, g_m$ then describe a *semialgebraic set* defined as

$$K := \{x \in \mathbb{R}^n \,:\, g_1(x) \geq 0, \ldots, g_m(x) \geq 0\}.$$

Finding $x^* \in \mathbb{R}^n$ which (if existent) satisfies

$$f(x^*) = \min_{x \in K} f(x)$$

is called a *polynomial optimization problem* (POP). The *moment method* designed to attack the kind of problems introduced above is based on work by N.Z. Shor [Sho87] dating to the year 1987. It uses the fact that a nonconvex polynomial optimization problem can be encoded into convex programs through the theory of moments and positive polynomials. This idea has been recently expanded on by Lasserre [Las01], and in the dual viewpoint by Parillo [Par03]. It yields a relaxation scheme which aims to approximate polynomial problems with *semidefinite optimization problems* (SDP). These linear optimization problems over the cone of symmetric matrices are easier to handle.

The basic idea behind this approach is to approximate the global minimum of f by the largest real λ such that $f - \lambda$ can be written as a sum of squares (SOS) in $\mathbb{R}[X_1, \ldots, X_n]$. This certificate for positivity can be realized as a semidefinite program and thus the λ in question provides an upper bound for the global minimum that can be determined quite efficiently. This first approximation already yields pretty good bounds for the global optimum f^* and has by now been developed further using some deep results from real algebraic geometry such as Hilbert's 17-th problem, Hamburger's moment problem and the so called *Positivstellensätze*. The result is that for a given POP that satisfies relatively general conditions one can construct a hierarchy of growing SDP–relaxations whose optimal solutions converge towards the optimal solution of the initial problem.

Exploiting symmetries in SDP–based relaxations for polynomial optimization

In this thesis we show how in the context of the Lasserre relaxation scheme for polynomial optimization symmetries can be advantageously used on two levels: On the one hand directly at the level of the polynomial formulation using the so-called *geometrical quotient*, on the other hand at the level of the semidefinite relaxation by using block diagonalization techniques.

The first approach uses invariant theory and the semialgebraic characterization of the so-called *orbit space* that Procesi and Schwarz [Brö98, PS85] provided. Here we use the fact that this description of the orbit space can be realized as a polynomial matrix inequality (PMI). This allows us to define a relaxation scheme in the geometric quotient (Theorem 3.11). This scheme allows exploitation of the fact that the transition to the invariant ring $\mathbb{R}[X]^G$ leads in many cases to a significant reduction of the degree of the polynomials involved.

The study of block diagonalizations of SDPs was initiated by Schrijver [Sch79, Sch05a] (in the general framework of matrix $*$-algebras)) and by Gatermann and Parrilo [GP04] (in the context of representation theory) and was recently used in may applications of SDPs [KOMK01, Sch05a, Gij05, Lau07b, BV08, BV09, BNdOFV09].

We provide a systematic treatment of block diagonalization in the setting of Lasserre's relaxation using the moment approach. Cimpric, Kuhlmann, and Scheiderer recently studied foundational aspects of symmetries in the problems of moments [CKS09]. Instead of considering a general SDP framework, we focus our attention on the specific SDPs coming from the relaxation where the symmetries on the original variables of the optimization problem induce specific additional symmetry structure on the moment and localizing matrices of the SDP–relaxation. To this end we suggest that a symmetry–adapted version of the relaxation scheme can be defined directly by using an appropriate basis for the moments. Here, the formulation of the relaxation scheme in the symmetry–adapted base will yield us symmetry–adapted versions of Putinar's Theorem (Theorem 3.2 and Theorem 3.4) and a symmetry–adapted relaxation scheme that converges (Theorem 3.6) under the same assumptions on the initial problem.

Positivity of symmetric polynomials and the degree principle

In order to exploit symmetries in the context of optimization problems that are defined by symmetric polynomials it will be useful to examine how much of the initial symmetry is carried over to the solutions. Indeed, many optimization problems that are given in a symmetric setting share the pleasant property that their solutions can be found among symmetric points, i.e. points that are invariant to the action of the symmetric group. The best known elementary example is that among all rectangles with given perimeter $2a + 2b$ the square maximizes the area. This was already observed by the French mathematician and philosopher Orly Terquem. In 1840 he studied problems of the above type. In [Ter40]

he postulated that it is evidently true that under the circumstances described above the optima will always be among the symmetric points. However already some years after Terquem the Russian mathematician Bouniakovsky [Bou54] provided concrete examples of symmetric optimization problems that have no symmetric solution.

In the setting of symmetric optimization problems under symmetric constraints we will derive a theorem that analyzes how much symmetry carries over to the minimizers in more detail. We will show that the symmetry of minimizers depends mainly on the degree of the polynomials involved.

Denoting the points in $\mathbb{R}^n$ (resp. $\mathbb{R}^n_{\geq 0}$) that have no more than d distinct (positive) components by A_d (resp. A_d^+) our result is phrased in the following theorem.

Theorem
Let $f, g_1, \ldots, g_m \in \mathbb{R}[X_1, \ldots, X_n]$ be symmetric and set

$$K = \{x \in \mathbb{R}^n \,:\, g_1(x) \geq 0, \ldots, g_m(x) \geq 0\}.$$

If f is of degree d and $k := \max\left\{2, \lfloor \frac{d}{2} \rfloor, \deg g_1, \ldots, \deg g_m\right\}$, then

$$\inf_{x \in K} f(x) = \inf_{x \in K \cap A_k} f(x) \text{ and}$$
$$\inf_{x \in K \cap \mathbb{R}^n_+} f(x) = \inf_{x \in K \cap A_k^+} f(x).$$

Hence the symmetry of the solution depends largely on the degree of the polynomials involved. The key to the proof of this *degree principle* lies in the study of the real univariate polynomials whose zeros lie all on the real axis. By means of the classical formula of Vieta the values of the elementary symmetric polynomials can be seen as coefficients of univariate polynomials. This makes it possible to obtain the steps of the proof based on statements which follow directly from the classical theorem of Rolle. When turning back this result to the positivity side of global optimization we recover a theorem which was initially proven by Vlad Timofte [Tim03], who established this result via the bounded solutions of a differential equation.

Corollary
Let $F_0 \in \mathbb{R}[X]$ be a symmetric polynomial of degree d and let $k := \max\left\{2, \lfloor \frac{d}{2} \rfloor\right\}$. Then the inequality $F_0(x) \geq 0$ holds for all $x \in \mathbb{R}^n$ (respectively x in the positive orthant $\mathbb{R}^n_+$) if and only if it holds for all $x \in A_k$ (respectively $x \in A_k^+$). Furthermore there is $x \in \mathbb{R}^n$ with $F_0(x) = 0$ if and only if there is $x \in A_k$ with $F_0(x) = 0$.

The reduction from Theorem 4.2 allows us to establish Timofte's theorem in a more natural way.

We will also mention a connection to the following theorem of Thomas Foregger [For87].

Theorem
Let $n \geq 2$, and suppose $\phi(x) = \phi(x_1, \ldots, x_n)$ is a real linear combination of elementary symmetric polynomials. Further set

$$C_\gamma := \left\{ x \in [0,1]^n : \sum_{i=1}^{n} x_i = \gamma \right\}.$$

Assume that the function $\phi : C_\gamma \to \mathbb{R}$ has a local extremum $a \in \operatorname{int}(C_\gamma)$ in the relative interior of C_γ then either ϕ is constant or a is the symmetric point in C_γ, i.e. $a = (\frac{\gamma}{n}, \ldots, \frac{\gamma}{n})$.

We will point out why Foregger's arguments used to prove his statement do not go through and are beyond repair. Therefore we will also apply the ideas used to prove the degree principle in order to deduce a correct proof for Foregger's theorem.

Optimizing with symmetric polynomials

In the discrete groups, the symmetric group $\mathcal{S}_n$ has -also due to its rich combinatorics- a prominent position. Therefore, we work out all the possibilities to exploit symmetries in detail using the example of the symmetric group $\mathcal{S}_n$.

We use the classical construction of the irreducible representations of the group $\mathcal{S}_n$ due to Wilhelm Specht [Spe37], which we generalize to our needs. Using the resulting *Specht polynomials* we show that the symmetry–adapted moment–relaxation can be specified very explicitly (Theorem 5.5). This provides the tools for some explicitly stated open issues in the study of unconstrained optimization of symmetric polynomials in Gatermann and Parrilo [GP04] (p. 124) (who – mentioning the lack of explicit formulas for the isotypic components – refer to the study of examples and asymptotics). By means of the combinatorics of the *irreducible representations* of the group $\mathcal{S}_n$, the so-called Specht modules, we can deduce a degree principle for the symmetry–adapted moment relaxation in the case of the group $\mathcal{S}_n$: The size of the resulting matrices and thus the complexity of the calculations in this case depends only on the degree of the relaxation (Theorem 5.7).

As a direct consequence of the symmetry–adapted moment relaxation we can specify in the dual viewpoint concrete representations for symmetric sums of squares (Theorem 5.10). In particular, we can characterize positive $\mathcal{S}_n$-invariant forms in the three Hilbert cases ($n = 1, d = 2,$ and $(n, d) = (3, 4)$) (Corollary 5.11, 5.12, 5.13).

Furthermore, we show that the Degree Principle can be applied profitably to exploit symmetries in the context of SDP–relaxations. To this end we study how to define a relaxation scheme based on this principle. This scheme will approximate the symmetrical polynomial optimization problem in n variables of degree d by a family of Lasserre-type relaxations in d variables. We show that under the general conditions on the polynomial

optimization problem (Putinar's condition) this scheme also provides a sequence of approximations that converge to the optimum (Theorem 5.14). In addition, we can prove the finite convergence of this scheme in some cases (Theorem 5.16).

Although in the general case of symmetric polynomials of degree 4 it is not necessarily true that positive polynomials can be represented as a sum of squares, we show in Theorem 5.17 that we can transform the question of positivity into a question of a sum of squares representation in this case.

Furthermore, we show how the approach of the orbit space can be fruitfully used in a special class of symmetric powersum–problems. The class studied here generalizes a problem that was investigated by Brandenberg and Theobald [BT06]. We show that in this case our approach to relaxation in the orbit space can be used to deduce both upper and lower bounds for problems of this type which can be calculated easily (Theorems 5.21 and 5.22).

SDP based bounds for generalized Hamming distances

To a large extent the initial applications of semidefinite optimization come from combinatorial optimization (for example [Lov79]). By means of a question coming from combinatorics of codes we show how the rich symmetry of this problem can be used to our benefit to make concrete calculations possible.

In the theory of binary codes mainly the so-called *Hamming distance* $d_H(x, y)$ is studied. For two elements $x, y \in \mathbb{F}_2^n$ it is defined as

$$d_H(x, y) = \#\{x_i \neq y_i\}.$$

In the 1970s Delsarte [Del73] was able to provide an approach to estimating the size of codes with given minimum distance, which is based on the solution of linear programs. A few years later Schrijver [Sch79], and independently McEliece, Rode, and Rumsey [MRR78] provided a link between Delsarte's LP method and a symmetrization of the graph parameter ϑ defined by Lovász, which is defined as the solution of an SDP. In recent years this relationship has led to new SDP–based bounds for codes with a given Hamming distance [Sch05a, Lau07b, Gij05, GMS10].

In this thesis we provide SDP–based bounds for the size of codes, which depend on so-called pseudo-distances. In contrast to the Hamming distance, which is defined for pairs of points, such pseudo-distances are defined for general k-tuples of points. An example of such a pseudo-distance which will be used to provide numerical results for our method is the *generalized Hamming distance*. This was first defined by Cohen, Litsyn, and Zémor [CLZ94] and goes back to works of Ozarow and Wyner [OW84] in the context of practical applications.

Our method to obtain SDP–based bounds in this case follows the idea initiated by Schrijver in [Sch05a] for triples and generalizes the parameter ϑ' to hypergraphs. A key feature of

our approach is that we can make use of the high symmetry of the *Hamming cube* to simplify the resulting SDPs. Only with this simplifications it is possible to solve the resulting programs numerically.

Structure of this thesis

This thesis is structured as follows: The first chapter gives an introduction to semidefinite and polynomial optimization. First, we give a brief introduction to the theory of semidefinite programs and limit ourselves to the aspects necessary in this thesis. In this context, we also define the parameter ϑ. We then expose how Hilbert's characterization of positive polynomials as sums of squares leads to the developement of the SDP–based approach to polynomial optimization.

The second chapter provides a brief introduction to the modern mathematical view point on symmetry. In particular, we deal with representation and invariant theory. In both cases we restrict ourselves to the case of finite groups. We start with linear representation theory, in particular, where especially Schur's lemma will be important. We then point out how representation theory can be used in the context of semidefinite programming as an important tool to reduce the computational complexity. We expose the connection of the representation theory of the symmetric group $\mathcal{S}_n$ to combinatorial objects and finally complete the overview with a summary of invariant theory.

In the third chapter of the thesis we investigate in more detail how the invariance of a polynomial optimization problem under a finite group can be explored in the context of SDP-relaxations and provide two approaches: On the one hand, we discuss how symmetry can be exploited in the context of the moment problem using linear representation theory. Here we develop a symmetry–adapted relaxation scheme. On the other hand, we also point out how invariant theory can be directly used profitably at the level of the polynomial formulation of the optimization problem.

In the fourth chapter, we deal with the issue of positivity of symmetric polynomials. We consider a generalization of a result by Vlad Timofte. We show how this generalization leads to a question about real roots of univariate polynomials and get a new elementary proof for both the Degree and the Half-Degree-Principle in this way.

The fifth chapter is used to study the techniques introduced for exploiting symmetry using the example of the symmetric group $\mathcal{S}_n$ in more detail. In order to deduce a precise description of the symmetry–adapted relaxation of a (POP) in this setting, we translate the classical representation theory of the group $\mathcal{S}_n$ into this context. This puts us in a position to further illuminate the situation in the case of $\mathcal{S}_n$-invariant POPs more precisely and also receive representations for positive symmetric polynomials in the so-called Hilbert cases. Then we show how to define a relaxation scheme by means of the Degree Principles. Finally, we study the orbit space approach in an example of power sums optimization.

In the sixth chapter we develop SDP–based bounds to a combinatorial problem coming

from coding theory. We briefly explain the relationship between the method of Delsarte and the SDP parameter ϑ. Then we show how a generalization of this parameter can be used to define SDP based bounds for generalized pseudo–distances. We then show how to use the rich symmetry of the Hamming cube to transform resulting otherwise intractable SDPs in numerical treatable SDPs of smaller size. Finally, we briefly discuss relations of our approach to other methods and provide numerical results.

The research presented in this dissertation is partially based on work with several co-authors:

The article [RT08] was used as ground for chapter one. Chapters two and five are based on work initiated in [JLRT06]. The main part of chapter four is based on [Rie10]. The connection to a theorem of Foregger and related questions are discussed in [KKR11]. Chapter six is presenting joint work with Christine Bachoc [BR11a]. In chapter seven we present a conjecture on the geometry of the cone of positive symmetric polynomials. Very recently this conjecture has been confirmed for the quartic case in [BR11b]. The thesis aims to relate the work presented in the mentioned articles and present it in a combined setting.

Contents

1

SDP and polynomial optimization

> Dieser Umstand führte Minkowski zum ersten Mal zu der Erkenntnis, daß überhaupt der Begriff des konvexen Körpers ein fundamentaler Begriff in unserer Wissenschaft ist und zu deren fruchtbarsten Forschungsmitteln gehört
>
> *Nachruf auf Hermann Minkowski*
> David Hilbert

Let $\mathbb{R}[X] := \mathbb{R}[X_1, \ldots, X_n]$ denote the ring of real polynomials and consider polynomials $f, g_1, \ldots, g_m \in \mathbb{R}[X]$. Solving polynomial optimization problems of the form minimize $f(x)$ where x is constrained to lie in a semialgebraic set

$$K := \{x \in \mathbb{R}^n \,:\, g_1(x) \geq 0, \ldots, g_m(x) \geq 0\}$$

is known to be a hard task in general. In recent years however, the interplay of semidefinite programming and algebraic geometry has led to new paradigms for solving or approximating these types of hard optimization problems. The key to these new paradigms consists in taking a view point in which the originally non–convex problem is reformulated in a convex structure. This convex structure then can be used to design semidefinite relaxations. In the first section of the present chapter we will present the basic ideas of semidefinite programs. In the second section we will show how the classical results on sums of squares representations for positive polynomials and moments of probability measures can be used to generate a SDP relaxation scheme that will provide naturally a converging sequence of lower bounds for the initial problem.

1.1 Semidefinite programming

1.1.1 From LP to SDP

Semidefinite programming (SDP) evolved in the 1970s as a natural generalization of linear programming (LP). In both optimization paradigms one asks to minimize or maximize a linear function under additional constraints. In the classical case of LP the constraints are given by linear inequalities. Therefore an LP can be described by the following normal form:

$$\begin{array}{lrcl} \inf & c^T x & & \\ \text{s.t.} & Ax & = & b\,, \\ & x & \geq & 0 \qquad (x \in \mathbb{R}^n), \end{array} \tag{1.1}$$

where $A \in \mathbb{R}^{m\times n}$ and $c \in \mathbb{R}^n$, $b \in \mathbb{R}^m$.

The feasible set given by the constraints is in this case a convex polyhedron

$$P := \{x \in \mathbb{R}^n \,:\, Ax = b,\ x \geq 0\}\,.$$

Although algorithmic approaches for solving such special cases of constraint optimization problems can be traced back to Fourier, it was George Danzig who introduced the *Simplex Algorithm* as a method to solve LPs in the late 1940's. His algorithm and the use of LPs in real life problems initiated a wave of intense research on linear optimization. Whereas the complexity of the Simplex algorithm is still an open field of research, LPs can in practice be solved very efficiently with the Simplex method.

Besides the Simplex method, which is still today the major method used by most industrial applications of LP, other possibilities for solving linear programs have been proposed. A major theoretical result was obtained by Khachiyan [Kha79] in 1979. He was able to show that the *Ellipsoid algorithm*, which was proposed by N.Z. Shor in 1972 can be used to solve LPs with rational input data in polynomial time. However, in practice this algorithm does not seem to be convenient. Only five years later, in 1984, Karmarkar [Kar84] introduced the so called *interior point method*. With this technique it is possible to solve a linear optimization problem with rational input data in $O(\sqrt{n}\log(1/\varepsilon))$ arithmetic steps up to a prescribed accuracy $\varepsilon > 0$. In contrast to the ellipsoid algorithms, interior point methods can be implemented quite efficiently. So using interior point methods a linear program with rational input data is solvable in polynomial time.

Von Neumann already seems to have seen the fact that taking a dual view on a linear program can be profitable. To every LP in the normal form (1.1) we can define the *dual program* to be

$$\begin{array}{lrcl} \sup & b^T y & & \\ \text{s.t.} & A^T y + s & = & c\,, \\ & s & \geq & 0\,. \end{array} \tag{1.2}$$

The primal and dual linear programs we associated to each other with this duality are connected by the so called *weak duality* and *strong duality* for linear programs. The first of these guarantees that the objective value of any feasible solution of the dual already gives a lower bound for the primal. The second states that if we have an optimal value of one of both programs, this values (if finite) agrees with the optimal value of the other.

Besides the applications of LP in industrial and military application for which LP initially was designed, combinatorial questions were also solved with linear programming methods. In this spirit *semidefinite programming* (SDP) was first discussed as a generalization of LP. The basic idea of an SDP is to replace the linear condition $x \geq 0$ on the vector $x \in \mathbb{R}^n$ by a positivity condition on a matrix variable $X \in \mathbb{R}^{n \times n}$.

We first give some notation: The set of all real symmetric $n \times n$ matrices is denoted with $\mathrm{Sym}_n(\mathbb{R})$. A matrix $A \in \mathrm{Sym}_n(\mathbb{R})$ is called *positive semidefinite* if $x^t A x \geq 0$ for all $x \in \mathbb{R}^n$. The set of all positive semidefinite matrices is denoted by $\mathrm{Sym}_n^+(\mathbb{R})$. If in fact $x^t A x > 0$ holds for all $x \in \mathbb{R}^n \setminus \{0\}$ we say that A is *positive definite* and we write $\mathrm{Sym}_n^{++}(\mathbb{R})$ for the set of all positive definite matrices. The following theorem gives some equivalent conditions for positive semidefiniteness of a matrix $A \in \mathrm{Sym}_n(\mathbb{R})$:

Theorem 1.1
Let $A \in \mathrm{Sym}_n(\mathbb{R})$. Then the following are equivalent

1. *$A \in \mathrm{Sym}_n^+(\mathbb{R})$.*
2. *$x^t A x \geq 0$ for all $x \in \mathbb{R}^n$.*
3. *All eigenvalues of A are nonnegative.*
4. *There is a unique lower triangular matrix $L \in \mathbb{R}^{n \times n}$ with $L_{jj} > 0$ for all j such that $LL^T = A$.*
5. *All principal minors of A are nonnegative.*

The fourth of the above equivalent conditions, which guarantees that we can define a real "square root" of any positive semidefinite matrix is also called *Cholesky–decomposition.*

We also remark the following useful characterization of semidefiniteness.

Theorem 1.2 (Schur complement)
Suppose $M \in \mathrm{Sym}_n(\mathbb{R})$ is given as

$$M = \begin{pmatrix} A & B \\ B^T & C \end{pmatrix}$$

with A in $\mathrm{Sym}_n^{++}(\mathbb{R})$ and C in $\mathrm{Sym}_n(\mathbb{R})$. Then we have that M is positive (semi-)definite if and only if $C - B^T A^{-1} B$ is positive (semi-)definite.

The matrix $C - B^T A^{-1} B$ in the above theorem is called the *Schur complement of A in M*.

In order to define a linear function on $\mathrm{Sym}_n(\mathbb{R})$ we will use the following scalar product.

Definition 1.3
Let $A, B \in \mathrm{Sym}_n(\mathbb{R})$ then we define $\langle A, B\rangle := \mathrm{Tr}(A \cdot B)$

Let $C, A_1, \ldots, A_m \in \mathrm{Sym}_n(\mathbb{R})$. Then with the notations from above we define the normal form of a *semidefinite program (SDP)* to be the following:

$$\begin{array}{lrcl} \inf \langle C, X\rangle & & & \\ \text{s.t.} & \langle A_i, X\rangle & = & b_i\,, \quad 1 \le i \le m\,, \\ & X & \succeq & 0, \text{ where } X \in \mathrm{Sym}_n(\mathbb{R})\,. \end{array}$$

Again as in the case of linear programming the *feasible set*

$$S := \{X \in \mathrm{Sym}_n(\mathbb{R}) \,:\, \langle A_i, X\rangle = b_i\,, 1 \le i \le m\,,\, X \succeq 0\}$$

is a convex set. In analogy to the polyhedra in the LP case the convex sets that can be represented with SDP constraints are called *spectrahedra*. In recent years the interior point methods which were originally proposed for linear programming were extended to semidefinite programming and provide algorithmic efficient methods for solving SDPs.

1.1.2 Duality in SDPs

Just like in the linear programming case we have an associated duality theory for semidefinite programming. Let $C, A_1, \ldots, A_m \in \mathrm{Sym}_n(\mathbb{R})$ and $b \in \mathbb{R}^m$ define an SDP in the normal form above. The *dual problem* to the normal form above is defined as

$$\begin{array}{ll} & \sup\, b^t y \\ \text{s.t.} & y \in \mathbb{R}^m, \quad C - \sum_{i=1}^m A_i y_i \succeq 0, \end{array}$$

where $y \in \mathbb{R}^m$ is the decision variable.

The main interest in duality again comes from the relation of optimal values for the primal and the dual. Again we have that one can be used to bound the other:

Theorem 1.4 (Weak Duality)
Let X be primally feasible and y be dually feasible, then we have

$$\langle C, X\rangle \ge b^t y.$$

Proof. The proof just follows by carefully inspecting the difference $\langle C, X\rangle - b^t y$. We have

$$\langle C, X\rangle - b^t y = \langle C - \sum_{i=1}^{m} A_i y_i, X\rangle \geq 0. \quad \square$$

Nevertheless, strong duality will not always hold as the following example shows.

Example 1.5
Consider the following SDP:

$$\begin{array}{l} \inf x_1 \\ \text{s.t.} \begin{pmatrix} 0 & x_1 & 0 \\ x_1 & x_2 & 0 \\ 0 & 0 & x_1 - 1 \end{pmatrix} \succeq \quad 0 \quad . \end{array}$$

By examining the positive semidefinite condition one finds that the spectrahedron that defines the feasible set is in fact given by $\{(x_1, x_2) \in \mathbb{R}^2 \,:\, x_1 = 0, x_2 \geq 0\}$. Hence we get the optimal values for the objective function to be 0. Now if one considers the corresponding dual we get:

$$\begin{array}{l} \sup -y_2 \\ \text{s.t.} \begin{pmatrix} y_1 & (1-y_2)/2 & 0 \\ (1-y_2)/2 & 0 & 0 \\ 0 & 0 & y_2 \end{pmatrix} \succeq \quad 0. \end{array}$$

In the dual case the feasible set is given by $\{(y_1, y_2) \in \mathbb{R}^2 \,:\, y_1 \geq 0, y_2 = 1\}$. Therefore we get an optimal value of -1.

So, in general we cannot expect that strong duality also holds. The following definition will provide an additional assumption necessary to ensure a strong duality.

Definition 1.6
An SDP problem in canonical form is *strictly feasible* if the spectrahedron

$$\{X \in \mathrm{Sym}_n(\mathbb{R}) \,:\, \langle A_i, X\rangle = b_i\,, 1 \leq i \leq m\,, \text{ and } X \succeq 0\}$$

contains a positive definite point $X \in \mathrm{Sym}_n^{++}(\mathbb{R})$.

Now, if we have strict feasibility of an SDP we can expect strong duality:

Theorem 1.7 (Strong Duality)
Let (P) and (D) denote a pair of dual semidefinite programs and let p^* respectively d^* denote the optimal values of (P) respectively (D). If p^* is finite and (P) strictly feasible then we have that also the dual problem is feasible and moreover the optimal values p^* and d^* agree.

1.1.3 Lovász ϑ–number

In this section we want to establish an example that shows some links between the semidefinite programming and combinatorial problems. As already mentioned in the previous section these links bear the roots of semidefinite programs.

A fundamental object in combinatorics is the notion of a graph. Let V be a finite set of *vertices* and define the *edges* as a finite set of pairs $E \subset V \times V$. A graph $\Gamma = (V, E)$ is a set of vertices with corresponding edges. An *independent set* in a graph $\Gamma = (V, E)$ is a set of vertices such that no edge in E connects any pair of vertices in the independent set. The *maximal size of an independent set* in a graph Γ is denoted by $\alpha(\Gamma)$. The *chromatic number* $\chi(\Gamma)$ is the minimum number of colors that are needed to color the vertices in such a way that no two connected vertices have the same color. In other words it is a minimal partition of the vertex set into independence sets. The problem to calculate $\alpha(\Gamma)$ or $\chi(\Gamma)$ for an arbitrary graph is an NP-hard problem (see for example [Law76]).

In his seminal paper [Lov79] Lovász introduced a parameter $\vartheta(\Gamma)$ as the solution to a semidefinite program to bound the parameters $\alpha(\Gamma)$ and $\chi(\Gamma)$.

Let $V = \{v_1, \ldots, v_n\}$ and $S \subset V$ any independent vertex set. We consider the characteristic function $\mathbb{1}_S$ of S and construct the function $F_S : V \times V \to \mathbb{R}$ defined by

$$F_S(v_i, v_j) := \frac{1}{|S|}\, \mathbb{1}_S(v_i)\, \mathbb{1}_S(v_j).$$

This function F_S is positive semidefinite, i.e., the $n \times n$ matrix M indexed by V, with coefficients $M_{i,j} := F_S(v_i, v_j)$, is positive semidefinite.

Further by the definition of M it is clear that we have $M \in \mathrm{Sym}_n(\mathbb{R})$. As $\mathbb{1}_S$ is the characteristic function of S and the set S contains by its definition only vertices that do not share an edge the following three properties of the matrix M also hold:

1. $M_{i,j} = 0$ if $\{v_i, v_j\} \in E$,
2. $\sum_{i=1}^{n} M_{i,i} = 1$,
3. $\sum_{i,j=1}^{n} M_{i,j} = |S|$.

Keeping the above properties of M in mind, we define the theta number with the following program:

Definition 1.8
The theta number of the graph $\Gamma = (V, E)$ with $V = \{v_1, v_2, \ldots, v_n\}$ is

$$\begin{aligned} \vartheta(\Gamma) \quad = \max \Big\{ \textstyle\sum_{i,j} B_{i,j} : \quad & B \in \mathbb{R}^{n\times n},\ B \succeq 0 \\ & \textstyle\sum_i B_{i,i} = 1, \\ & B_{i,j} = 0 \quad (i,j) \in E \Big\}. \end{aligned} \tag{1.3}$$

The dual program for ϑ is defined as:

$$\begin{aligned} \vartheta(\Gamma) \quad = \min \big\{ \quad t: \quad & B \succeq 0 \\ & B_{i,i} = t-1, \\ & B_{i,j} = -1 \quad (i,j) \notin E \big\}. \end{aligned} \tag{1.4}$$

Notice that as (1.3) is strictly feasible by strong duality the two definitions will provide the same value.

Given a graph Γ, its complementary graph $\overline{\Gamma}$ is defined by switching edges and non-edges. Using these definitions, Lovász could show the following remarkable bounds on the graph parameters introduced above.

Theorem 1.9 (Sandwich theorem)

$$\alpha(\Gamma) \leq \vartheta(\Gamma) \leq \chi(\overline{\Gamma})$$

Proof. The first inequality follows directly from the properties of M defined above.

For the second inequality, consider a coloring of $\overline{\Gamma}$. This coloring defines a function $c : V \to \{1, \ldots, k\}$. Using this function we define the matrix C with $C_{i,j} = -1$ if $c(i) \neq c(j)$, $C_{i,i} = k-1$ and $C_{i,j} = 0$ otherwise. The so defined matrix C provides a feasible solution of (1.4) and thus $\vartheta(\Gamma) \leq \chi(\overline{\Gamma})$. □

As the ϑ-number is defined as the optimal solution of a semidefinite program it is easier to calculate and provides by the above theorem an approximation of graph-invariants that are otherwise hard to compute. Beginning with Lovász's work many other SDP–relaxations of hard problems have been proposed in graph theory and in other domains, so Lovász's remarkable result can be seen as the root of a long list of applications of semidefinite programming.

1.2 Optimization and real algebraic geometry

Finding the optimal value of a polynomial function under additional polynomial constraints is a problem that arises naturally in many applications. In this section we will outline the recent research on how the relation of optimization problems of the form

$$\begin{aligned} p^* \quad = \quad & \inf p(x) \\ & \text{s.t. } g_1(x) \geq 0, \ldots, g_m(x) \geq 0\,, \end{aligned} \tag{1.5}$$

with classical questions of sums of squares decompositions of positive polynomials provides methods to generate a sequence of relaxations that converge to the solution. First we will study the particular case of global optimization and then use the dual viewpoint in order to show how general polynomial optimization problems can be attacked.

1.2.1 Global optimization and sums of squares

In the case of a global optimization the polynomial problem (1.5) specializes to finding the minimum of a real polynomial function i.e.,

$$\inf_{x\in\mathbb{R}^n} f(x). \tag{1.6}$$

Now we consider the set

$$\mathcal{P}_n := \{f \in \mathbb{R}[X], \text{ such that } f(x) \geq 0 \, \forall x \in \mathbb{R}^n\}.$$

Further we denote $\mathcal{P}_{n,d}$ the elements in $\mathcal{P}$ of degree d.

As we find that for all $\lambda, \gamma \geq 0$ and $p, q \in \mathcal{P}_n$ (in $\mathcal{P}_{n,d}$) the polynomial $\lambda p + \gamma q$ is again in $\mathcal{P}_n$ (in $\mathcal{P}_{n,d}$) we can conclude that $\mathcal{P}_n$ and $\mathcal{P}_{n,d}$ are in fact convex cones. With this observation in mind we can transfer the initial global optimization problem (1.6) into the framework of convex optimization by a simple but effective change of view:

$$\sup_{f-\lambda\in\mathcal{P}_n} \lambda. \tag{1.7}$$

This new formulation as a convex problem in an infinite dimensional vector space is in general as hard to handle as the original problem. However, it provides a powerful way of relaxing the original problem based on the following definition.

Definition 1.10
We say that a polynomial $p \in \mathbb{R}[X]$ is a *sum of squares (SOS)* if there are polynomials $q_1, \ldots, q_m \in \mathbb{R}[X]$ such that $p = \sum_{i=1}^{m} q_i^2$. The set of all sums of squares of given degree d in n variables will be denoted by $\Sigma_{n,d}$. Further we will denote Σ_n as the set of all sums of squares in n variables.

From an algorithmic point of view sums of squares are easier to handle than positive polynomials. Powers and Wörmann [PW98] showed that using the Gram Matrix method one can decide wether a given polynomial is a sum of squares with the help of semidefinite programs.

In order to present how the connection from sums of squares to SDPs is established, let $p \in \mathbb{R}[X]$ be of even degree $2d$ and let Y denote the vector of all monomials in the variables $X_1, \ldots, X_n$ of degree at most d; so the vector Y consists of $\binom{n+d}{d}$ components. Every polynomial $s = s(X)$ of degree d is uniquely determined by its coefficient relative to Y and p decomposes into a form

$$p = \sum_j (s_j(X))^2 \quad \text{with polynomials } s_j \text{ of degree at most } d$$

if and only if we have that with the coefficient vectors s_j of the polynomials $s_j(X)$ we find

$$p \;=\; Y^T\big(\sum_j s_j s_j^T\big)Y\,.$$

With the Cholesky–decomposition (see Theorem 1.1) this holds exactly if and only if the matrix $Q := \sum_j s_j s_j^T$ is positive semidefinite. So the existence of a sums of squares decomposition of p follows by providing a feasible solution to a semidefinite program, i.e we have

Lemma 1.11
A polynomial $p \in \mathbb{R}[X]$ of degree $2d$ is a sum of squares, if there is a positive semidefinite matrix Q with

$$p \;=\; Y^T Q Y.$$

With this observation in mind the following problem can be solved using semidefinite programs:

$$\max_{p-\lambda\in\Sigma_{n,d}} \lambda. \tag{1.8}$$

As obviously every $p \in \Sigma_n$ is positive and hence $\Sigma_n \subset \mathcal{P}_n$, it is clear that a solution of (1.8) gives an upper bound for the problem (1.7). In view of the implications of this inclusion it is natural to ask if also the converse might be true.

This question of how to characterize the cone of positive polynomials in terms of sums of squares of polynomials is in fact a classical one. It goes back to Hilbert and Minkowski. The latter had to defend his thesis at the University of Königsberg. His opponent in this public defense was Hilbert. Among other questions related to quadratic forms, Minkowski was asked if all positive polynomials were in fact a sum of squares of polynomials. It is interesting to note, that in the case of univariate polynomials this is true, as stated in the following theorem.

Theorem 1.12
Let $f \in \mathbb{R}[t]$ be a univariate polynomial. Then we have $f(t) \geq 0$ for all $t \in \mathbb{R}$ if and only if $p \in \Sigma_1$.

Proof. As f has only real coefficients over $\mathbb{C}$ we have a factorization in the form $f = q\bar{q}$ where $q = q_1 + iq_2$ and $\bar{q} = q_1 - iq_2$ for some real polynomials q_1, q_2. From this factorization we deduce that $f = q_1^2 + q_2^2$ □

During his defense Minkowski argued that for any arbitrary number of variables it should no longer be true that the two cones of positive polynomials and SOS-polynomials coincide. However, his arguments were not precise. Motivated by Minkowski's argumentation Hilbert began to investigate this problem. In his seminal paper of 1888 [Hil88] he was able

to derive the following beautiful characterization of all cases in which positive polynomials are sums of squares.

Theorem 1.13 (Hilbert)
We have equality in the inclusion $\Sigma_{n,d} \subseteq \mathcal{P}_{n,d}$ exactly in the following three cases:

1. *The univariate case $n = 1$.*
2. *The quadratic case $d = 2$.*
3. *The case $n = 2, d = 4$.*

That positivity coincides with the sums of squares property in the univariate case was already explained in the above theorem. Further the second statement follows from Cholesky–decomposition of every positive semidefinite quadratic form. The proof of the third case is far from being obvious so we will not include it here (for a reference see [PRSS04, Sch10] and [PS10] for an elementary proof).

However, it is even more surprising that the characterization in Hilbert's statement above really covers all cases. Hilbert's original proof for the fact that the inclusion is strict in the other cases was not constructive at all. He was able to show the existence of positive polynomials that are not sums of squares by observing that polynomials of degree d satisfy linear relations, known as the Cayley–Bacharach relations, which are not satisfied by polynomials of full degree $2d$. It took until the 1960s until the first concrete counter example showing the strict inclusion was given by Motzkin.

Theorem 1.14
The Motzkin Polynomial

$$X^4Y^2 + X^2Y^4 - 3X^2Y^2 + 1$$

is positive but not a sum of squares.

After Motzkin's initial example more positive polynomials that are not sums of squares were constructed. In particular Bosse [Bos07] was able to construct many examples of two dimensional polynomials that are positive but not sums of squares. Very recently Blekherman [Ble10] could provide a geometrical construction of faces of the sums of squares cone $\Sigma_{n,d}$ that are not faces of the cone $\mathcal{P}_n$.

Despite the negative result that in general a positive polynomial is not always a sums of squares of polynomials Hilbert could later show that every bivariate nonnegative polynomial is a sums of squares of rational functions. In his list of 23 problems he then asked if this is true in general, i.e., if every nonnegative polynomial could be represented as sum of squares of rational functions. This 17th of Hilbert's problems very much initiated the development of modern real algebraic geometry and was solved by Emil Artin in 1927. Artin could establish the following fundamental characterization of positive polynomials:

Theorem 1.15
Let $p \in \mathbb{R}[X]$ such that $p(x) \geq 0$ for all $x \in \mathbb{R}^n$. Then there are rational functions $q_1, \ldots, q_m \in \mathbb{R}(X)$ such that $p = \sum_{i=1}^{m} q_i^2$.

Although this beautiful statement relates positive polynomials to sums of squares, the fact that rational functions need to be considered makes it a priori hard to use an approach similar to (1.8) based on this characterization as there is no bound on the degrees of the denominators needed in the representation of a positive polynomial as sums of squares of rational functions.

1.2.2 Positivstellensätze

In contrast to algebraic geometry over algebraically closed fields such as the complex numbers, real algebraic geometry is concerned with the problem of finding real solutions to systems of polynomial (in-)equalities.

A set $K \subset \mathbb{R}^n$ is called a *basic closed semialgebraic set* if it can be described as the set of solutions in the form

$$K = \{x \in \mathbb{R}^n \,:\, g_1(x) \geq 0, \ldots, g_m(x) \geq 0\},$$

where $g_i \in \mathbb{R}[X]$, and *basic open semialgebraic set* if all inequalities above are replaced by strict inequalities (i.e., $g_i(x) > 0$).

In general the term *semialgebraic set* is used for the finite union of basic sets. A fundamental question in this setting is to decide, if a given semialgebraic set is empty or not. In classical algebraic geometry the corresponding question on systems of equations can be decided using a fundamental result due to Hilbert:

For $f_1, \ldots, f_k \in \mathbb{C}[X]$ we denote by $\mathcal{I}(f_1, \ldots, f_k)$ the ideal generated by $f_1, \ldots, f_k$. In this setting Hilbert established the following characterization of the cases when the variety $V(\mathcal{I}(f_1, \ldots, f_k))$, i.e., the common set of zeros of all polynomials in $\mathcal{I}(f_1, \ldots, f_k)$, is empty.

Theorem 1.16 (Hilbert's Nullstellensatz)
The following two are equivalent:

1. *The set $\{x \in \mathbb{C}^n \,:\, f_i(x) = 0 \text{ for } 1 \leq i \leq k\}$ is empty.*
2. *$1 \in \mathcal{I}(f_1, \ldots, f_k)$.*

The remarkable consequence of Hilbert's Nullstellensatz is that it gives an explicit *algebraic certificate* of the emptiness of any algebraic set:

Indeed, if one can find any polynomials $g_1, \ldots, g_k$ such that

$$1 = f_1 g_1 + \ldots + f_k g_k$$

this relation provides that

$$\{x \in \mathbb{C}^n \,:\, f_1(x) = \cdots = f_k(x) = 0\} \text{ is empty.}$$

While the criterion of Hilbert's Nullstellensatz is of course also sufficient if one is interested in the emptiness of real semialgebraic sets it is not necessary. For example every quadratic polynomial of the form $ax^2 + bx + c$ poses two complex roots. Yet, only when the discriminant $D = b^2 - 4ac$ is nonnegative we will find real roots. This easy example already suggests that the situation with semialgebraic sets is more delicate. After Hilbert's fundamental result in algebraic geometry it took until the 1960 until Krivine and Stengle could provide an analogue of Hilbert's Nullstellensatz for the semialgebraic setting. The name *Positivstellensatz* is used for this statement to signify the connection to Hilbert's Nullstellensatz. We will need the following definitions in order to state the Positivstellensatz:

Definition 1.17
For $f_1, \ldots, f_k \in \mathbb{R}[X]$ the *algebraic cone* generated by $g_1, \ldots, g_k$ is defined as

$$\mathcal{A}(f_1, \ldots, f_k) \;=\; \left\{ p \in \mathbb{R}[X] \,:\, p = \sum_{I \subseteq \{1,\ldots,n\}} s_I \prod_{i \in I} g_i \right\}$$

with polynomials $s_I \in \Sigma_n$.

Moreover we define the *multiplicative monoid* as

$$\mathcal{M}(f_1, \ldots, f_k) := \left\{ \prod_{i=1}^{r} g_i \,:\, g_i \in \{f_1, \ldots, f_k\}\,,\, r \in \mathbb{N} \right\}.$$

With these notations defined we are ready to state the Positivstellensatz due to Stengle [Ste73]:

Theorem 1.18 (Positivstellensatz)
Let $f_1, \ldots, f_k, g_1, \ldots, g_s, h_1, \ldots, h_l \in \mathbb{R}[X]$. Then the following are equivalent:

1. *The set*
$$K := \{x \in \mathbb{R}^n \,:\, f_i(x) \geq 0, g_j(x) \neq 0, h_t(x) = 0 \,\forall i, j, t\}$$
is empty.
2. *There are polynomials $F \in \mathcal{A}(f_1, \ldots, f_k), G \in \mathcal{M}(g_1, \ldots, g_s)$ and $H \in \mathcal{I}(h_1, \ldots, h_l)$ such that*
$$F + G^2 + H = 0.$$

With this statement at hand let us reexamine the case of the quadratic polynomial $x^2 + bx + c$ and assume that $D = b^2 - 4c < 0$. We now define the polynomials

$$F := 1, \quad G := \frac{X + \frac{b}{2}}{\sqrt{c - \frac{b^2}{4}}}, \text{ and } \quad H := \frac{-(X^2 + bX + c)}{c - \frac{b^2}{4}}$$

and see that the relation $F + G^2 + H = 0$ is satisfied.

The Positivstellensatz can already be used in a suitable way for finding the optima of a real valued polynomial over a semialgebraic set K. For this purpose we note the following corollary:

Corollary 1.19
Let $K := \{x \in \mathbb{R}^n : g_1(x) \geq 0, \ldots g_m(x) \geq 0\}$. Then $f \in \mathbb{R}[X]$ is nonnegative on K, i.e., $f(x) \geq 0 \, \forall x \in K$ if there is $k \in \mathbb{N}$ and $F \in \mathcal{A}(-f, g_1, \ldots, g_m)$ with $F + f^{2k} = 0$.

With the above corollary minimizing a polynomial f on the set K translates therefore into the task to determine the largest real λ such that the polynomial $f - \lambda$ has such a certificate. The main concern with this statement is that it does not provide any possibility to control the degrees of the polynomials involved. This in turn makes it hard to find them algorithmically.

Hence it is necessary to add further refinements to the assumptions in order to make it algorithmically possible to link semidefinite programming techniques with positivity. The first of these additional assumptions is that K is a compact set. In the setting of compact sets Schmüdgen [Sch91] was able to show the following result:

Theorem 1.20 (Schmüdgen)
Let $K := \{x \in \mathbb{R}^n : g_1(x) \geq 0, \ldots g_k(x) \geq 0\}$ be a compact set and f be a polynomial that is positive on K. Then $f \in \mathcal{A}(g_1, \ldots, g_k)$.

So with the additional hypotheses that K is compact Schmüdgen's characterization gives already a wide simplification to the Positivstellensatz of Stengle. For the purpose of the semidefinite relaxation a further assumption will provide a version which is more suitable for optimization purposes. This was first observed by Putinar [Put93] who proved that by assuming in addition to the compactness of K a further constraint directly on the polynomials that define K, it is possible to derive a tighter characterization for polynomials that are strictly positive on K.

Definition 1.21
Given polynomials $g_1, \ldots, g_m \in \mathbb{R}[X]$ the *quadratic module* generated by $g_1, \ldots, g_m$ is defined as

$$\mathrm{QM}(g_1, \ldots, g_m) := \{s_0 + s_1 g_1 + \cdots + s_m g_m : s_0, \ldots, s_m \in \Sigma_n\}$$

A quadratic module $\mathrm{QM}(g_1, \ldots, g_m)$ is called *archimedean* if

$$N - \sum_{i=1}^{n} x_i^2 \in \mathrm{QM}(g_1, \ldots, g_m)$$

for some $N \in \mathbb{N}$.

Theorem 1.22 (Putinar's Positvstellensatz)
Let $K := \{x \in \mathbb{R}^n : g_1(x) \geq 0, \ldots, g_k(x) \geq 0\}$ be a compact set and assume that the corresponding quadratic module $\mathrm{QM}(g_1, \ldots, g_m)$ is archimedean. Then every polynomial p that is strictly positive on K – i.e., $p(x) > 0$ holds for all $x \in K$ – is in $\mathrm{QM}(g_1, \ldots, g_m)$ and has therefore a representation of the form

$$p \;=\; s_0 + s_1 g_1 + \cdots + s_m g_m \tag{1.9}$$

with $s_0, \ldots, s_m \in \Sigma$.

The archimedean condition seems at first a bit unhandy. In the following theorem due to Schmüdgen [Sch91] we collect equivalent conditions on when a quadratic module is archimedean.

Theorem 1.23
The following are equivalent:

1. *$\mathrm{QM}(g_1, \ldots, g_m)$ is archimedean.*
2. *There exist finitely many $t_1, \ldots, t_s \in \mathrm{QM}(g_1, \ldots, g_m)$ such that the set*

   $$\{x \in \mathbb{R}^n : t_1(x) \geq 0, \ldots, t_s(x) \geq 0\}$$

   is compact and $\prod_{i \in I} t_i \in \mathrm{QM}(g_1, \ldots, g_m)$ for all $I \subset \{1, \ldots, s\}$.
3. *There is a $p \in \mathrm{QM}(g_1, \ldots, g_m)$ such that $\{x \in \mathbb{R}^n : p(x) \geq 0\}$ is compact.*

It is interesting to note that the strict positivity of p is in general necessary for the statement in Putinar's Positivstellensatz to be true. Indeed the following elementary example shows that the statement is not correct for nonnegative polynomials.

Example 1.24
Consider the one dimensional semialgebraic set

$$K := \left\{x \in \mathbb{R} : (1 - x^2)^3 \geq 0\right\}.$$

The corresponding quadratic module $\mathrm{QM}((1 - X^2)^3)$ is archimedean as we have

$$2 - x^2 \;=\; \frac{2}{3} + \frac{4}{3}\big(X^3 - \frac{3}{2}X\big)^2 + \frac{4}{3}\big(1 - X^2\big)^3.$$

Now consider the polynomial $p(X) = 1 - X^2$. As K is in fact equal to the interval $[0, 1]$ we have $p \geq 0$ on K. Now, if we assume a representation of p in the form (1.9) we would have

$$1 - X^2 \;=\; s_0(X) + s_1(X)(1 - X^2)^3 \quad \text{with } s_0, s_1 \in \Sigma_1\,. \tag{1.10}$$

But this implies that the right hand side of (1.10) has to vanish at $x = 1$. Now, as we examine the order of the root $x = 1$ we find that on the right hand side $x = 1$ is a root of order at least 2, whereas on the left hand side p vanishes only of order 1 at $x = 1$. This clearly gives a contradiction and hence a representation in the form (1.10) is impossible.

1.2.3 Duality and the moment problem

We already explained in the context of linear and semidefinite programming that the concept of duality is fundamental if one considers optimization problems. In the case of positive polynomials the duality will provide a link to the *moment problem*. This classical problem arose within Stieltjes' creation of the analytical theory of continued fractions. Later Hamburger made it a question of its own right.

Given a sequence $y = (y_\alpha)_{\alpha \in \mathbb{N}^n}$ the *moment problem* asks to characterize the necessary and sufficient conditions that need to be posed on (y_α) to guarantee that there is a Borel measure μ with

$$y_\alpha = \int x^\alpha d\mu.$$

Let μ be a measure on $\mathbb{R}^n$. Then μ defines a linear map from $\mathbb{R}[X]$ to $\mathbb{R}$ defined as $L(f) = \int f d\mu$. We denote with $\mathcal{M}_n$ the positive hull of the $L \in \mathrm{Hom}(\mathbb{R}[X], \mathbb{R})$ which are coming from integration. With these notations defined the classical moment problem translates to characterizing the elements in $\mathcal{M}_n$. Take for example $v \in \mathbb{R}^n$ and define a linear function as evaluation at v, i.e., $L_v(f) := f(v)$. Then the corresponding measure is just the Dirac–measure supported at v.

It follows directly from the principles of integration that a linear map that comes from integration should not map positive polynomials to the negative reals. That this requirement is already enough was first proven by Haviland [Hav36]. His result characterizes all linear maps that come from integration.

Theorem 1.25 (Haviland's Theorem)
Let $L \in \mathrm{Hom}(\mathbb{R}[X], \mathbb{R})$ be a linear functional. Then the following are equivalent:

1. *There exists a Borel measure μ with $L(f) = \int f d\mu$ for all $f \in \mathbb{R}[X]$.*
2. *$L(f) \geq 0 \, \forall f \in \mathcal{P}$.*

With this in mind we will expose the connection to positive polynomials and duality. For this recall that $\mathcal{P}$ is a convex cone. To every convex cone we can associated its dual cone

defined as follows.

Definition 1.26
Let V be an $\mathbb{R}$–vector space and $K \subset V$ a cone. Then its dual cone K^* is defined

$$K^* := \{L \in \mathrm{Hom}(V, \mathbb{R}) : L(y) \geq 0, \text{ for all } y \in K\} .$$

So Haviland's Theorem in fact states that $\mathcal{P}_n^* = \mathcal{M}_n$.

We have already seen that the cone $\mathcal{P}_n$ is very hard to handle but that we could make use of the cone Σ_n (see Definition 1.10) and the inclusion $\Sigma_n \subset \mathcal{P}_n$. Also on the dual side we will profit from the corresponding dual inclusion:

Given $L \in \mathrm{Hom}(\mathbb{R}[X], \mathbb{R})$ we can associate a bilinear form $\mathcal{L}$ by

$$\begin{aligned} \mathcal{L} : \mathbb{R}[X] \times \mathbb{R}[X] &\mapsto \mathbb{R} \\ (p, q) &\mapsto L(p \cdot q). \end{aligned}$$

Now let $\mathcal{M}_n^+$ denote the positive hull of elements in $\mathrm{Hom}(\mathbb{R}[X], \mathbb{R})$ such that the corresponding bilinear form $\mathcal{L}$ is positive semidefinite. We now have

Proposition 1.27
For a linear functional $L \in \mathrm{Hom}(\mathbb{R}[X], \mathbb{R})$ we have $L(f) \geq 0$ for all $f \in \Sigma_n$ if and only if the associated bilinear from $\mathcal{L}$ is positive definite. In other words $\Sigma_n^* = \mathcal{M}_n^+$.

In particular this yields Hamburger's original solution to the 1-dimensional Moment problem:

Theorem 1.28
A sequence of real numbers $y_0, y_1, y_2, \ldots$ is a sequence of moments from a measure on the real line if and only if

$$\begin{pmatrix} y_0 & y_1 & y_2 & \cdots \\ y_1 & y_2 & y_3 & \cdots \\ y_2 & y_3 & y_4 & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

is positive semidefinite.

1.2.4 General optimization and Lasserre's method

With the duality exposed in the last section the following dual approach using the moment problem was introduced by Lasserre [Las01] in order to solve more general optimization

problems. For given $p, g_1, \ldots, g_m \in \mathbb{R}[X]$ we now consider the general optimization problem of the form

$$\inf p(x) \;\text{ subject to }\; g_1(x) \geq 0, \ldots, g_m(x) \geq 0\,.$$

Its feasible set $K \subset \mathbb{R}^n$ is the basic closed semialgebraic set

$$K := \{x \in \mathbb{R}^n \,:\, g_j(x) \geq 0, \quad j = 1, \ldots, m\}\,. \tag{1.11}$$

For reasons described below we will need the following technical assumption:

Assumption 1.29
The feasible set K defined in (1.11) is compact and there exists a polynomial $u \in \mathbb{R}[X]$ such that the sublevel set $\{x \in \mathbb{R}^n \,:\, u(x) \geq 0\}$ is compact and u has the representation

$$u \;=\; u_0 + \sum_{j=1}^{m} u_j\, g_j \tag{1.12}$$

for some sums of squares polynomials $u_0, u_1, \ldots, u_m \in \mathbb{R}[X]$.

Recall from Theorem 1.23 that this assumption in turn implies that the quadratic module generated by the polynomials $g_1, \ldots, g_m$ is in fact archimedean. Furthermore it guarantees that K is compact and therefore the infimum is attained on K.

Like in the case of global optimization the idea is to convexify the problem. To this end we consider the following equivalent problem:

$$p^* \;=\; \min_{x \in K} p(x) \;=\; \min_{\mu \in \Pi(K)} \int p\, d\mu\,, \tag{1.13}$$

where $\Pi(K)$ denotes the set of all probability measures μ supported on the set K.

From Haviland's theorem we know that measures correspond to linear maps which map nonnegative polynomials to $\mathbb{R}^+$. Now, given a polynomial p that is nonnegative on K we see that for every positive $\varepsilon > 0$ the polynomial $p + \varepsilon$ is in fact positive. As under the assumption made above the quadratic module $QM(g_1, \ldots, g_m)$ is archimedean we find by Putinar's Positivstellensatz that $p + \varepsilon \in QM(g_1, \ldots, g_m)$. This was used by Putinar to characterize the linear maps $L \in \mathrm{Hom}(\mathbb{R}[X], \mathbb{R})$ that come from integration with respect to measures $\mu \in \Pi(K)$.

Theorem 1.30 (Putinar)
Suppose Assumption 1.29 holds for the set K and define $g_0 := 1$.

A linear map $L \in \mathrm{Hom}(\mathbb{R}[X], \mathbb{R})$ is the integration with respect to a probability measure μ on K i.e.,

$$\exists \mu\, \forall p \in \mathbb{R}[X] :\; L(p) = \int p\, d\mu,$$

if and only if $L(1) = 1$ *and for* $0 \leq i \leq m$ *the bilinear forms*

$$\begin{aligned} \mathcal{L}_{g_i} : \mathbb{R}[X] \times \mathbb{R}[X] &\mapsto \mathbb{R} \\ (p, q) &\mapsto L(p \cdot q \cdot g_i) \end{aligned}$$

are all positive semidefinite.

With this characterization we can restate (1.13) in the form

$$p^* = \min \{L(p) \ : \ L \in \mathrm{Hom}(\mathbb{R}[X], \mathbb{R}),\ L(1) = 1 \text{ and each } \mathcal{L}_{g_i} \succeq 0\}\,. \tag{1.14}$$

Now fix any basis $\mathcal{B} = \{b_1, b_2, \ldots\}$ of the vector space $\mathbb{R}[X]$ (for example the monomial basis x^α) and consider the infinite dimensional *moment matrix* $M(y)$ defined by

$$M(y)_{i,j} := L(b_i \cdot b_j)\,.$$

Furthermore for each g_k define in an analogous manner the *localizing matrix* $M(g_k * y)$ by

$$M(g_k * y)_{i,j} := L(g_k \cdot b_i \cdot b_j).$$

Now suppose we have a sequence y indexed by the elements of $\mathcal{B}$. Then this sequence comes from a measure μ supported on K if and only if the resulting matrices are positive semidefinite.

With these matrices a truncated version of (1.14) can be constructed.

Let $k \geq k_0 := \max\{\lceil \deg p/2 \rceil, \lceil \deg g_1/2 \rceil, \ldots, \lceil \deg g_m/2 \rceil\}$, and consider the hierarchy of semidefinite relaxations:

$$Q_k : \begin{array}{l} \inf_y \sum_\alpha p_\alpha y_\alpha \\ \qquad\qquad M_k(y) \ \succeq \ 0\,, \\ M_{k-\lceil \deg g_j/2 \rceil}(g_j * y) \ \succeq \ 0\,, \quad 1 \leq j \leq m\,, \end{array} \tag{1.15}$$

with optimal value denoted by $\inf Q_k$ (and $\min Q_k$ if the infimum is attained).

Although each of the relaxation values might not be optimal for the original problem, Lasserre was able to derive the following convergence result.

Theorem 1.31 (Lasserre)
Let Assumption 1.29 hold and consider the hierarchy of SDP-relaxations $(Q_k)_{k \geq k_0}$ *defined in (1.15). Then the sequence* $(\inf Q_k)_{k \geq k_0}$ *is monotone non-decreasing and converges to the optimal value* p^**, that is,*

$$\inf Q_k \uparrow p^* \text{ as } k \to \infty.$$

Although there are conditions that make it possible to decide if an optimal value has been reached after a certain iteration (see for example [HL05, Las10]), in general only in some situations finite convergence can be guaranteed:

Let $p, g_1, \dots g_m \in \mathbb{R}[X]$ and $V(g_1, \dots, g_m) := \{x \in \mathbb{R}^n : g_1(x) = \dots = g_n(x) = 0\}$. We consider the problem

$$\inf_{x \in V(g_1,\dots,g_m)} p(x).$$

Laurent [Lau07a] could show that finite convergence occurs in the situation where the feasible set is given by finitely many points

Theorem 1.32 (Laurent)
If the ideal generated by $g_1, \dots, g_m$ is zero-dimensional then the Lasserre relaxation scheme of the above problem has finite convergence i.e there is an $l \geq k_0$ such that

$$\inf Q_l = p^*.$$

1.2.5 Polynomial matrix inequalities

An interesting case of a polynomial optimization problem which will be relevant for some of our approaches arises when the polynomial constraints can be realized as positive semidefiniteness of a matrix whose entries are polynomials. To be more precise:

Consider the set $\mathrm{Sym}_m(\mathbb{R})$ of real symmetric $m \times m$-matrices. A *polynomial matrix inequality (PMI)* optimization problem is an optimization problem of the form

$$\begin{aligned} f^* &= \min f(x) \\ &\quad \text{s.t. } G(x) \succeq 0, \end{aligned}$$

where f is a real polynomial and $G : \mathbb{R}^n \to \mathrm{Sym}_m(\mathbb{R})$ is a polynomial mapping (i.e., each entry $G_{ij}(X)$ of the symmetric matrix $G(X) \in \mathrm{Sym}_m(\mathbb{R})$ is a polynomial in the variables $X = (X_1, \dots, X_n)$.)

Theorem 1.1 states that in order for a matrix to be positive semidefinite, all its principle minors have to be nonnegative. So, a first idea to derive bounds on the optimal solution of a PMI could be to explicitly write down the inequalities that would ensure the nonnegativity of the principal minors of the matrix $G(x)$. This in turn leads to a polynomial problem and one could use the standard techniques described in the previous section. Although this is possible one would have to deal with polynomials of large degree. Even if all $G(x)_{i,j}$ are linear polynomials the polynomial inequalities one needs to consider are of degree m. This high degree could make it already hard to explicitly calculate the first possible relaxation.

To overcome this problem an SDP hierarchy was proposed in [HL06] that takes the semidefiniteness of a polynomial matrix into account. The basic idea is to generalize

the standard approach in a suitable way by defining a localizing matrix for the matrix $G(x)$,

$$M(G * y)_{i,j,l,k} = L(b_i \cdot b_j \cdot G(x)_{l,k}) .$$

Let $k \geq k_0 := \max\{\lceil \deg f/2 \rceil, \lceil \deg G(x)_{i,j} \rceil\}$. Then with these notations at hand one can define a relaxation in an analogous manner:

$$Q_k : \begin{array}{rcl} \inf_y \sum_\alpha f_\alpha y_\alpha & & \\ M_k(y) & \succeq & 0 , \\ M_{k-m}(G * y) & \succeq & 0 . \end{array} \tag{1.16}$$

In order to guarantee the convergence of this relaxation one needs to assume Putinar's condition viewed in this setting:

Assumption 1.33
Suppose that there is $u \in \mathbb{R}[X]$ such that the level set $\{x \in \mathbb{R}^n : u(x) \geq 0\}$ is compact and u has the representation

$$u = u_0 + \langle R(X), G(X) \rangle \tag{1.17}$$

for some sums of squares polynomials $u_0 \in \mathbb{R}[X]$ and a sums of squares matrix $R(X) \in \mathbb{R}[X]^{m \times m}$.

Now we have the following:

Theorem 1.34
If $G(x)$ meets the Assumption 1.33 then the sequence $(\inf Q_k)_{k \geq k_0}$ is monotone non-decreasing and converges to f^*; that is,

$$\inf Q_k \uparrow f^* \text{ as } k \to \infty.$$

2

Representation and invariant theory

Denn wer den Schatz,
das Schöne, heben will,
Bedarf der höchsten Kunst:
Magie der Weisen

Faust
Goethe

During all times symmetry has been attributed to beauty and truth. However, it was not until the 19th century that the pioneers Niels Abel and Evariste Galois gave rise to a quantification of symmetry by their abstract concept of a group. This chapter explains this abstract point of view as far as needed in this thesis. Namely, we will focus on linear representation theory and invariant theory, where we will restrict ourselves to finite groups in both cases. The first section will provide some basics from linear representation theory and we will expose how the concept of representations can be used in order to simplify semidefinite programs. In the second section we will study the representation theory of the symmetric group $\mathcal{S}_n$. Finally, in the last section we will provide some basics of invariant theory.

2.1 Linear representation theory

The aim of representation theory is to understand groups by representing their elements as linear transformations of a vector space. In this way structural questions on a group can be analyzed by means of linear algebra. On the other hand we will expose here that also properties of matrices like positive semidefiniteness can be easier checked when additionally a group action is assumed. A standard reference for linear representation theory is e.g. [Ser01], which we mainly follow in this chapter. Although the concepts of linear representation theory are defined over any fields, in this chapter we will mostly assume that the ground field is the complex numbers.

Definition 2.1
Let G be a finite group. A *representation of* G is a finite dimensional vector space V together with a group–homomorphism

$$\rho : G \to \mathrm{GL}(V)$$

into the group of invertible linear transformations of V. The *degree* of the representation is the dimension of V.

Two representations (V, ρ) and (V', ρ') of the same group G are *equivalent* if there is an isomorphism $\phi : V \to V'$ such that

$$\rho'(g) = \phi\rho(g)\phi^{-1} \quad \text{for all } g \in G.$$

Another way of looking at representations is to observe that a representation ρ induces an action of G on V and hence one obtains a G–module structure on V. Also, given a G–module V let $\phi : G \to \mathrm{GL}(V)$ be the map sending g to $v \mapsto gv$. Then clearly ϕ is a representation of G. So the concepts of G–modules and representations of G are equivalent notions.

Once we have chosen a basis $b_1, \ldots, b_n$ for V we can identify the image of G under ρ as a matrix subgroup X of the invertible $n \times n$ matrices with complex coefficients. We will write $X(g)$ for the matrix corresponding to $g \in G$.

A linear map $\phi : V \to W$ between two G–modules is called a G–homomorphism if $\phi(g(v)) = \phi(v)$ for all $g \in G$ and $v \in V$. The set of all G–homomorphism between V and W is denoted by $\mathrm{Hom}_G(V, W)$ and two G–modules are called *isomorphic*, if there is a G–isomorphism from V to W.

Let V be a G–module, then the *endomorphism algebra* of V is defined to be

$$\mathrm{End}\, V := \{\phi : V \to V : \phi \text{ is a } G\text{–homomorphism}\}.$$

If we work with a matrix representation, this corresponds to the notion of the *commutant algebra*, which is defined as

$$\mathrm{Com}\, X := \left\{T \in \mathbb{C}^{n\times n} : TX(g) = X(g)T \text{ for all } g \in G\right\}.$$

Example 2.2

1. The one-dimensional representation $V = \mathbb{C}$ with $g(v) = v$ for all $g \in G$ and $v \in \mathbb{C}$ is called the trivial representation.
2. Take any set S on which G acts and set $\mathbb{C}\{S\} = \oplus_{s\in S}\mathbb{C}e_s$ with formal symbols e_s ($s \in S$). Then the obvious action of G on $\mathbb{C}\{S\}$ defined via $g(e_s) = e_{g(s)}$ turns $\mathbb{C}\{S\}$ into a G–module. In the special case when $S = G$ this is called the *regular representation*.

The key objects to study the structure of the action of G on a vector space V are the fixed subspaces. If there is a proper submodule W of V (i.e., a G–invariant subspace W of V) then the representation (ρ, V) is called *reducible*. In the other case, if the only G–invariant subspaces are V and $\{0\}$, then (V, ρ) is called *irreducible*.

Let $\langle \cdot, \cdot \rangle$ be a scalar product on V. In general, this does not need to be G–invariant. However, we can use it to define an invariant one by setting

$$\langle x, y \rangle_G := \frac{1}{|G|} \sum_{g \in G} \langle g(x), g(y) \rangle.$$

Suppose now that the G–module V is reducible, i.e., there is another G–module $W \subset V$. Using the fact that we have a G–invariant scalar product on V we see that also

$$W^{\perp} := \{y \in V \ \ \langle x, y \rangle_G = 0, \text{ for all } x \in W\}$$

is in fact a $G - module$. Using this argument iteratively one gets the decomposition of a G–module into a direct sum of irreducible submodules:

Theorem 2.3 (Maschke's theorem)
Any G–module $V \neq \{0\}$ defined over a field with characteristic zero is the direct sum of irreducible G–submodules $W_1, \ldots, W_k$:

$$V = W_1 \oplus W_2 \oplus \cdots \oplus W_k. \tag{2.1}$$

However, this decomposition is not necessarily unique. Nevertheless, for every irreducible representation W_i the sum of all irreducible components isomorphic to W_i and occurring in V is uniquely determined. Each of theses sums

$$V_i := \bigoplus_{j=1}^{m_i} W_j$$

is called an *isotypic component*.

If in contrast to the above theorem the characteristic of the ground field is positive, a similar result only holds if the characteristic does not divide the size of G.

Consider two groups G_1 and G_2 and define their product $G := G_1 \times G_2$. Let V_1 be a G_1-module and V_2 be a G_2-module. Now, the vector space $V := V_1 \otimes V_2$ has a basis $\{v_1^1 \otimes v_1^2, \ldots, v_n^1 \otimes v_m^2\}$ where $\{v_1^1, \ldots, v_n^1\}$ is a basis of V_1 and $\{v_1^2, \ldots, v_m^2\}$ is a basis of V_2. Using this basis of V we can define an action of G on V by setting $gv = g_1 v_i^1 \otimes g_2 v_j^2$ for $v = v_i^1 \otimes v_j^2$ and with $g = (g_1, g_2) \in G$.

Let V be a G module and X be a corresponding matrix group. Then the *character*

$$\chi : G \to \mathbb{C}$$

of V is the map defined by

$$\chi(g) = \mathrm{Tr}(X(g)) \text{ for all } g \in G.$$

Although we chose a basis for the matrix representation, the trace does not depend on this arbitrary choice. Hence the character only depends purely on the representation. Given two characters χ_1, χ_2 we define a scalar product by setting

$$\langle \chi_1, \chi_2 \rangle := \frac{1}{|G|} \sum_{g \in G} \chi_1(g) \cdot \overline{\chi_2(g)}.$$

We note the following.

Proposition 2.4
Let $\chi_1, \chi_2 : G \to \mathbb{C}$ be characters of two representations V_1, V_2. Then we have

1. *$\chi(g) = \chi(g')$ for all g' in the same conjugacy class of g.*
2. *If χ is the character of $V_1 \oplus V_2$, then $\chi = \chi_1 + \chi_2$.*
3. *If χ is the character of $V_1 \otimes V_2$, then $\chi = \chi_1 \cdot \chi_2$.*

By considering the resulting characters we get that the irreducible representations of the products of two groups can be constructed using tensor products:

Proposition 2.5
Let G_1 and G_2 be two groups. Then any irreducible $(G_1 \times G_2)$–module V is isomorphic to $V_1 \otimes V_2$ where V_1 and V_2 are irreducible modules for G_1 and G_2.

A fundamental goal is to construct the irreducible representations of a given group G. A fruitful way to do this can be to use subgroups or larger groups and study the behavior of the irreducible representations under restriction or induction:

Definition 2.6
Let $H < G$ be a subgroup.

1. Restriction: If V is a G–module then V is also an H-module. $V\downarrow_H^G$ will be used to denote the resulting H-module. If χ is the character of V then the resulting character will be denoted by $\chi\downarrow_H^G$.
2. Induction: Consider a complete system of representatives $\{x_1, \ldots, x_t\}$ of G/H, so that $G = x_1 H \cup \cdots \cup x_t H$. Then

$$V \uparrow_H^G = \bigoplus_{i=1}^{t} x_i V$$

where the left action of G is as follows: for every i, we can find j and $h \in H$ that both depend on g such that $gx_i = x_j h$. Now define $gx_i v := x_j(hv)$. The resulting character will be denoted by $\psi\uparrow_H^G$.

The duality between the operations of restriction and induction is expressed in the following important theorem:

Theorem 2.7 (Frobenius reciprocity)
Let H be a subgroup of G and let χ be a character of H and ψ a character of G. Then

$$\langle \chi\uparrow_H^G, \psi\rangle = \langle \chi, \psi\downarrow_H^G\rangle.$$

The following fundamental observation that was first proven by Issai Schur in 1905 will play a central role in our usage of representation theory:

Theorem 2.8 (Schur's lemma)
Let V and W be two irreducible representations of a group G. Then a G–homomorphism ϕ from V to W is either zero or an isomorphism. In particular, a homomorphism from V to itself is equivalent to multiplication by a scalar.

Proof. Let ϕ be a G–homomorphism. Then it is clear that kernel of ϕ and the image of ϕ are G–invariant. Hence if ϕ is neither an isomorphism nor the zero map, its kernel will be a non trivial G–submodule of V and its image a non trivial G–submodule of W, which is a contradiction. □

Although Schur's lemma is not very hard to prove it is fundamental in the sense that various properties of irreducible representations become visible through it. We note some of these in the following corollaries.

Corollary 2.9
Let W be an irreducible representation and V any other representation. Then the multiplicity of irreducible representations isomorphic to W that are contained in V equals $\dim \mathrm{Hom}(W, V)$.

Corollary 2.10
Two characters χ_1, χ_2 corresponding to distinct irreducible representations are orthogonal i.e., we have $\langle \chi_1, \chi_2\rangle = 0$.

Corollary 2.11
Let V be an irreducible G–module and $\langle \cdot, \cdot\rangle_G$ be a non-trivial invariant Hermitian form on V. Then $\langle \cdot, \cdot\rangle_G$ is unique up to a real scalar multiple.

Corollary 2.12
Let $V := m_1W_1 \oplus m_2W_2 \oplus \ldots \oplus m_kW_k$ be a complete decomposition of a representation V such that $\dim W_i = d_i$. Then we have:

1. $\dim V = m_1d_1 + \ldots + m_kd_k$,
2. $\operatorname{End} V \simeq \bigoplus_{i=1}^{k} \mathbb{C}^{m_i \times m_i}$.
3. *Let χ be the character of V and χ_i the character of W_i then we have $\langle \chi, \chi_i \rangle = m_i$.*
4. *There is a basis of V such that*
   a) *the matrices of the corresponding matrix group X are of the form*

$$X(g) = \bigoplus_{l=1}^{k} \bigoplus_{j=1}^{m_i} X^{(l)}(g),$$

   where $X^{(l)}$ is a matrix representation corresponding to W_l.
   b) *The corresponding commutant algebra is of the form*

$$\operatorname{Com} X \simeq \left\{ \bigoplus_{l=1}^{k} (M_i \otimes I_{d_l}) \right\},$$

   where $M_l \in \mathbb{C}^{m_l \times m_l}$ and I_{d_l} denotes the identity in $\mathbb{C}^{d_l \times d_l}$.

A basis for V as in the corollary above is called *symmetry adapted* basis. If we are given any matrix representation it is interesting to explicitly calculate such a basis:

Let X be a matrix representation associated with V and $Y^l(g) := (Y^l(g))_{i,j}$ be any matrix representation corresponding to an irreducible representation W_l. We define for $\alpha, \beta = 1, \ldots, d_l$ the following map:

$$\pi_{\alpha,\beta} := \frac{n_i}{|G|} \sum_{g \in G} Y^l_{\beta,\alpha}(g^{-1}) X(g).$$

Proposition 2.13
With the notation from above the map $\pi_{1,1}$ is a projection from V onto a subspace $V_{l,1}$ isomorphic to W_l. Further $\pi_{1,\beta}$ maps $V_{l,1}$ onto $V_{l,\beta}$ which is another irreducible component of V isomorphic to W_l.

In other words the above defined π can be used to calculate a symmetry adapted basis.

Keeping the above in mind, our main interest in representation theory comes from the possibility of applying Schur's lemma to matrix calculations. More precisely, consider a linear representation $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ and let $X \in \mathbb{C}^{n \times n}$ a matrix such that

$$\rho(g)X = X\rho(g) \text{ for all } g \in G.$$

If the representation ρ decomposed as $\rho = m_1\rho_1 \oplus \ldots \oplus m_k\rho_k$, with $d_i = \dim \rho_i$ we can use a symmetric adapted based for $\mathbb{C}^n$ in order to block diagonalize X. Indeed, let T be a matrix collecting the elements of a symmetry adapted basis as columns. Then we find by the above corollary that $Y := T^{-1}XT$ has block diagonal form with k blocks Y_i of dimension $m_i \cdot d_i$ corresponding to the irreducible representations. These blocks Y_i further decompose into d_i equal blocks B_i of dimension m_i, so Y is of the form:

$$Y = \begin{pmatrix} Y_1 & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & Y_k \end{pmatrix}, \qquad \text{with } Y_i := \begin{pmatrix} B_i & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & B_i \end{pmatrix}.$$

Thus we arrive in a situation, where the matrix has been simplified quite a lot.

In this section we presented the theory of linear representations in the context of complex representation. However, in the sequel, we will be mostly concerned with finite groups acting linearly on a real vector space and symmetric real matrices. A generalization of the classical theory to the real case is presented for example in [Ser01]. In this case one has to distinguish three cases: Absolutely irreducible representations, representations of complex type, and very rarely representations of quaternian type. In the first case the real irreducible representation $\rho_i(g)$, which is given by real matrices stays irreducible if one extends the scalars to the complex numbers. In the other two cases a real irreducible representation decomposes further into two complex irreducible representations: in the case of complex type into two complex conjugate representations, in the quaternian case into twice a complex irreducible. However, one can define a real symmetry adapted basis for the real representation (see [FW93, GSS88] and the example below).

Example 2.14
The cyclic group C_4 acts on $\mathbb{R}^4$ by cyclicly permuting coordinates. Then a symmetry adapted basis for the complexification of this representation to $\mathbb{C}^4$ is given by the Fourier basis:

$$T = \begin{pmatrix} 1 & i & -1 & -i \\ 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \end{pmatrix}.$$

Now by combining the conjugate complex representations we get a symmetry adapted basis for $\mathbb{R}^4$: Denote by $t^{(1)}, \ldots, t^{(4)}$ the columns above. Then the real matrix with columns $(t^{(1)}, t^{(2)} + t^{(4)}, t^{(3)}, \frac{1}{i}(t^{(2)} - t^{(4)}))$ defines a symmetry adapted basis for $\mathbb{R}^4$.

Now we want to explain how representation theory can be applied to SDPs in the case when the program is invariant by a group action. Following mainly [GP04, Val08, BGSV10] we will expose how in this case we can use the above results from Schur's lemma to simplify the complexity i.e., the dimensions of the matrices, drastically by using block diagonalization.

Consider the following semidefinite program in canonical form:

$$\begin{array}{lrcl} \inf & \langle C, X\rangle & & \\ \text{s.t.} & \langle A_i, X\rangle & = & b_i\,, \quad 1 \le i \le m\,, \\ & X & \succeq & 0, \text{ where } X \in \mathrm{Sym}_n(\mathbb{R})\,, \end{array}$$

and we will denote $\mathcal{L} := \left\{ X \in \mathrm{Sym}_n^+(\mathbb{R}) \,:\, \langle A_i, X\rangle = b_i, \text{ for } 1 \le i \le m \right\}$ the corresponding spectrahedron and y^* its optimal value.

Now assume that $(\mathbb{R}^n, \rho)$ is an n-dimensional representation of a finite group G. As we can always chose an orthonormal basis for $\mathbb{R}^n$ with respect to a G–invariant scalar product, we can assume without loss of generality that the corresponding matrices are orthonormal i.e., we have $\rho^T(g)\rho(g) = \mathrm{Id}$ for all $g \in G$. Now this representation naturally carries over to a representation σ on $\mathrm{Sym}_n(\mathbb{R})$ by:

$$\sigma(g)(X) := \rho(g)^T X \rho(g), \qquad \text{for } X \in \mathrm{Sym}_n(\mathbb{R}) \text{ and } g \in G.$$

A given subset $\mathcal{L} \subseteq \mathrm{Sym}_n(\mathbb{R})$ is now called *invariant with respect to* σ if for all $X \in \mathcal{L}$ we have $\sigma(g)(X) \in \mathcal{L}$, for all $g \in G$.

By the construction of σ we see that the cone of positive semidefinite matrices Sym_n^+ is always an invariant set. Further a linear functional $\langle C, X\rangle$ is invariant with respect to σ, if $\langle C, \sigma(g)(X)\rangle = \langle C, X\rangle$ for all $g \in G$. Finally, a semidefinite program is said to be a *σ-invariant SDP* if both the cost function $\langle C, X\rangle$ as well as the feasible set $\mathcal{L}$ are σ-invariant.

The key observation for an invariant SDPs is that due to convexity we can restrict its feasible set $\mathcal{L}$ to the smaller set

$$\mathcal{L}^G := \{X \in \mathcal{L} \,:\, \sigma(g)(X) = X \text{ for all } g \in G\}$$

of feasible matrices that are G–invariant.

To an invariant semidefinite program in canonical form we construct the following *G–symmetrized version:*

$$\begin{array}{lrcl} \inf & \langle C, X\rangle & & \\ \text{s.t.} & \langle A_i, X\rangle & = & b_i\,, \quad 1 \le i \le m\,, \\ & X & = & \sigma(g)(X) \quad \text{for all } g \in G, \\ & X & \succeq & 0, \text{ where } X \in \mathrm{Sym}_n(\mathbb{R})\,. \end{array}$$

Its optimal value is denoted by y_G^*, On the one hand it now follows that every feasible solution to the G–symmetrized version gives a feasible solution to the original semidefinite program. This implies $y_G^* \le y^*$. On the other hand if the matrix X is feasible for the initial semidefinite program which is G–invariant we have that also for every $g \in G$ the matrix $\sigma(g)(X)$ is feasible and $\langle C, X\rangle = \langle C, \sigma(g)(X)\rangle$ for every $g \in G$. Hence we can apply the so called *Reynolds Operator* to X i.e., $X_G := \frac{1}{|G|}\sum_{g\in G} \sigma(g)(X)$ yielding a feasible solution $X_G \in \mathcal{L}^G$. This in turn implies $y_G^* \le y^*$ and we have the following.

Theorem 2.15
To every σ–invariant semidefinite program there is a G–symmetrized version which gives the same optimal value.

Now consider the decomposition of

$$\mathbb{R}^n := W_1^1 \oplus W_2^1 \oplus \dots W_{m_1}^1 \oplus W_1^2 \dots \oplus W_{m_k}^k$$

into real irreducible representations such that the W_j^i are isomorphic for all j with with $\dim W_j^i = d_j$. As ρ is supposed to be orthogonal we can assume the resulting real symmetry-adapted basis of $\mathbb{R}^n$ to be orthonormal. The elements of this basis will be denoted by $\left\{v_{11}^1, \dots, v_{1d_1}^1, \dots, v_{m_k d_k}^k\right\}$, i.e., the elements $\left\{v_{i1}^j, \dots, v_{id_j}^j\right\}$ form an orthonormal $\mathbb{R}$-basis of the G-module W_i^j in the above decomposition.

Let T be the matrix collecting the elements of the symmetry adapted basis as columns now we have that for every matrix $X \in \mathcal{L}^G$ the matrix $M := T^T X T$ is block diagonal and hence $X \succeq 0$ if and only if $M \succeq 0$.

Now, we define for every l in $\{1, \dots, k\}$ a $m_l \times m_l$ matrix M_l component wise by

$$M_{l,i,j} := (v_{i1}^l)^T X v_{j1}^l.$$

A finer analysis of Corollary 2.12 and the related basis transformation yields that

$$M = \bigoplus_{l=1}^{k} (M_l \otimes I_{d_i}),$$

hence $M \succeq 0$ if and only if $M_l \succeq 0$ for all $1 \leq l \leq k$.

In order to write down the resulting SDP in block-diagonal form in a convenient way the following $m_l \times m_l$ matrices $E_l(i,j)$ with coefficients

$$E_{l,u,v}(i,j) := \sum_{h=1}^{d_l} v_{uh}^k(i) \cdot v_{vh}^k(j)$$

are used.

With these *zonal matrices* we can reconstruct the matrix X given the matrices M_l by

$$X_{ij} = \sum_{l=1}^{k} \langle M_l, E_l(i,j) \rangle.$$

Hence the symmetrized version of the SDP simplifies to

$$\begin{array}{lrcl} \inf \langle C, X \rangle & & & \\ \text{s.t.} & \langle A_{i,j}, X \rangle & = & b_i\,, \quad 1 \leq j, \leq m\,, 1 \leq i \leq k, \\ & X_{i,j} & = & \sum_{l=1}^{k} \langle E_l(i,j), M_l \rangle, \\ & M_l & \succeq & 0, \text{ where } M_l \in \mathrm{Sym}_{m_i}(\mathbb{R}), 1 \leq l \leq k. \end{array}$$

2.2 Symmetric group

The representation theory of the symmetric group was one of the topics that founded modern representation theory. Already Frobenius and Young could describe the irreducible characters of the symmetric group in a beautiful combinatorial way. Our exposition mainly follows [Sag01].

The objects used to derive combinatorial description are so called *Young tableaux*. We will start to present these objects in the first section. Although the irreducible characters where already understood in the beginning of the 20th century it was not before the 1930's when Wilhelm Specht was able to construct the associated irreducible representations combinatorially. These irreducible representations therefore are called *Specht modules*. We will construct these modules in the second section. Finally we remark how the so called permutation representation, which will be needed later, decomposes.

2.2.1 Young tableaux

Definition 2.16
For $n \geq 1$, a *partition* λ of n is a sequence of positive integers $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_l)$ satisfying $\lambda_1 \geq \lambda_2 \geq \ldots \lambda_l > 0$ and $\sum_{i=1}^{l} \lambda_i = n$. We will write $\lambda \vdash n$ to denote that λ is a partition of n.

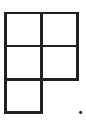
The number 5 for example has the following partitions:

$$(5), (4,1), (3,2), (3,1,1), (2,2,1), (2,1,1,1), (1,1,1,1,1).$$

In order to obtain a complete description of the irreducible representations in an inductive way it will be important to compare two partitions. This will be done by the so called *dominance order*: We write $\lambda \trianglerighteq \mu$ for two partitions $\lambda, \mu \vdash n$ if $\lambda_1 + \cdots + \lambda_i \geq \mu_1 + \cdots + \mu_i$ for all i. With these first definitions at hand we can define the Young Diagram associated with a partition.

Definition 2.17
A Young Diagram associated with a partition $\lambda \vdash n$ is a set of n boxes that are arranged in left-justified row, such that the number of boxes in the i-th row is exactly λ_i[1].

For example the Young Diagram associated with $(2,2,1) \vdash 5$ is of the form



[1]The way we note Young tableaux follows the English notation (see [Sag01]). Some authors follow the French notation and thus their Young tableaux will be an up side down reflection of the ones used here

Partitions of n are interesting for the representation theory of $\mathcal{S}_n$ because, as we will see later on, they naturally describe the irreducible representations. As a first step to this end we associate with each partition λ a so called *Young group*:

Definition 2.18
Let $\lambda \vdash n$. Then a subgroup of $\mathcal{S}_n$ of the form

$$\mathcal{S}_\lambda = \mathcal{S}_{\lambda_1} \times \mathcal{S}_{\lambda_2} \times \ldots \times \mathcal{S}_{\lambda_l}$$

is called a *Young Group* corresponding to λ.

Our interest in these groups comes from the fact that the induced representation $\mathbf{1}\uparrow_{\mathcal{S}_\lambda}^{\mathcal{S}_n}$, where $\mathbf{1}$ denotes the trivial representation, will be essential to describe the irreducible representations.

A nice combinatorial way to characterize the modules $\mathbf{1}\uparrow_{\mathcal{S}_\lambda}^{\mathcal{S}_n}$ will be given using so called *Young tableaux*:

Definition 2.19
A *Young tableau* of shape $\lambda \vdash n$ is a Young Diagram together with an entry in every box from $\{1, \ldots, n\}$, and each of these numbers occurs exactly once. A *standard Young tableau* is a Young tableau in which all rows and columns are numbered increasingly.

Example 2.20
For the partition $(2, 2, 1) \vdash 5$, two possible Young tableau are given by

$$\begin{array}{|c|c|}\hline 1 & 3 \\ \hline 5 & 2 \\ \hline 4 \\ \cline{1-1}\end{array}\,, \qquad \begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 & 5 \\ \hline 4 \\ \cline{1-1}\end{array}\,.$$

Only the second one is a standard Young tableau.

The action of $\mathcal{S}_n$ on $\{1, \ldots, n\}$ induces an action on the set of Young tableaux. Two Young tableaux t_1 and t_2 are called *row equivalent* if the corresponding rows of the two tableaux contain the same numbers. The classes of equivalent Young tableaux are called *tabloids*, and the equivalence class of a tableau t is denoted by $\{t\}$.

Let $\{t\}$ be a λ–tabloid. Then the group $\mathcal{S}_{\lambda_1} \times \ldots \times \mathcal{S}_{\lambda_l}$ stabilizes $\{t\}$. The action of $\mathcal{S}_n$ gives rise to an $\mathcal{S}_n$-module:

Definition 2.21
Suppose $\lambda \vdash n$. The *permutation module* M^λ *corresponding to* λ is the $\mathcal{S}_n$-module defined by $M^\lambda = \mathbb{C}\{\{t_1\}, \ldots, \{t_l\}\}$, where $\{t_1\}, \ldots, \{t_l\}$ is a complete list of λ–tabloids.

Observe that the module M^λ can be seen as a realization of the induced representation of $\mathcal{S}_n$ from the trivial representation of $\mathcal{S}_{\lambda_1} \times \ldots \times \mathcal{S}_{\lambda_l}$. This observation justifies the following proposition.

Proposition 2.22
If $\lambda \vdash n$ then M^λ is a cyclic module, generated by any given λ–tabloid. Furthermore, we have $\dim M^\lambda = \frac{n!}{(\lambda_1! \cdot \lambda_2! \cdots \lambda_m!)}$.

Example 2.23
If $\lambda = (1, 1, \ldots, 1) \vdash n$ then $M^\lambda \cong \mathbb{C}\mathcal{S}_n$. In case $\lambda = (2, 1)$ a complete list of λ–tabloids is given by the representatives

$$\begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 \\ \cline{1-1}\end{array}\ , \qquad \begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 \\ \cline{1-1}\end{array}\ , \qquad \begin{array}{|c|c|}\hline 2 & 3 \\ \hline 1 \\ \cline{1-1}\end{array}\ . \tag{2.2}$$

Each tabloid is stabilized by a Young group isomorphic to $\mathcal{S}_2 \times \mathcal{S}_1$.

2.2.2 Specht modules

The smallest non trivial case of a symmetric group is the group $\mathcal{S}_2 := \{1, \sigma_1\}$. This group is abelian and hence all irreducible representations are one-dimensional. One is just the trivial representation $\mathbf{1}$, the other corresponds to the signum of the permutations, i.e., $\mathrm{sgn}(1) = 1, \mathrm{sgn}(\sigma_1) = -1$. Now the irreducible representations of higher symmetric groups can be interfered using the induction defined in Definition 2.6 inductively using these two.

Definition 2.24
Let t be a Young tableau for $\lambda \vdash n$, and let C_i be the set of entries in the i-th column of t. The group $\mathrm{CStab}_t = \mathcal{S}_{C_1} \times \mathcal{S}_{C_2} \times \cdots \times \mathcal{S}_{C_\nu}$ (where $\mathcal{S}_{C_i}$ is the symmetric group on $\mathcal{C}_i$) is called the *column stabilizer* of t.

Now given $\lambda \vdash n$ and t_λ a λ-tableau. By interchanging the rows of t_λ with its columns we construct a new tableau $t_{\lambda'}$ corresponding to another partition $\lambda' \vdash n$. This partition λ' is called the transposition of λ. With this notation the following fundamental result due to Frobenius and Young characterizes all irreducible representations of $\mathcal{S}_n$.

Theorem 2.25 (Frobenius–Young–correspondence)
With the definitions from above for every $\lambda \vdash n$ it holds that

$$\mathbf{1}\uparrow_{\mathcal{S}_\lambda}^{\mathcal{S}_n} \bigcap \mathrm{sgn}\uparrow_{\mathcal{S}_{\lambda'}}^{\mathcal{S}_n}$$

is an irreducible representation of $\mathcal{S}_n$.

Now as the irreducible representations of the symmetric group $\mathcal{S}_n$ are in 1-1-correspondence with the conjugacy classes of $\mathcal{S}_n$ and therefore with the partitions of n, the above

theorem really provides a complete list of all irreducible representations of $\mathcal{S}_n$. A construction of the corresponding $\mathcal{S}_n$ modules is given by the so called *Specht modules*. This will be explained in the following.

For $\lambda \vdash n$, the *polytabloid associated* with a λ-tableau t is defined by

$$e_t \;=\; \sum_{\sigma \in \mathrm{CStab}_t} \mathrm{sgn}(\sigma)\sigma\,\{t\}\ .$$

Then for a partition $\lambda \vdash n$ the *Specht module* $\mathfrak{S}^\lambda$ is the submodule of the permutation module M^λ spanned by the polytabloids e_t. Now recall that every tabloid $\{t\}$ is stabilized by $\mathcal{S}_\lambda$ and further by construction of the polytabloid we have $\sigma(e_t) = \mathrm{sgn}(\sigma) \cdot e_t$. for all $\sigma \in \mathcal{S}_{\lambda'}$. Hence we find that the cyclic module spanned by the various e_t is in fact isomorphic to the representation $\mathfrak{S}^\lambda$ defined above. So the following theorem can be established.

Theorem 2.26
For every $\lambda \vdash n$ the Specht module $\mathfrak{S}^\lambda$ is an irreducible $\mathcal{S}_n$ module. Further the set

$$\{e_t \,|\, t \text{ is a standard } \lambda - \text{tableau}\}$$

is a basis of $\mathfrak{S}^\lambda$.

So the dimension of $\mathfrak{S}^\lambda$ denoted by f^λ is given by the number of standard Young tableaux for $\lambda \vdash n$.

Example 2.27
For $n \geq 2$, we have the decomposition into irreducible components $M^{(n-1,1)} = \mathfrak{S}^{(n)} \oplus \mathfrak{S}^{(n-1,1)}$. Namely, since the one-dimensional subspace spanned by the sum $t_1 + \cdots + t_n$ is closed under the action of $\mathcal{S}_n$, we have a copy of the *trivial* representation (which is isomorphic to the Specht module $\mathfrak{S}^{(n)}$) as irreducible component in $M^{(n-1,1)}$. Moreover, since the tabloids in (2.2) are completely determined by the entry in the second row, we have identified a copy of the $(n-1)$-dimensional Specht module $\mathfrak{S}^{(n-1,1)}$ in $M^{(n-1,1)}$. Indeed, the permutation module $M^{(n-1,1)}$ decomposes as $M^{(n-1,1)} = \mathfrak{S}^{(n)} \oplus \mathfrak{S}^{(n-1,1)}$.

2.2.3 Decomposing the permutation module

The decomposition of the partition module M^μ for a general partition $\mu \vdash n$ will be of special interest for us. It can be described in a rather combinatorial way as follows:

Definition 2.28

1. A generalized *Young tableaux* of *shape* λ is a Young tableau T for λ such that the entries are replaced by any n-tuple of natural numbers. The content of T is the sequence μ_i such that μ_i is equal to the number of $i's$ in T.
2. A generalized Young tableau is called semi standard, if its rows weakly increase and its columns strictly increase.
3. For $\lambda, \mu \vdash n$ the *Kostka number* $K_{\lambda\mu}$ is defined to be the number of semi standard Young tableaux of shape λ and content μ.

For example, the tableau

1	1	2
2	3	

is semi-standard, whereas the tableau

1	1	2
1	2	

is not semi-standard.

The significance of the above definitions lies in the fact that the semi standard Young tableaux of shape λ and content μ can be used to define a basis for $\mathrm{Hom}(\mathfrak{S}^\lambda, M^\mu)$. Combining this basis with the statement in Corollary 2.9 gives the following theorem, which originates from Young's work and describes the decomposition of the permutation module.

Theorem 2.29 (Young's rule)
Let $\mu \vdash n$ and consider the permutation module M^μ. Then we have the following decomposition:

$$M^\mu = \bigoplus_{\lambda \trianglerighteq \mu} K_{\lambda\mu} \mathfrak{S}^\lambda.$$

2.3 Invariant theory

Invariant theory is a classical field of mathematical study. Its roots can be traced back to Gauß and his work on quadratic forms. In this section we will provide some basics of invariant theory as far as it will be needed in the sequel. For further insight into this fascinating topic we refer to [CLO07, Stu93], from which we collect the statements presented in this section.

Let G be a finite group and $\rho : G \mapsto \mathrm{GL}_n$ be a representation of G on $V = \mathbb{C}^n$. Now the action of G on V can be extended to an action of G on the ring of polynomials $\mathbb{C}[X] = \mathbb{C}[X_1, \ldots, X_n]$ by setting $f^g := f(\rho(g)(x))$ for all $g \in G$.

Definition 2.30
A polynomial $f \in \mathbb{C}[X]$ is called *invariant* if $f^g = f$ for all $g \in G$. The set of all invariant polynomials is denoted by $\mathbb{C}[X]^G$.

As the invariance property is not affected by addition or multiplication with an invariant polynomial, the set of invariants from a ring:

Proposition 2.31
Let G be a finite group, then $\mathbb{C}[X]^G$ is a subring of $\mathbb{C}[X]$.

A very useful tool to work with polynomials in invariant setting is the so called *Reynolds operator* defined as follows.

Definition 2.32
For a finite group G the map $R_G(f) := \frac{1}{|G|} \sum_{g \in G} f^g$ is called the *Reynolds operator* of G.

We collect some of the interesting properties of R_G below. They mostly follow by explicit calculations.

Proposition 2.33
The Reynolds operator of a finite group G has the following properties:

1. *R_G is a $\mathbb{C}[X]^G$- linear map.*
2. *For $f \in \mathbb{C}[X]$ we have $R_G(f) \in \mathbb{C}[X]^G$.*
3. *R_G is the identity map on $\mathbb{C}[X]^G$ i.e., $R_G(f) = f$ for all $f \in \mathbb{C}[X]^G$.*

As seen above $\mathbb{C}[X]^G$ is a subring of $\mathbb{C}[X]$. However, it is not obvious whether there exists a finite generating set of this subring. This was a wide area of research in the second half of the 19th century and so the fact that Hilbert in 1890 could provide a proof in the case of finite groups using new techniques brought him international recognition.

Theorem 2.34
Let G be a finite group. Then the invariant ring $\mathbb{C}[X]^G$ is generated by finitely many homogeneous invariants.

In his 14-th problem Hilbert asked whether for all groups the set of invariants would be finitely generated. By giving a counter example to this question, Nagata could prove in 1959 that not all invariants are generated finitely.

Suppose that G is a finite group then we can represent the invariant ring in the form

$$\mathbb{C}[X]^G = \mathbb{C}[f_1, \ldots, f_m]$$

for some finite set of generators. We will also use the term *fundamental invariants* for

these generators. This now implies that every $f \in \mathbb{C}[X]^G$ can be expressed as

$$f = g(f_1, \ldots, f_m)$$

for some polynomial $g \in \mathbb{C}[y_1, \ldots, y_m]$. However, it does not need to be the case that g is uniquely defined. In the case that there are two polynomials $g_1, g_2 \in \mathbb{C}[y_1, \ldots, y_m]$ with

$$g_1(f_1, \ldots, f_m) = g_2(f_1, \ldots, f_m),$$

we define $h = g_1 - g_2$. This provides an algebraic relation $h(f_1, \ldots, f_m) = 0$ among the fundamental invariants. In this case any element in $\mathbb{C}[X]^G$ is only defined up to this algebraic relation $h(f_1, \ldots, f_m) = 0$.

If we denote the set of fundamental invariants $F := \{f_1, \ldots, f_m\}$ then

$$I_F = \{h \in \mathbb{C}[y_1 \ldots, y_m] \, : \, h(f_1, \ldots, f_m) = 0\}$$

denotes the algebraic relations among $f_1, \ldots, f_m$. This ideal of relations I_F is in fact a prime ideal in $\mathbb{C}[y_1, \ldots, y_m]$.

Definition 2.35
Let $F := \{f_1, \ldots, f_m\}$ be a set of polynomials in $\mathbb{C}[X]$. Then the *evaluation homomorphism* Ev_F is given by

$$\mathrm{Ev}_F(g) := g(f_1, \ldots, f_m).$$

Now let F be a set of generators of $\mathbb{C}[X]^G$, we know that Ev_F maps $\mathbb{C}[y_1, \ldots, y_m]$ to $\mathbb{C}[X]^G$. As observed above, the kernel of Ev_F is exactly the ideal I_F. Now the first isomorphism theorem implies the following.

Proposition 2.36
Let $\mathbb{C}[X]^G = \mathbb{C}[f_1, \ldots, f_m]$ and I_F be the ideal of relations. Then there is an isomorphism

$$\mathbb{C}[y_1, \ldots, y_m]/I_F \simeq \mathbb{C}[X]^G.$$

A more geometric picture of the situations is obtained by associating the ideal of relations I_F with the variety $V_F = V(I_F) \subset \mathbb{C}^m$. We note the following.

Proposition 2.37

1. *V_F is the smallest variety containing the parametrization*

$$\begin{aligned} y_1 &= f_1(x_1, \ldots, x_n) \\ \vdots &\quad \vdots \\ y_m &= f_m(x_1 \ldots, x_n). \end{aligned}$$

2. *$I_F = I(V_F)$, i.e., I_F is the ideal of all polynomials vanishing on V_F.*
3. *V_F is an irreducible variety.*
4. *Let $\mathbb{C}[V_F]$ be the coordinate ring of V_F. Then there is an isomorphism*

$$\mathbb{C}[V_F] \simeq \mathbb{C}[X]^G.$$

Definition 2.38
Let $a \in \mathbb{C}^n$, then the orbit of a denoted by G_a is the set of points to which a is mapped to under the action of G, i.e.,

$$G_a := \{g(a) \;\; g \in G\}.$$

The set of all G–orbits on $\mathbb{C}^n$ is denoted by $\mathbb{C}^n/G$ and is called the *orbit space*.

As we have that the orbits G_a and G_b of two points in $\mathbb{C}^n$ are either equal or disjoint, the action of G on $\mathbb{C}^n$ naturally defines an equivalence relation by $a \sim b$ if and only if $b = g(a)$ for some $g \in G$.

Theorem 2.39
Let G be a finite group and suppose that $\mathbb{C}[X]^G = \mathbb{C}[f_1, \ldots, f_m]$ then

1. *The polynomial mapping $F : \mathbb{C}^n \to V_F$ defined by*

$$F(a_1, \ldots, a_n) = (f_1(a), \ldots, f_m(a))$$

   is surjective i.e., it covers all of V_F.
2. *The map sending the G–orbit G_a to the point $F(a) \in V_F$ is a bijective map from $\mathbb{C}^n/G$ to V_F.*

3

Exploiting symmetries in SDP based relaxations for polynomial optimization

Ce qui embellit le désert, dit le petit prince, c'est qu'il cache un puits quelque part

Le petit prince
Antoine de Saint-Exupéry

ALTHOUGH the semidefinite relaxations for polynomial optimization problems introduced in the first section provide a way to attack otherwise hard problems in general the sizes of the resulting SDPs grow fast with the problem size:

Typically, the SDP-relaxation of order k in the hierarchy involves $O(n^{2k})$ variables and linear matrix inequalities (LMIs) of size $O(n^k)$. Therefore, and in view of the present status of SDP solvers, the applicability of the basic methodology is limited to small or medium size problems unless some specific characteristics are taken into account.

One of these characteristics is symmetry. Indeed a lot of problems for which one wishes to calculate the SDP relaxations are naturally equipped with a sort of symmetry. Therefore, exploiting this additional structure is one of the major techniques to reduce the computational effort that needs to be invested in order to solve these problems. This chapter develops two methods to exploit symmetries in the setting of SDP based relaxations for polynomial optimization. To this end we follow two distinct ways.

First we provide a systematic treatment of the block diagonalization in the setting of Lasserre's relaxation. Using the framework of linear representation theory we suggest a that a symmetry-adapted version of the relaxation scheme, that is block-diagonal can be defined directly using an appropriate basis for the moments. Further we show that under Putinar's condition (Assumption 1.33) the resulting sequence of approximations converges to the optimal value of the initial polynomial optimization problem.

Secondly we investigate the possibilities of exploiting symmetries in the context of the formulation of the polynomial optimization problems. This approach will be based on results from invariant theory. Namely we show how the description of the real part of the orbit space (Definition 2.3.7), which was initially given by Procesi and Schwarz, can be combined with Lasserre's Relaxation Scheme for Polynomial Matrix Inequality (PMI) problems (see Chapter 1.2.5) in order to design an relaxation scheme in the geometric quotient.

3.1 A block diagonal relaxation scheme

We assume that finite group G acts on $\mathbb{R}^n$ via a linear representation ρ and recall that to every $f \in \mathbb{R}[X]$ and $g \in G$ we can associate a polynomial $f^g := f(g^{-1}(X))$ hence G also acts on the ring of polynomials.

Let $g_1, \ldots, g_m \in \mathbb{R}[X]$ and K be the basic closed semialgebraic set defined by these polynomials. Via the linear representation ρ each $g \in G$ maps K to another semi algebraic set $\sigma(K)$ and we will denote

$$K^G := \bigcap_{g \in G} \sigma(K)\,.$$

In the sequel we will often assume that K is invariant under the action of G i.e., $K = K^G$. Note that this does not necessarily require that any of its generators g_i is invariant under the action of G on $\mathbb{R}[X]$.

Dually we can also define an action of G on the set of measures. For each measure μ with support in $\mathbb{R}^n$, ρ induces an action of G on $\Pi(\mathbb{R}^n)$ by setting $g(\mu(f)) := \mu(f^g)$.

A measure μ on K is said to be *G-invariant* if for all $f \in \mathbb{R}[X]$ and $g \in G$ we have

$$\int_K f\, d\mu \;=\; \int_K f^g\, d\mu \;=\; \int_{g^{-1}(K)} f\, d\mu,$$

and the subset of all invariant probability measures on K by $\Pi(K)^G$. For a comprehensive foundational treatment of invariant measures we refer to [CKS09]. Here, we mainly need the following simple connection:

Lemma 3.1
With the definitions above we have

1. *For any semi-algebraic set K we have $\Pi(K)^G = \Pi(K^G)^G$.*
2. *Let f be a G-invariant function then $\sup_{x \in K} f(x) = \sup_{\mu \in \Pi(K)^G} \int f d\mu$.*

Proof. (1) As K^G is contained in K the inclusion $\supseteq$ is obvious. For the other direction assume that $\mu \in \Pi(K)^G$ is such that $\mu(B) > 0$ for some $B \in \mathcal{B}$ with $B \not\subseteq K^G$.

Hence there is a $\sigma \in G$ such that $\mathcal{B}$ is not contained in $\sigma(K)$. But this implies that $\sigma^{-1}(\mathcal{B})$ is not contained in K which is a contradiction because μ is supposed to be invariant under the action of G.

(2) Let f be a G-invariant function and (x_k) be a sequence in K such that $(f(x_k))$ converges to $f^* = \sup_{x\in K} f(x)$. Recall that

$$\begin{aligned} f^* = \inf_{\mu\in\Pi(K)} \int f d\mu &\leq \inf_{\mu\in\Pi(K^G)} \int f d\mu \quad \text{as } K \subseteq K^G \\ &\leq \inf_{\mu\in\Pi(K^G)^G} \int f d\mu = \inf_{\mu\in\Pi(K)^G} \int f d\mu \,. \end{aligned}$$

To each x_k we can define a Dirac measure μ_k supported in x_k. Now this gives a converging sequence $(\int f(x)d\mu_k)$. Define the measures $\mu_k^* := \frac{1}{|G|}\sum_{\sigma\in G}\sigma(\mu_k)$, this implies $\mu_k^* \in \Pi(K)^G$ for every k.

Since f is G-invariant, $\int f(x)d\mu_k^* = f(x_k)$ which in turn implies $\int f(x)d\mu_k^* \to f^* \leq \inf_{\mu\in\Pi(K)^G} \int f d\mu$, and so $f^* = \inf_{\mu\in\Pi(K)^G} \int f d\mu$. □

So in order to find the supremum or infimum of an invariant function on an invariant set K we only have to consider the invariant measures supported on K. Hence to make a relaxation scheme for this setting similar to the one presented in the previous section, we only have to take those linear maps $L \in \mathrm{Hom}(\mathbb{R}[X], \mathbb{R})$ into account that are invariant with respect to G.

Generalizing Putinar's Theorem to this situation we can also characterize them by looking at bilinear forms.

Theorem 3.2
Let $g_1, \ldots, g_m$ be G-invariant, define $K := \{x \in \mathbb{R}^n : g_1(x) \geq 0, \ldots, g_m(x) \geq 0\}$, and let $L^s \in \mathrm{Hom}(\mathbb{R}[X], \mathbb{R})$ be a G-linear map. Suppose Assumption 1.29 holds for the set K and set $g_0 := 1$. Consider the bilinear forms

$$\begin{aligned} \mathcal{L}_{g_i}^s : \mathbb{R}[X] \times \mathbb{R}[X] &\to \mathbb{R} \\ (p, q) &\mapsto \frac{1}{|G|}\sum_{\sigma\in G} L^s(p \cdot q \cdot g_i^\sigma) \,. \end{aligned}$$

Then L^s is the integration with respect to an invariant probability measure on K if and only if $\mathcal{L}_{g_i}^s \succeq 0$ for all $0 \leq i \leq m$.

Proof. Suppose μ is a G-invariant measure supported in K. From Proposition 3.1 we deduce that for every polynomial g_i the measure μ is actually supported on

$$\bigcap_{\sigma\in G} \{x \in \mathbb{R}^n : g_i^\sigma(x) \geq 0\} \,.$$

Hence according to Theorem 1.22 the bilinear form $(p,q) \mapsto \frac{1}{|G|}\sum_{\sigma\in G} L(p\cdot q\cdot g^\sigma)$ is positive semi definite and therefore all the $\mathcal{L}^s_{g_i}$ are psd. On the other hand, if the forms $\mathcal{L}^s_{g_i}$ are positive semi definite then at least one of the summands also has to be. But the linear form L^s is invariant and thus every summand is positive semi definite. □

So an invariant optimization problem can be rephrased as

$$p^* \;=\; \inf\left\{L^s(p) \,:\, L^s \in \mathrm{Hom}(\mathbb{R}[X],\mathbb{R}) \text{ is } G\text{-linear}, L^s(1)=1 \text{ and each } \mathcal{L}^s_{g_i} \succeq 0\right\}. \quad (3.1)$$

Now we can make use of the results from representation theory. Namely as for every fixed $d \in \mathbb{N}$ the space $\mathbb{R}[X]_d$ of polynomials of degree at most d can be viewed as a G-module there exists a decomposition of the form (2.1)

$$\mathbb{R}[X]_d \;=\; V_1 \oplus V_2 \oplus \cdots \oplus V_h \quad (3.2)$$

with $V_i = W_{i1} \oplus \cdots \oplus W_{i\eta_i}$ and $\nu_i := \dim W_{ij}$. Here, the W_{ij} are the irreducible components and the V_i are the isotypic components i.e., the direct sum of isomorphic irreducible components. The component with respect to the trivial irreducible representation corresponds to the invariant polynomials of degree at most d. The elements of the other isotypic components are called *semi-invariants*.

From now on let us assume that all the g_i are G-invariant.

Recall that for any compact group G there is a scalar product $\langle\cdot,\cdot\rangle$ on $\mathbb{R}[X]$ which is G-invariant i.e., $\langle g, f\rangle = \langle g_\sigma, f_\sigma\rangle$ for every $f, g \in \mathbb{R}[X]$ and every $\sigma \in G$.

We assume a decomposition of $\mathbb{R}[X]_d$ like in (3.2) above, consider $V_i = W_{i1} \oplus \cdots \oplus W_{i\eta_i}$ and pick any $b_{i,1,1} \in W_{i1}$. Then using the fact that the W_{ij} are isomorphic for all j we can find $b_{i,j,1} \in W_{ij}$ such that $\phi_{i,j}(b_{i,j,1}) = b_{i,j+1,1}$, where $\phi_{i,j}$ is a G-isomorphism that maps $W_{i,j}$ to $W_{i,j+1}$. Now using for example by Gram-Schmidt every $b_{i,j,1}$ can be extended to an orthogonal basis of W_{ij}. As the resulting basis $\mathcal{B} = \{b_{1,1,1}, \ldots, b_{h,\eta_h,\nu_h}\}$ will be a *symmetry-adapted basis* of $\mathbb{R}[X]_d$ we can combine Schur's Lemma and the above generalization of Putinar's Theorem and deduce the following proposition:

Proposition 3.3
Let $g_1, \ldots, g_m$ be G-invariant, define $K := \{x \in \mathbb{R}^n \,:\, g_1(x) \geq 0, \ldots, g_m(x) \geq 0\}$, and let $L^s \in \mathrm{Hom}(\mathbb{R}[X],\mathbb{R})$ be a G-linear map. Suppose Assumption 1.29 holds for the set K and set $g_0 := 1$.

For every $d \in \mathbb{N}$ let $\mathbb{R}[X]_d$ be decomposed as in (3.2), take any symmetry-adapted basis $\mathcal{B}$ as described above and for all i define

$$\mathcal{S}_i := \{b_{i,1,1}, b_{i,2,1}, \ldots, b_{i,\eta_i,1}\}.$$

Then a G-linear map $L^s : \mathbb{R}[X] \to \mathbb{R}$ is the integration with respect to a measure μ supported on K if and only if every of the bilinear maps $\mathcal{L}^s_{g_i}$ restricted to all $\mathcal{S}_i$ is positive semidefinite.

Proof. By Proposition 3.2 we have to ensure that the bilinear maps $\mathcal{L}^s_{g_i}$ are psd. Now by Corollary 2.11 we have that on every irreducible component $W_{i,j}$ the Hermitian forms $\mathcal{L}^s_{g_i}$ and $\langle \cdot, \cdot \rangle_G$ agree up to a real multiplicative constant i.e., $\langle a, b \rangle_G = \lambda_{ij} \mathcal{L}^s_{g_i}(a \cdot b)$. But as every $b_{i,j,1}$ can be extended to an orthonormal (with respect to $\langle \cdot, \cdot \rangle_G$) basis of $W_{i,j}$, this in turn implies that $\mathcal{L}^s_{g_i}$ is positive semi definite if and only if its restrictions on every set $\mathcal{S}_i := \{b_{i,1,1}, b_{i,2,1}, \ldots, b_{i,\eta_i,1}\}$ are positive semi definite. □

We also record the following symmetric version of Putinar's Positivstellensatz.

Theorem 3.4
Let $f, g_1, \ldots, g_m \in \mathbb{R}[X]$ be G-invariant polynomials and consider

$$K = \{x \in \mathbb{R}^n \,:\, g_1(x) \geq 0, \ldots g_m(x) \geq 0\}\,.$$

If f is strictly positive on K, then

$$f = \sum_{s_i} \sigma_0^{s_i} + \sum_{k=1}^{m} g_k \sum_{s_i} \sigma_k^{s_i},$$

where $\sigma_j^{s_i} \in \Sigma\mathbb{R}[X]^2_{s_i}$ and $\mathbb{R}[X]_{s_i}$ denotes the i-th isotypic component of $\mathbb{R}[X]$.

Proof. If $f > 0$ on K, then also for the polynomial $f^G := \sum_{\pi \in G} f(\pi^{-1}(x))0$ we have $f^G > 0$ on K and hence $f = \frac{1}{|G|} f^G$. By applying the classical version of Putinar's Positivstellensatz f can be represented in the form

$$f = \sigma_0 + \sum_{k=1}^{m} g_k \sigma_k \text{ with } \sigma_0, \sigma_k \in \Sigma\mathbb{R}[X]^2.$$

Now by letting G act on this expression we get for f^G:

$$f^G = \underbrace{\sum_{\pi \in G} \sigma_0(\pi^{-1}(x))}_{=:\sigma_0'} + \sum_{k=1}^{m} \underbrace{\sum_{\pi \in G} g_k(\pi^{-1}(x))}_{=|G| g_k} \underbrace{\sum_{\pi \in G} \sigma_k(\pi^{-1}(x))}_{=:\sigma_k'}\,.$$

Thus we conclude that there is Putinar type representation of $f = \frac{1}{|G|} f^G$, with G-invariant SOS-polynomials $\frac{1}{|G|}\sigma_k'$. Now as was observed in [GP04] (Theorem 5.3) every G-invariant SOS polynomials σ_k' has a SOS-representation with sums of squares coming from the isotypic components. □

Now putting all this together we can derive the following: For every $k \in \mathbb{N}$ let $\mathcal{B}_k := \{b_1, b_2, \ldots\}$ be a basis of the real vector space of invariant polynomials in n variables of degree at most $2k$. Let $V_1, V_2, \ldots, V_h$ denote the distinct irreducible representations

of a given group G. Further let $\mathcal{S}_k^j := \left\{ s_1^j, s_2^j, \ldots, s_{\eta_j}^j \right\}$ contain the first elements of a symmetry-adapted basis for the polynomials of degree at most k. Then we define the *symmetry-adapted moment matrix* $M^s(y)$ by

$$M_k^s(y) := \bigoplus_j M_{k,j}^s(y), \text{ where } M_{k,j}^s(y)_{u,v} := \mathcal{L}^s(s_u^j \cdot s_v^j). \tag{3.3}$$

The entries of $M^s(y)$ are indexed by the elements of $\mathcal{B}_k$. Also we define the *symmetry-adapted localizing matrices* in a similar manner.

Let p_{b_i} denote the coefficients of p in the basis $\mathcal{B}$ and define the symmetry-adapted relaxation

$$Q_k^s : \begin{array}{rcl} \inf_y \sum_i p_{b_i} y_{b_i} & & \\ M_k^s(y) & \succeq & 0\,, \\ M_{k-\lceil \deg g_j/2 \rceil}^s(g_j\, y) & \succeq & 0\,, \quad 1 \le j \le m \end{array} \tag{3.4}$$

with optimal value denoted by $\inf Q_k^s$ (and $\min Q_k^s$ if the infimum is attained).

Remark 3.5
The symmetry-adapted setting defined above can give a significant reduction of the SDPs that need to be calculated. Indeed the number of variables involved equals the size of $\mathcal{B}_k$. Furthermore, the symmetry-adapted moment matrix is block diagonal and the size of each block equals η_i.

A generalization of Theorem 1.31 to this setting can now be reformulated as follows.

Theorem 3.6
Let Assumption 1.29 hold and let $(Q_k^s)_{k \ge k_0}$ be the hierarchy of SDP-relaxations defined in (3.4). Then $(\inf Q_k^s)_{k \ge k_0}$ is a monotone non-decreasing sequence that converges to p^* i.e., $\inf Q_k^s \uparrow p^*$ as $k \to \infty$.

Proof. As $\Pi(K)^G \subseteq \Pi(K)$ one has $\inf Q_k^s \ge \inf Q_k$ for all $k \ge k_0$. In addition, for any measure μ on K we let $\mu^\# = \frac{1}{|G|} \sum_{\sigma \in G} \sigma(\mu)$. As K is supposed to be G-invariant we have $\mu^\#$ is on K. This proves that $\inf Q_k^s \le p^*$ for all $k \ge k_0$, and so, $\inf Q_k \le \inf Q_k^s \le p^*$ for all $k \ge k_0$. Combining the latter with Proposition 1.31 yields the desired result. □

Remark 3.7
If not all g_i are invariant but the set K is invariant or even if just the set of optimal values is invariant, one still can only look at invariant moments. However the above block structure will only apply for the moment matrix and the localizing matrices for the invariant polynomials. Note that however still the variables in the localizing matrices correspond to a basis for the space of invariants.

We will study the resulting hierarchy for the case of the symmetric group in chapter 5.

3.2 PMI-relaxations via the geometric quotient

As a second possibility to explore symmetries we will use the techniques of Invariant theory as presented in chapter 2 namely the characterization of the orbit space. This approach leads very naturally to polynomial matrix inequalities (PMI). The key feature of this procedure is that in some cases, this can decrease the degrees of the polynomials strongly. In chapter 5 we will demonstrate this phenomenon in a certain case for symmetric power sum problems, where we will use this approach in order to obtain easy to calculate lower bounds and sometimes even upper bounds for these minimization problems by a very simple SDP relaxation.

Recall from Theorem 2.34 that the ring $\mathbb{C}[X]^G$ is finitely generated and the coordinate ring of an algebraic variety, the so called orbit space. The Hilbert map $\pi : \mathbb{C}^n \to \mathbb{C}^m$ associated to the inclusion $\mathbb{C}[X]^G \subseteq \mathbb{C}[X]$ discussed in Theorem 2.39 provides a surjective homomorphism from $\mathbb{C}^n$ to this orbit space.

In order to study optimization problems we need to restrict to the reals instead to work with complex numbers. In contrast to the algebraically closed case the problem is that if we restrict π to $\mathbb{R}^n$ in general, the resulting map $\tilde{\pi}$ will not be surjective. Nevertheless, the projection

$$\begin{array}{rcl} \tilde{\pi} : \mathbb{R}^n & \to & \mathbb{R}^n/G \subseteq \mathbb{R}^m \\ x & \mapsto & (\pi_1(x), \ldots, \pi_m(x)) \end{array}$$

defines an embedding of the orbit space into $\mathbb{R}^m$. We highlight this phenomenon with the following example:

Example 3.8
Let $G = D_4$ be the dihedral group acting on $\mathbb{R}^2$. In this case fundamental invariants that generate $\mathbb{C}[X, Y]^{D_4}$ are given by $f_1 = x^2 + y^2$ and $f_2 = x^2y^2$. As f_1 and f_2 are in fact algebraically independent, we find that $\mathbb{C}^n/D_4 \simeq \mathbb{C}^2$. Now we restrict the map π to $\mathbb{R}^2$. Obviously, the image of $\pi(\mathbb{R}^2)$ is contained in $\mathbb{R}^2$. On the other hand, as $f_1(x, y) \geq 0$ for all $(x, y) \in \mathbb{R}^2$, we find that $\pi^-1(-1, 0) \notin \mathbb{R}^2$. Therefore, the restricted map $\tilde{\pi}$ is not surjective.

Therefore, in oder to describe the image of $\mathbb{R}^n$ under $\tilde{\pi}$ we need add further constraints. In the above example for instance it is clear that as $f_1(x, y) \geq 0$ for all $(x, y) \in \mathbb{R}^n$ we must have that $\tilde{\pi}(\mathbb{R}^2) \subseteq \{(z_1, z_2) \in \mathbb{R}^2 : z_1 \geq 0\}$. In view of the example it seems therefore promising to add such positivity constraints to characterize the image $\tilde{\pi}(\mathbb{R}^n)$ as a semi algebraic subset of $\mathbb{R}^n$. This is in fact possible and the characterization has been done by Procesi and Schwarz, who have determined polynomial inequalities which have to be taken additionally into account in order to characterize the embedding of $\mathbb{R}^n/G$ into the coordinate variety of the invariant ring of G (see also Bröcker [Brö98]) and we will outline this briefly:

As G is a finite group we know that there exists a G-invariant inner product $\langle \cdot, \cdot \rangle$. For a polynomial p the differential dp is defined by $dp = \sum_{j=1}^{n} \frac{\partial p}{\partial x_j} dx_j$. Then carrying over the inner product to the differentials yields $\langle dp, dq \rangle = \sum_{j=1}^{n} \frac{\partial p}{\partial x_j} \cdot \frac{\partial q}{\partial x_j}$. The inner products $\langle d\pi_i, d\pi_j \rangle$ $(i, j \in \{1, \ldots, m\})$ are G-invariant, and hence every entry of the symmetric matrix

$$J \;=\; (\langle d\pi_i, d\pi_j \rangle)_{1 \le i,j \le m}$$

is G-invariant.

Following the ideas of [PS85] this construction now can be used to describe the real part of the orbit space.

Theorem 3.9 (Procesi, Schwarz)
Let $G \subseteq \mathrm{GL}_n(\mathbb{R})$ be a compact matrix group, and let $\pi = (\pi_1, \ldots, \pi_m)$ be fundamental invariants of G. Then the orbit space is given by polynomial inequalities,

$$\mathbb{R}^n/G \;=\; \pi(\mathbb{R}^n) \;=\; \{z \in \mathbb{R}^n \,:\, J(z) \succeq 0,\, z \in V(I)\}\,,$$

where $I \subseteq \mathbb{R}[z_1, \ldots, z_m]$ is the ideal of relations of $\pi_1, \ldots, \pi_m$.

Example 3.10
Let us explore this result by continuing the above example. We have $\frac{\partial f_1}{\partial x} = 2x$, $\frac{\partial f_1}{\partial y} = 2y$, $\frac{\partial f_2}{\partial x} = xy^2$, $\frac{\partial f_2}{\partial y} = x^2 y$. This yields the matrix

$$A = \begin{pmatrix} 4(x^2+y^2) & 8x^2y^2 \\ 8x^2y^2 & 4(x^2y^4 + y^2x^4) \end{pmatrix}.$$

Now we translate the entries of A into the two invariants f_1 and f_2 and get

$$J = \begin{pmatrix} 4f_1 & 8f_2 \\ 8f_2 & 4f_1f_2 \end{pmatrix}.$$

The principle minors of J are $4f_1$, $4f_1f_2$ and $4f_1 \cdot 4f_1f_2 - (8f_2)^2$. With these we can characterize $\pi(\mathbb{R}^2)$ as

$$\mathbb{R}^2/D_4 := \left\{(z_1, z_2) \in \mathbb{R}^2 \,:\, 4z_1 \ge 0,\, 4z_1z_2 \ge 0,\, 4z_1z_2.(8z_2)^2 \ge 0\right\}.$$

Let $\tilde{p}$ and $\tilde{g_1}, \ldots, \tilde{g_m}$ be the expressions for p and $g_1, \ldots g_m$ in the primary invariants. By Theorem 3.9, the G-symmetric optimization problem (1.5) can be equivalently expressed in the orbit space:

$$\begin{aligned} &\inf \tilde{p}(z) \\ &\text{s.t.} \quad z \in V(I)\,, \\ &\qquad \tilde{g_1}(z) \ge 0, \ldots, \tilde{g_m}(z) \ge 0, \\ &\qquad J(z) \succeq 0\,. \end{aligned} \tag{3.5}$$

This is a PMI (as introduced in Section 1.2.5) and one can use the techniques introduced there to derive an SDP relaxation scheme. Let $s_1(z), \ldots, s_t(z)$ be the t algebraic relations between the fundamental invariants $\pi_1, \ldots \pi_m$. Then we can build the following sequence of SDP relaxations

$$Q_k^q : \quad \begin{array}{rcll} \inf_y \sum_\alpha p_\alpha y_\alpha & & & \\ M_k(y) & \succeq & 0\,, & \\ M_{k-m}(J * y) & \succeq & 0\,, & \\ M_{k-\lceil \deg \tilde{g}_j/2 \rceil}(\tilde{g}_j\, y) & \succeq & 0 \text{ for } & 1 \leq j \leq m, \\ M_{k-\lceil \deg s_l/2 \rceil}(s_l\, y) & = & 0 \text{ for } & 1 \leq l \leq t. \end{array} \qquad (3.6)$$

Theorem 3.11
Let $p, g_1, \ldots, g_m$ be G invariant. If the PMI in (3.6) meets condition 1.33 the sequence $(\inf Q_k^q)_{k \geq k_0}$ is monotone non-decreasing and converges to p^*; that is,

$$\inf Q_k^q \uparrow p^* \text{ as } k \to \infty.$$

Proof. By Theorem 3.9 the problem described by p and $g_1, \ldots, g_m$ is equivalent to 3.5. Now we can conclude with Theorem 1.34. □

Remark 3.12
It would be very interesting to characterize the situations where 3.9 meets condition 1.33 in terms of the original set K, in particular those situations where both of the resulting SDP relaxations converge.

4

Positivity for symmetric polynomials

> The chief forms of beauty are order and symmetry and definiteness, which the mathematical sciences demonstrate in a special degree
>
> *Metaphysics*
> Aristotle

CERTIFYING that a given polynomial in n real variables is positive had been one of the main motivations leading to the development of modern real algebraic geometry. In this chapter we are going to investigate the positivity question for symmetric polynomials from an optimization point of view. Many optimization problems that are given in a symmetric setting share the pleasant property that their solutions can be found among the symmetric points, i.e., the points that are invariant to the action of the symmetric group. The best known elementary example for instance is that among all rectangles with given perimeter $a+b$ the square maximizes the area. This was already observed by Terquem who postulated in [Ter40] this to be a general fact. Contrary to this postulate it was observed already some rears after Terquem by the Russian mathematician Bouniakovsky [Bou54] that in general there does not need to be a symmetric point amongst the minimizers of a symmetric problem.

The main result presented in this chapter will analyze how much symmetry will be passed on to the minimal points of general symmetric polynomials under symmetric constraints. We will show that the symmetry of minimizers is depending mainly on the degree of the polynomials involved.

When turning this result back to the positivity side of global optimization we recover a theorem which was initially proven by Vlad Timofte [Tim03], who established this result via the bounded solutions of a differential equation. Although his proof is correct, it does not fully visualize the situation. The reduction from Theorem 4.2 allows us to establish Timofte's theorem in a more natural way.

Further we will explain the connection to a theorem of Foregger [For87]. It was pointed out to us by Salma Kuhlmann and Alexander Kovačec [KK10] that Foregger's attempt to prove his statement seems to be flawed. We will point out why it is in fact to be beyond repair and also give a correct reasoning based on the proof of Theorem 4.2 in the discussion at the end.

Finally, we will remark in the discussion at the end of this chapter that a similar result holds for even symmetric polynomials.

4.1 The statements

The points in $\mathbb{R}^n$ that are invariant with respect to the permutation action of the symmetric group $\mathcal{S}_n$ are precisely those consisting only of one distinct component. The more distinct the components of a point x are, the less symmetric is x. So the following definitions can be seen as a measure of symmetry:

Definition 4.1

1. For $x \in \mathbb{R}^n$ let $n(x) = \#\{x_1, \ldots, x_n\}$ denote the number of distinct components of x and $n^*(x) = \#\{x_1, \ldots, x_n \,|x_j \neq 0\}$ denote the number of distinct non zero elements.
2. For $d \in \mathbb{N}$ let $A_d := \{x \in \mathbb{R}^n : n(x) \leq d\}$ i.e., the points in $\mathbb{R}^n$ with at most d distinct and $A_d^+ := \left\{x \in \mathbb{R}_+^n : n^*(x) \leq d\right\}$ i.e points with at most d distinct positive elements.

So for example A_1 consists of the symmetric points.

Using these sets as a measure of symmetry the following theorem will be the essence of this chapter.

Theorem 4.2
Let $F_0, F_1, \ldots, F_m \in \mathbb{R}[X]^{S_n}$ be symmetric and

$$K = \{x \in \mathbb{R}^n \,:\, F_1(x) \geq 0, \ldots, F_m(x) \geq 0\}\,.$$

If F_0 is of degree d and $k := \max\{2, \lfloor \frac{d}{2} \rfloor, \deg F_1, \ldots, \deg F_m\}$ then

$$\begin{aligned} \inf_{x \in K} F_0(x) &= \inf_{x \in K \cap A_k} F_0(x) \text{ and} \\ \inf_{x \in K \cap \mathbb{R}_+^n} F_0(x) &= \inf_{x \in K \cap A_k^+} F_0(x). \end{aligned}$$

So although it is true that the minimizers need not to be amongst the fully symmetric points our statement shows that some of the symmetry still can be expected when looking for the minima. In Chapter 5 we will show how Theorem 4.2 can be used to exploit

symmetry in the context of solving symmetric optimization problems. As an immediate consequence we note the following implications for deciding emptiness of real algebraic varieties given by symmetric polynomials i.e., the question if a system of symmetric equations has a real solution:

Corollary 4.3 (Degree principle)
Let $F_1, \ldots, F_k \in \mathbb{R}[X]^{\mathcal{S}_n}$ be symmetric polynomials of degree at most d. Then the real variety

$$V_{\mathbb{R}}(F_1, \ldots, F_k)$$

is empty if and only if

$$V_{\mathbb{R}}(F_1, \ldots, F_k) \cap A_d$$

is empty.

Proof. Let $F_0 := x_1 + \ldots + x_n$. Now as

$$\inf_{x \in V_{\mathbb{R}}(F_1,\ldots,F_k)} F_0(x) < \infty \text{ if and only if } V_{\mathbb{R}}(F_1, \ldots, F_k) \neq \emptyset$$

we can conclude with Theorem 4.2. □

As was already mentioned also the following statement due to Timofte is an immediate corollary:

Corollary 4.4 (Half degree principle for inequalities)
Let $F \in \mathbb{R}[X]^{\mathcal{S}_n}$ be a symmetric polynomial of degree d and define $k := \max\left\{2, \lfloor \frac{d}{2} \rfloor\right\}$. Then F is non negative i.e., $F(x) \geq 0$ for all $x \in \mathbb{R}^n$ if and only if $F(y) \geq 0$ for all $y \in A_k$. Further F is copositive, i.e., $F(x) \geq 0$ for all $x \in \mathbb{R}^n_+$ if and only if $F(y) \geq 0$ for all $y \in A^+_k$.

Proof. This follows immediately from Theorem 4.2 as for all F_0 we have $F_0 \geq 0$ if any only if $\inf_{x \in \mathbb{R}^n} F_0 \geq 0$. □

In addition to the inequality case it was pointed out by David Grimm [Gri05] that as A_k is connected for all k we also can deduce a half degree principle for symmetric real hypersurfaces from the above corollary:

Corollary 4.5 (Half degree principle for hypersurfaces)
Let $F_0 \in \mathbb{R}[X]^{\mathcal{S}_n}$ be of degree d and let $k := \max\left\{2, \lfloor \frac{d}{2} \rfloor\right\}$. Then there is $x \in \mathbb{R}^n$ with $F_0(x) = 0$ if and only if there is $x \in A_k$ with $F_0(x) = 0$.

Proof. Suppose there is no $y \in A_k$ with $F(y) = 0$. As A_k is connected and F_0 continuous we find that either $F_0(x) > 0$ or all $x \in A_k$ or $F_0(x) < 0$ for all $x \in A_k$. This in any case

implies that F_0 is either strictly positive or strictly negative and thus we can interfere that F_0 has no zeros. □

Remark 4.6
In view of the second corollary it seems natural to ask, if the half degree principle does in general also apply to any system of symmetric equalities. However, if one considers the set $K := \{x \in \mathbb{R}^n : x_1 + x_2 + x_3 = 0, x_1^2 + x_2^2 + x_3^2 = 1, x_1^3 + x_2^3 + x_3^3 = 0\}$, one finds K is not empty but $K \cap A_2$ is empty.

Besides symmetric polynomials, also even symmetric polynomials can be of interest. A polynomial f is called *even symmetric* if it is symmetric and involves only monomials of even degree. Alternatively, f is invariant by the hyper-octahedral group $\mathcal{S}_n \wr \mathcal{S}_2$. We will show in the discussion at the end that using the proof of Theorem 4.2 we are able to directly deduce the corresponding theorem for even symmetric polynomials:

Theorem 4.7
Let $F_0, F_1, \ldots, F_m \in \mathbb{R}[X]^{\mathcal{S}_n}$ be even symmetric consider

$$K = \{x \in \mathbb{R}^n : F_1(X) \geq 0, \ldots, F_m(X) \geq 0\}.$$

If F_0 is of degree $2d$ and $k := \max\left\{\lfloor \frac{d}{2} \rfloor, \deg F_1, \ldots, \deg F_m\right\}$, then

$$\inf_{x \in K} F_0(x) = \inf_{x \in K \cap A_k} F_0(x).$$

On the way to prove Theorem 4.2 we will examine critical points of linear functions on the orbit space of $\mathcal{S}_n$. This will also provide a proof of the following theorem which was originally published by Foregger in [For87].

Theorem 4.8
Let $n \geq 2$, let $\phi(x) = \phi(x_1, \ldots, x_n)$ be a real linear combination of elementary symmetric polynomials, and define

$$C_\gamma := \left\{ x \in [0,1]^n : \sum_{i=1}^{n} x_i = \gamma \right\}.$$

Suppose $\phi : C_\gamma \to \mathbb{R}$ attains at a point $\underline{a} \in \operatorname{int}(C_\gamma)$, the relative interior of C_γ, a local extremum. Then ϕ is constant or $\underline{a}$ is the symmetric point in C_γ, i.e., $\underline{a} = (\frac{\gamma}{n}, \frac{\gamma}{n}, \ldots, \frac{\gamma}{n})$.

The new proof we give in the final discussion seems necessary since we will show that the original proof given by Foregger in [For87] is beyond repair.

4.2 Symmetric polynomials and the orbit space of $\mathcal{S}_n$

Symmetric polynomials are a very classical object of study which appeared naturally already in study of the formation of coefficients of polynomials from their roots. In fact the classical formula of Vieta will have a prominent importance for the proof of Theorem 4.2.

The group $\mathcal{S}_n$ is finite and therefore from Hilbert's Finiteness Theorem 2.34 we can interfere that there is a finite set of polynomials generating the ring $\mathbb{C}[X]^{S_n}$ of invariant polynomials. Among the possible polynomials for this generating set the following two families are of special interest:

Definition 4.9
For $n \in \mathbb{N}$, we consider the following two families of symmetric polynomials.

1. For $0 \leq k \leq n$ let $p_k := \sum_{i=i}^{k} X_i^k$ denote the k-th power sum polynomial
2. For $0 \leq k \leq n$ let $e_k := \sum_{1 \leq i_1 < i_2 < \ldots < i_k \leq n} X_{i_1} X_{i_2} \cdots X_{i_k}$ denote the k-th elementary symmetric polynomial

These two families of symmetric polynomials are linked to each other by the so called Newton identities (see e.g. [Mea92]):

$$k(-1)^k e_k + \sum_{i=1}^{k} (-1)^{i+k} p_i e_{k-i} = 0. \tag{4.1}$$

As already indicated above the importance of the two families comes from the fact that they generate the invariant ring in this case, i.e., we have the following:

Theorem 4.10
Let $\mathcal{R}$ be any ring. Then the ring of symmetric polynomials $\mathcal{R}[X]^{S_n}$ is a polynomial ring in the n elementary symmetric polynomials $e_1, \ldots, e_n$, i.e. every symmetric polynomial F can uniquely be written as $F = G(e_1, \ldots, e_n)$ for some polynomial $G \in \mathcal{R}[X]$.

Proof. Let F be a symmetric polynomial and we are going to compare the monomial involved in F using lexicographic order on the degrees i.e., $x_1^{\alpha_1} \cdots x_n^{\alpha_n} \geq_{Lex} x_1^{\beta_1} \cdots x_n^{\beta_n}$ if $\sum \alpha_i > \sum \beta_i$ or if the first non zero element of the sequence $(\alpha_i - \beta_i)$ is positive.

Let $a \cdot x_1^{\gamma_1} \cdots x_n^{\gamma_n}$ be the biggest monomial with respect to the Lex-order. As F is supposed to be symmetric it follows that $\gamma_1 \geq \gamma_2 \geq \cdots \geq \gamma_n$. Now we consider the polynomial $H := a \cdot e_1^{\gamma_2 - \gamma_1} \cdot e_2^{\gamma_3 - \gamma_2} \cdots e_n^{\gamma_n}$. The greatest monomial of H is equal to $a \cdot x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ hence if we consider $\tilde{F} = F - H$ this term will get lost. Now we can use the same arguments with $\tilde{F}$. As the leading monomial of each step will be canceled this procedure will terminate and give us a description of F as polynomial in the elementary symmetric polynomials

$e_1, \ldots, e_n$. It remains to show that this representation is unique, i.e., that $e_1, \ldots, e_n$ are really algebraically independent. Suppose, that there is $0 \neq G \in \mathcal{R}[z_1, \ldots, z_n]$ such that $g(e_1(x), \ldots, e_n(x))$ is identically zero. Now consider any monomial $z_1^{a_1} \cdots z_n^{a_n}$ of G then the initial monomial of $e_1^{a_1} \cdots e_n^{a_n}$ will be $x_1^{a_1+a_2+\ldots+a_n} x_2^{a_1+a_2+\ldots+a_n} \cdots x_n^{a_1+a_2+\ldots+a_n}$. But as the linear map

$$(a_1, \ldots, a_n) \mapsto (a_1 + \ldots + a_n, a_2 + \ldots + a_n, \ldots, a_n)$$

is injective, all other monomials of G will have different initial monomial. The lexicographically largest monomial is not cancelled by any other monomial, and therefore $G(e_1, \ldots, e_n) \neq 0$. □

We remark that due to the Newton identities 4.1 every $e_i(x)$ can be expressed uniquely using the power sum polynomials. Hence we get the following corollary immediately:

Corollary 4.11
Let $\mathcal{R}$ be a ring of characteristic 0. Then the ring of symmetric polynomials $\mathcal{R}[X]^{S_n}$ is a polynomial ring in the first n power sum polynomials $p_1, \ldots, p_n$.

Let F be a given real symmetric polynomial of degree $d \leq n$, then the above theorem can be used to further analyze the elementary symmetric polynomials that need to be taken into consideration. We find in fact:

Proposition 4.12
Let $F \in \mathbb{R}[X]$ be symmetric of degree d. Then there is unique polynomial $G \in \mathbb{R}[Z_1, \ldots, Z_d]$ of the form

$$G = G_1(Z_1, \ldots, Z_{\lfloor \frac{d}{2} \rfloor}) + \sum_{i=\lfloor \frac{d}{2} \rfloor + 1}^{d} G_i(Z_1, \ldots Z_{d-i}) Z_i, \tag{4.2}$$

with $G_i \in \mathbb{R}[Z_1, \ldots, Z_d]$ such that

$$F = G(e_1, \ldots, e_d).$$

Proof. A proof for the announced expression of G in equation (4.2) can be given by carefully inspecting the above constructive proof of Theorem 4.10 But we will deduce the claim directly from the statement in Theorem 4.10. Let $G \in \mathbb{R}[Z_1, \ldots, Z_n]$ be the unique polynomial with $F = G(e_1, \ldots, e_n)$. Take a finite set $I \subset \mathbb{Z}^n_{\geq 0}$ such that $G = \sum_{i \in I} g_i Z_1^{i_1} \cdots Z_n^{i_n}$, with $g_i \in \mathbb{R}$. As $e_1^{i_1} \cdots e_n^{i_n}$ is a homogeneous polynomial of degree $i_1 + 2i_2 + \cdots + ni_n$ and $\deg F = d$, we infer $g_i = 0$ for all i with $\sum_l l i_l > d$. Now assume that $j \geq \lfloor \frac{d}{2} \rfloor + 1$ and $i_j \geq 1$. Then the condition $\sum_l l i_l \leq d$ implies first that $i_j = 1$ and further that $i_k = 0$ for all $k > d - j$. This means that the sum of terms of G that contain Z_j with $j \geq \lfloor \frac{d}{2} \rfloor + 1$ can be written in the form $\sum_{j=\lfloor \frac{d}{2} \rfloor}^{d} G_j(Z_1, \ldots Z_{d-j}) Z_j$ for certain polynomials G_j. Finally

combining all the other terms of G into a polynomial $G_1(Z_1, \ldots, Z_{\lfloor \frac{d}{2} \rfloor})$ we arrive at the above representation. □

To emphasize the impact that the above proposition has for the considerations in this chapter note that by Proposition 4.12 we have for the polynomial $G \in \mathbb{R}[Z_1, \ldots, Z_n]$ representing F in elementary symmetric polynomials the following:

1. There will be no monomial that contains a variable $Z_j, j > d$.
2. There will be no monomial that contains two variables Z_j, Z_i with $i, j \geq \lfloor \frac{d}{2} \rfloor$.
3. The variables Z_j with $i \geq \lfloor \frac{d}{2} \rfloor$ occur at most linearly in every monomial.

These properties in mind clearly it would be preferable to work with the polynomial function $G : \mathbb{R}^n \to \mathbb{R}$ instead of F. As was exposed in Chapter 2 this is possible if one works over an algebraically closed field as the Hilbert map $\pi : \mathbb{C}^n \to \mathbb{C}^n/S_n$ is surjective in this case (see Theorem 2.39).

Although we have seen the general machinery to describe the real part of the orbit space in the last chapter, in the case of the symmetric group this can be even seen more elementary by the following geometrical arguments:

Every $x \in \mathbb{C}^n$ can be viewed as the n roots of the univariate polynomial

$$f = \prod_{i=1}^{n} (T - x_i).$$

The classical Vieta formula implies that f can also be written as

$$f = T^n - e_1(x)T^{n-1} + \ldots \pm e_n(x).$$

Using geometric language the identification of the n roots with the n coefficients can be thought of as giving rise to a surjective map

$$\begin{array}{rccc} \pi : & \mathbb{C}^n & \longrightarrow & \mathbb{C}^n \\ & x := (x_1, \ldots, x_n) & \longmapsto & \pi(x) := (e_1(x), \ldots, e_n(x)) \end{array}.$$

Obviously π is constant on $\mathcal{S}_n$ orbits and hence the ring $\mathbb{C}[X]^{\mathcal{S}_n}$ is exactly the coordinate ring of the image of π which thus coincides with the *orbit space*.

It is worth mentioning that π has very nice continuity properties: Obviously the coefficients of a univariate polynomial f depend continuously on the roots, but also the converse is true:

Theorem 4.13
Let $f = \prod_{i=1}^{k} (T - x_i)^{m_i} = \sum_{j=0}^{n} a_j T^j$ be a univariate polynomial and define $0 < \varepsilon < |\min_{i \neq j} x_i - x_j|/2$. Then there is $\delta > 0$ such that every polynomial $g = \sum_{j=0}^{n} b_j T^j$ with coefficients satisfying $|a_j - b_j| < \delta$ has exactly m_i zeros in the disk around x_i with radius ε.

Proof. See for example Theorem. 1.3.1 in [RS02] . □

As we want to know about the points having real pre-image we will restrict π to $\mathbb{R}^n$. In this case the restriction maps into $\mathbb{R}^n$ but it fails to be surjective: Already the easy example X^2+1 shows that we can find n real coefficients that define a polynomial with strictly less than n real zeros. Polynomials with real coefficients that only have real roots are sometimes called *hyperbolic*. The right tool to characterize the univariate hyperbolic polynomials is the so called Sylvester-Matrix:
Let K be any field of characteristic 0 and take $f = T^n + a_1T^{n-1} + \ldots + a_n \in K[T]$ a univariate normalized polynomial. Its n zeros $\alpha_1, \ldots, \alpha_n$ exist in the algebraic closure of K. For $r = 0, 1, \ldots$ let $p_r(f) := \alpha_1^r + \ldots + \alpha_n^r$ be the r-th power sum evaluated at the zeros of f. Although it seems that this definition involves the a priori not known algebraic closure of K and the roots of f, which are also not known a priori, these numbers are well defined. We have $p_r(f) \in K$ and using Vieta and the Newton relations, we can express the power sums as polynomials in the coefficients of f.

Definition 4.14
The Sylvester Matrix $S(f)$ of a normalized univariate polynomial of degree n is given by

$$S(f) := (p_{j+k-2}(f))_{j,k=1}^{n}.$$

Without too much abuse of notation we will use $S(z)$ for every $z \in R^n$ to denote the Sylvester Matrix of corresponding polynomial whose coefficients are z.

Now the key observation we will need is Sylvester's version of Sturm's theorem.

Theorem 4.15
Let R be a real closed field and $f \in R[T]$ a normalized polynomial of degree $n \geq 1$.

1. *The rank of $S(f)$ is equal to the number of distinct zeros of f in the algebraic closure $R(\sqrt{-1})$.*
2. *The signature of $S(f)$ is exactly the number of real roots of f.*

See for example [KS89, BPR06] or [Syl53] for proofs of the above statements.

Remark 4.16
If one choses the set of elementary symmetric polynomials $e_1(x), \ldots, e_n(x)$ as primary invariants and proceeds according to the theory used in Section 2 of Chapter 3, one finds that the Sylvester Matrix agrees (up to a scalar factor) with the matrix J in Theorem 3.9 in this case.

Using the above theorem we see that $f \in \mathbb{R}[T]$ is hyperbolic if and only if $S(f)$ is positive semidefinite (denoted by $S(f) \succeq 0$). Now the strategy in order to prove Theorem 4.2 is to

take the view point of the real orbit space. Instead of F on $\mathbb{R}^n$, we will have to examine G over the set

$$\mathcal{H} := \{z \in \mathbb{R}^n : T^n - z_1 T^{n-1} + \ldots \pm z_n \text{ has only real roots}\}$$

and the sets

$$\mathcal{H}^k := \{z \in \mathcal{H} : T^n - z_1 T^{n-1} + \ldots \pm z_n \text{ has at most } k \text{ distinct zeros}\}.$$

So Theorem 4.2 follows directly from the following

Theorem 4.17
Let $F \in \mathbb{R}[X]$ of degree $d \geq 2$ and $G \in \mathbb{R}[Z_1, \ldots, Z_d]$ such that $F = G(e_1, \ldots e_d)$. Then we have:

1. $G(\mathcal{H}) = G(\mathcal{H}^d)$,
2. $\inf_{z \in \mathcal{H}} G(z) = \inf_{z \in \mathcal{H}^k} G(z)$ *for all* $2 \leq \lfloor d/2 \rfloor \leq k \leq n$,
3. $\inf_{z \in \mathcal{H} \cap \mathbb{R}^n_+} G(z) = \inf_{z \in \mathcal{H}^k \cap \mathbb{R}^n_+} G(z)$ *for all* $2 \leq \lfloor d/2 \rfloor \leq k \leq n$.

Before we give the proof of the above theorem and thus the proof of Theorem 4.2, we will need some very elementary facts about polynomials with only real roots. We will show these facts about hyperbolic polynomials in the next section.

4.3 Hyperbolic polynomials

The main problem that we will have to deal with in order to prove the main theorems is the question which changes of the coefficients of a hyperbolic polynomial will result in polynomials that are still hyperbolic. This question is in fact very old and has already been studied by Pólya, Schur and Szegő (see for example [Obr63, PS14, PS98]). However, we will argue that already some implications of the following classical statements on the roots of real univariate polynomials which can be found for example in [Kat84, Obr63, PS98] will be sufficient to prove the main statements.

Proposition 4.18
Let $f \in \mathbb{R}[T]$. Then the following hold:

1. *The n complex roots of f depend continuously on the coefficients, i.e. there are n continuous functions $r_1, \ldots, r_n$ depending on the coefficients that parametrize the roots.*

2. *If $\alpha \in \mathbb{C}$ is a root of f then also its complex conjugate $\bar{\alpha} \in \mathbb{C}$ is a root of f.*
3. *Let $a, b \in \mathbb{R}$ with $a < b$ and $f(a) = f(b) = 0$. Then the derivative polynomial f' has a root in (a, b).*

Now the following statements on hyperbolic polynomials follow immediately from these facts by careful inspection of the possible roots.

Corollary 4.19
Let $f = T^n + a_1 T^{n-1} + \ldots + a_n$ be hyperbolic. Then the following hold:

1. *Let $a, b \in \mathbb{R}$ with $a \leq b$. If f has k roots (counted with multiplicities) in $[a, b]$ then f' has at least $k - 1$ roots in $[a, b]$ (also counted with multiplicities).*
2. *All higher derivatives of f are also hyperbolic.*
3. *If $a \in \mathbb{R}$ is a root of order k of f' then a is also a root of order $k + 1$ of f.*
4. *If $a_i = a_{i+1} = 0$ then $a_j = 0$ for all $j \geq i$.*

Proof. Let $t_1 < x_2 < \ldots < t_p$ be the distinct real roots of f and assume $d_1, \ldots, d_p$ as respective multiplicities.

(1) If $a = b$ then f has a multiple root of order d_j at $t_j = a$. Hence its derivative has a root of order $d_j - 1$ at t_j. If $a < b$ at each t_i the derivative f' has a root of order $d_i - 1$. Further from Proposition 4.18 (3) we see that f' has a root in each open interval (t_i, t_{i+1}). Hence in total f' has at least $d_1 - 1 + d_2 - 1 + \ldots + d_k - 1 + (k - 1) = d - 1$ zeros.

(2) f has n zeros on the real line and by (1) it follows from Proposition 4.18 (3) that f' has its $n - 1$ roots on the real line, and so by induction all further derivatives are also hyperbolic.+

(3) Otherwise the number of roots does not match.

(4) If $a_i = a_{i+1} = 0$ there is a derivative of f with a multiple root at $t = 0$. But then $t = 0$ is also a multiple root of f of order $n - i + 1$ hence $a_j = 0$ for all $j \geq i$. □

As already mentioned we want to know, which small perturbations of coefficients of a hyperbolic polynomial will result in a hyperbolic one.

Proposition 4.20
Let $f \in \mathbb{R}[T]$ be a hyperbolic polynomial of degree n with exactly k distinct roots.

(a) If $k = n$ then for any non zero polynomial g of degree at most n there exists $\delta_n > 0$ such that for $0 < \varepsilon < \delta_n$ the polynomials $f \pm g$ are also hyperbolic with n distinct roots.

(b) If $k < n$ then for each $1 \leq s \leq k$ there is a polynomial g_s of degree $n - s$ and a $\delta_s > 0$ such that for all $0 < \varepsilon < \delta_s$ the polynomials $f \pm \varepsilon g_s$ are also hyperbolic and have strictly more distinct zeros.

Proof. (a) This follows directly by Proposition 4.18 (1) and (2).

(b) Let $x_1, \ldots, x_k$ be the distinct roots of f. We can factor

$$f = \underbrace{\left(\prod_{i=1}^{s}(T - x_i)\right)}_{:=p} \cdot g_1,$$

where the set of zeros of g_1 contains only elements from $\{x_1, \ldots x_k\}$ and g_1 is of degree $n - s$. Now we can apply (a) to see that $p \pm \varepsilon_s$ is hyperbolic for all $\varepsilon_s < \delta_s$. Furthermore we see that $p \pm \varepsilon_s$ has none of its roots in the set $\{x_1, \ldots, x_k\}$. Hence $(p \pm \varepsilon_s) \cdot g_1 = f \pm \varepsilon_s g_1$ is hyperbolic and has more than k distinct roots.

□

As we also want restrict to $\mathbb{R}^n_+$ the following easy observation will also be useful:

Proposition 4.21
The map π maps $\mathbb{R}^n_+$ onto $\mathcal{H}_+ := \mathbb{R}^n_+ \cap \mathcal{H}$.

By definition of the set $\mathcal{H}_+$ it could be possible that there are all sorts of polynomials with zero coefficients. But to conclude the main theorem also in the version on $\mathcal{H}_+$ we will need the following proposition which follows from Corollary 4.19.

Proposition 4.22
Let $f := T^n + a_1 T^{n-1} + \ldots + a_n$ be a hyperbolic polynomial with only non negative roots. If $a_{n-i} = 0$ for one i then $a_{n-j} = 0$ for all $j \leq i$.

Proof. First observe that if f has only positive roots then by Proposition 4.18(3) all its derivatives share this property. If $a_{n-i} = 0$ we know that the i-th derivative $f^{(i)}$ of f has a root at $t = 0$. But as $f^{(i-1)}$ has also only positive roots, also $f^{(i-1)}(0) = 0$. Now the statement follows since Corollary 4.19 (3) now implies that f has a multiple root of order i at $t = 0$. □

To study the polynomials on the boundary of $\mathcal{H}_+$ the following consequence of Proposition 4.20 will be helpful:

Proposition 4.23
Let $f \in \mathbb{R}[T]$ be a hyperbolic polynomial of degree n with $k < n$ distinct roots and assume that for $m < k$ the polynomial f has a root of order m at $T = 0$. Then for each $1 \leq s \leq k$ there is a polynomial g_s of degree $n - s$ with m-fold root at $T = 0$ and $\delta_s > 0$ such that for all $0 < \varepsilon < \delta_s$ the polynomials $f \pm \varepsilon g$ are also hyperbolic and have strictly more different zeros.

Proof. Just consider the hyperbolic polynomial $\tilde{f} := \frac{f}{T^m}$ of degree $n-m$ with $k-m$ distinct zeros. Applying 4.20 to $\tilde{f}$ we get $\tilde{g}_s$ of degree $n-m-s$ but then obviously $g_s := \tilde{g}_s T^m$ meets the announced statements. □

4.4 Proof of the main theorem

This last section uses the statements about univariate polynomials given in the previous section to prove the main statements. The proofs will be based on a elementary optimization problem. In order to introduce this problem we will first give some notation:

Recall that to each S_n orbit of any $x \in \mathbb{R}^n$ we associate the polynomial

$$f = \prod_{i=1}^{n}(T - x_i) = T^n + \sum_{i=1}^{n}(-1)^i a_i T^{n-i},$$

We will consider optimization problems over sets of the form

$$\mathcal{H}(a_1, \ldots, a_s) := \{z \in \mathbb{R}^n \,:\, z_1 = a_1, \ldots, z_s = a_s,\, T^n - z_1 T^{n-1} + \ldots \pm z_n \text{ is hyperbolic}\},$$

i.e. over the set of all monic hyperbolic polynomials of degree n that agree with f on the leading $s+1$ coefficients.

Now for the proof of the main theorem will take a look at linear optimization problems of the from:

$$\begin{aligned} &\min c^t z \\ &z \in \mathcal{H}(a_1, \ldots, a_s), \end{aligned}$$

where $c \in \mathbb{R}^n$ defines any linear function and $a_1, \ldots, a_s$ are fixed. To make the later argumentation easier, we set the minimum of any function over the empty set to be infinity.

A priori it may not be obvious that such problems have an optimal solution. But, this is a consequence of the following lemma:

Lemma 4.24
For any $s \geq 2$ every set $\mathcal{H}(a_1, \ldots, a_s)$ is compact.

Proof. As the empty set is compact we can assume that there is $z \in \mathcal{H}(a_1, a_2)$. Let $x_1, \ldots, x_n$ be the roots of $f_z := T^n - z_1 T^{n-1} + \ldots \pm z_n$. Then we have $e_1(x) = -a_1$ and $e_2(x) = a_2$. Hence we have $\sum_{i=1}^{n} x_i^2 = (e_1(x))^2 - 2e_2(x) = a_1^2 - 2a_2$. This shows that x is contained in a ball, thus $\mathcal{H}(a_1, a_2)$ is bounded, and hence so is $\mathcal{H}(a) \subseteq \mathcal{H}(a_1, a_2)$. Furthermore as by Proposition 4.18 (1) the roots of a polynomial depend continuously on the coefficients it is clear that $\mathcal{H}(a)$ is closed and therefore compact. □

We will use $\mathcal{H}^k(a_1,\ldots,a_s)$ to refer to the points in $\mathcal{H}(a_1,\ldots,a_s)\cap\mathcal{H}^k$, i.e. to those monic hyperbolic polynomials which have at most k distinct zeros and prescribed coefficients $a_1,\ldots,a_s$.

The crucial observations which will be the core of the theorems we want to prove lies in the geometry of the optimal points of the above optimization problems. This is noted in the following lemma:

Lemma 4.25
Let $n>2$, $s\in\{2,\ldots,n\}$, $c\in\mathbb{R}^n$ with $c_j\neq 0$ for at least one $j\in\{s+1,\ldots,n\}$ and $a\in\mathbb{R}^s$ such that $\mathcal{H}(a)\neq\emptyset$. We consider the optimization problem

$$\min_{z\in H(a)} c^t z.$$

Let M denote the set of minimizers of this problem. Then we have $\emptyset\neq M\subseteq\mathcal{H}^s(a)$.

Proof. Since by the above lemma $\mathcal{H}(a)$ is compact, there is at least one minimizer z, showing the nonemptyness of M. So if $M\subseteq H^s(a)$ we are done.
Hence to prove the statement by contradiction we assume that $M\not\subseteq H^s(a)$. Take $z\in M$ such that the number k of roots of the monic polynomial

$$f_z := T^n - z_1T^{n-1}+\ldots\pm z_n$$

is maximal. By assumption $s<k\leq n$. If $k=n$ we chose $y\in\mathbb{R}^n$ such that $c^ty<0$. By Proposition 4.20 (a) we deduce that there is a $\delta_n>0$ such that for all $0<\varepsilon<\delta_n$ we find that the polynomial $f_z+\varepsilon(y_1T^{n-1}+\ldots\pm y_n)$ is still hyperbolic. Thus by the choice of y we have $z+\varepsilon y\in\mathcal{H}(a)$ but by construction we have $c^t(z-\varepsilon y)<c^tz$ for all $0<\varepsilon<\delta_n$ which clearly contradicts the optimality of z. If on the other hand we have $k<n$ then by Proposition 4.20 we find $y\in\{0\}^k\times\mathbb{R}^{n-k}$ and $\delta_k>0$ such that for

$$g := T^{n-k}-y_{k+1}T^{n-k-1}+\ldots\pm y_n$$

we have that $f\pm\varepsilon g$ is hyperbolic for all $0<\varepsilon<\delta_k$. Thus by the choice of y the point $z\pm\varepsilon y$ will be in $\mathcal{H}(a)$ for all $0<\varepsilon<\delta_k$. Without loss of generality we may assume that $c^ty\leq 0$. This in turn implies

$$c^t(z+\varepsilon y)\leq c^tz\leq z-\varepsilon y,$$

since z is supposed to be a minimizer we must have that also $(z+\varepsilon y)$ is a minimizer. However, by Proposition 4.20 $f-\varepsilon g$ has strictly more distinct components, which clearly contradicts our choice of z and we can conclude. □

From the above lemma we can conclude the following important corollary:

Corollary 4.26
Every set $\mathcal{H}(a_1,\ldots,a_s)\neq\emptyset$ with $s\geq 2$ contains a point $\tilde{z}$ with $\tilde{z}\in\mathcal{H}^s(a_1,\ldots,a_s)$.

Proof. If $n \in \{1, 2\}$ the statement is clear. So we can assume $n > 2$. Take $c \in \mathbb{R}^n$ with $c_i \neq 0$ for one $i > s$ Then the function $c^t z$ will not be constant over $\mathcal{H}(a_1, \ldots, a_s)$. But as $\mathcal{H}(a_1, \ldots, a_s)$ is compact we know the minimal value is attained and we can conclude with Lemma 4.25. □

To transfer the half degree principle to $\mathbb{R}^n_+$ we will also need to know what happens to the minima when we intersect a set $\mathcal{H}(a_1, \ldots, a_s)$ with $\mathbb{R}^n_+$. We denote this intersection with $\mathcal{H}^+(a_1, \ldots, a_s)$ and define

$$\mathcal{H}^{(s,+)}(a_1, \ldots, a_s) := \mathcal{H}^+(a_1, \ldots, a_s) \cap \mathcal{H}^s(a_1, \ldots, a_s) \cup \mathcal{H}(a_1, \ldots, a_s, 0, 0, \ldots, 0).$$

With these appropriate notations we have a same type of argument as in Lemma 4.25:

Lemma 4.27
Let $s \in \{2, \ldots, n\}$, $c \in \mathbb{R}^n$ with $c_j \neq 0$ for at least one $j \in \{s+1, \ldots, n\}$ and $a \in \mathbb{R}^s$ such that $\mathcal{H}^+(a) \neq \emptyset$. Consider the optimization problem

$$\min_{z \in H^+(a)} c^t z.$$

Let M denote the set of minimizers of this problem. Then we have $\emptyset \neq M \subseteq \mathcal{H}^{(s,+)}(a)$.

Proof. The argument works out almost the same way as in Lemma 4.25: Indeed if $z \in \mathcal{H}^+(a_1, \ldots, a_s)$ has strictly positive components small perturbations of these will not change the positivity and the same arguments can be used. So just the cases of $z \in \mathcal{H}^+(a_1, \ldots, a_s)$ with zero components need special consideration. So assume we have a $\tilde{z} \in \mathcal{H}(a_1, \ldots, a_s)$ with zero components such that

$$c^t \tilde{z} = \min_{z \in \mathcal{H}^+(a_1, \ldots, a_s)} c^t z.$$

But with Proposition 4.22 we see that there is $i \in \{1, \ldots, n\}$ such that $\tilde{z}_j = 0$ for all $j \geq i$. If $i \leq s + 1$ we have already that that $\tilde{z} \in \mathcal{H}^{(s,+)}(a_1, \ldots, a_s)$ But if $s + 1 < i$ we can see from Proposition 4.23 that there is $0 \neq \tilde{y} \in \{0\}^s \times \mathbb{R}^{i-s} \times \{0\}^{n-i}$ such that $\tilde{z}_1 \pm \varepsilon \tilde{y} \in \mathcal{H}(a_1, \ldots, a_s) \cap \mathbb{R}^N_+$ for small positive ε and argue as in the previous lemma. □

Now to we are able to deduce the proof of Theorem 4.17:

Proof of Theorem 4.17.

1. We know from Proposition 4.12 that

$$G = G_1(Z_1, \ldots, Z_{\lfloor \frac{d}{2} \rfloor}) + \sum_{i=\lfloor \frac{d}{2} \rfloor + 1}^{d} G_i(Z_1, \ldots Z_{d-i}) Z_i.$$

So G is constant on any set $\mathcal{H}(a_1, \ldots, a_d)$. As we have

$$\bigcup_{(a_1,\ldots,a_d)\in\mathbb{R}^d} \mathcal{H}(a_1, \ldots, a_d) = \mathcal{H},$$

the first statement in Theorem 4.17 follows now directly from Corollary 4.26.

2. We will have to see that

$$\min_{z\in\mathcal{H}\subset\mathbb{R}^n} G(z) = \min_{z\in\mathcal{H}^k} G(z).$$

Again we decompose the space in the form:

$$\bigcup_{(a_1,\ldots,a_k)\in\mathbb{R}^k} \mathcal{H}(a_1, \ldots, a_k) = \mathcal{H}$$

Therefore

$$\min_{z\in\mathcal{H}} G(z) = \min_{a_1,\ldots,a_k} \min_{z\in\mathcal{H}(a_1,\ldots,a_k)} G(z).$$

But for fixed $z_1 = a_1, \ldots, z_k = a_k$ the function $G(z)$ is just linear and now we can apply Lemma 4.25 and see that:

$$\min_{z\in\mathcal{H}(a_1,\ldots,a_k)} G(z) = \min_{z\in\mathcal{H}^k(a_1,\ldots,a_k)} G(z).$$

and we get the second statement in Theorem 4.17.

3. Again the function G is linear over the sets $\mathcal{H}^+(a_1, \ldots, a_k)$ and we can argue as above by using Lemma 4.27.

□

4.5 Discussion

To conclude this chapter we want to give short discussion on some related issues:

As was already mentioned in the introduction, Foregger stated a theorem concerning critical points of elementary symmetric functions. Here we will remark that Foregger's Theorem 4.8 can be deduced using the same ideas that were used to establish the main theorem. This new proof we give here seems necessary since the original proof given by Foregger in [For87] fails as we will explain in the following:

Using exactly the notation used in [For87], Foregger defines on page 383 the set

$$C_{\gamma^*} = \left\{ y \in \mathbb{R}^s : \sum_{i=1}^{s} y_i = \gamma^*, y_i \in [0,1] \right\} \subset \mathbb{R}^s.$$

Then he derives on p.384 for $s < n$, $c \in \mathbb{R}^{n-s}$ constant, and $y \in \mathbb{R}^s$, the first two lines in the following chain; the third line then is a consequence of noting that $E_0(y) = 1$, and $E_1(y) = \gamma^*$.

$$\begin{aligned} 0 &= \phi^*(y) \\ &= \sum_{k=0}^{n} E_k(y) \sum_{r=k}^{n} c_r E_{r-k}(c) - \sum_{r=2}^{n} c_r E_r(0,c) \\ &= \sum_{r=0}^{n} c_r E_r(c) + \gamma^* \sum_{r=1}^{n} c_r E_{r-1}(c) - \sum_{r=2}^{n} c_r E_r(0,c) + \sum_{k=2}^{n} E_k(y) \sum_{r=k}^{n} c_r E_{r-k}(c). \end{aligned}$$

Now Foregger claims that

$$\sum_{r=k}^{n} c_r E_{r-k}(c) = 0, \text{ for } k = 2, 3, \ldots, n. \tag{4.3}$$

But we remark that $y \in \mathbb{R}^s$, so the definition of the elementary symmetric functions requires $E_{s+1}(y) = \cdots = E_n(y) = 0$. This is a fact not taken into consideration in [For87]. At any rate, since the functions $1, E_2, E_3, \ldots, E_s$ are linearly independent on C^*_γ we may infer the equations (4.3) for $k = 2, \ldots, s$. The problem is that these equations are claimed by Foregger not only for $k = 2, \ldots, s$, but for $k = 2, \ldots, n$, and then used in the order $k = n, n-1, ..., 1$, to derive that $c_n, c_{n-2}, \ldots, c_1$, are 0. However, this reasoning is impossible once we take $E_{s+1}(y) = \cdots = E_n(y) = 0$ into account. But then the proof given by Foregger fails.

The following connection to Lemma 4.27 will now provide a valid proof.

Proof of Theorem 4.8. We assume that the function $\phi(x) := \sum_{i=1}^{n} c_i e_i(x)$ in Foregger's theorem is not constant, but $\underline{a} \in \text{int}(C_\gamma)$, is a local extremum distinct from the symmetric

point in C_γ, i.e., $\underline{a} \neq \frac{\gamma}{n} 1_n$. To deduce Foregger's statement we can now proceed as in Lemma 4.27:

Indeed, consider the $\alpha := (e_1(\underline{a}), \ldots, e_n(\underline{a})) \in \mathcal{H}(\gamma) \cap \pi([0,1]^n)$. As then with the same type of arguments as in the proof of Lemma 4.27 we can either find $\beta_1, \beta_2 \in \mathcal{H}(\gamma)$ such that $c^t\beta_1 < c^t\alpha < c^t\beta_2$ or we find β_3 in the interior of $\mathcal{H}(\gamma)$ with $c^t\beta_3 = c^t\alpha$. As $\underline{a}$ is in the relative interior of C_γ we could chose $\beta_1, \beta_2, \beta_3 \in \mathcal{H}(\gamma) \cap \pi((0,1)^n)$. Hence both cases contradict the fact the α is an extremum for the linear function $c^t x$ on $\pi(C_\gamma)$ respectively that $\underline{a}$ is an extremum of ϕ on C_γ. □

As it was was remarked in the beginning, the statements given here generalize directly to even symmetric polynomials. To see this just observe that the fundamental invariants in this case are $p_2, \ldots, p_{2n}$ (see [Hum92] Example 3.12). So every even symmetric polynomial $F \in \mathbb{R}[X]$ of degree $2d$ has a unique representation in the form $F(X) = G(p_2, \ldots, p_{2n})$.

Now if we substitute variables such that $u_i = x_i^2$ we arrive at a symmetric polynomial $\tilde{F}(u_1, \ldots u_n) = G(p_1, \ldots, p_n)$. By variable substitution we have $F(\mathbb{R}^n) = \tilde{F}(\mathbb{R}^n_+)$. Thus we can apply Theorem 4.17 in order to deduce the analogous statement in Theorem 4.7 for even symmetric polynomials.

Finally we also mention the following equivalent formulation of Corollary 4.26 in terms of univariate polynomials:

Proposition 4.28
Let $f \in \mathbb{R}[T]$ be a univariate polynomial of degree n which factors

$$f = \prod_{i=1}^{n} (T - x_i), \text{ with } x_i \in \mathbb{R},$$

then for every $d \in \{1, \ldots, n\}$ there is $\tilde{f}_d \in \mathbb{R}[T]$, with $\deg(f - \tilde{f}_d) < n - d$ and $\tilde{f}_d$ has only d distinct roots all of which are real.

5

Optimizing with symmetric polynomials

> The universe is built on a plan the profound symmetry of which is somehow present in the inner structure of our intellect.
>
> Paul Valery

AMONGST the discrete groups the symmetric group $\mathcal{S}_n$ has - also due to its rich combinatorics - a prominent position. Therefore this chapter aims to work out all the possibilities to exploit symmetries in detail using the example to the symmetric group $\mathcal{S}_n$. While the representation theory of the symmetric group is a classical topic (as reviewed in Chapter 2.2), it yields some interesting (even somewhat surprising) results in our setting.

First, in Section 5.1 we discuss the block diagonalization for the symmetric group. By realizing the irreducible components in a suitable basis of polynomials (generalized Specht polynomials as defined below), the moment matrix can be characterized rather explicitly (Theorem 5.6).

As corollaries, we derive some concrete representation theorems for symmetric polynomials in Section 5.2.

In Section 5.3 we show how to reduce an SDP-relaxation to a family of lower-dimensional relaxations with the help of the degree principle provided in chapter 4. In the special case of symmetric polynomials of degree 4 this reduces the non-negativity problem to an SOS problem (and thus to a semidefinite feasibility problem), see Theorem 5.17.

Finally we will provide SDP-based upper and lower bounds for a special class of symmetric optimization problems.

5.1 Moment matrices for the symmetric group

Recall from the preliminaries presented in chapter 2 that the irreducible representations of $\mathcal{S}_n$ are in natural bijection with the partitions of n. In order to construct a suitable generalized moment matrix we will need a graded decomposition of the vector space $\mathbb{R}[X]$ into $\mathcal{S}_n$-irreducible components. A classical construction of Specht gives a realization of the Specht modules as polynomials (see [Spe37]):

For $\lambda \vdash n$ let t_λ be a λ-tableau and $\mathcal{C}_1, \ldots, \mathcal{C}_\nu$ be the columns of t_λ. To t_λ we associate the monomial $X^{t_\lambda} := \prod_{i=1}^{n} X_i^{l(i)-1}$, where $l(i)$ is the index of the row of t_λ containing i. Note that for any λ-tabloid $\{t_\lambda\}$ the monomial X^{t_λ} is well defined, and the mapping $\{t_\lambda\} \mapsto X^{t_\lambda}$ is an $\mathcal{S}_n$-isomorphism. For any column $\mathcal{C}_i$ of t_λ we denote by $\mathcal{C}_i(j)$ the element in the j-th row and we associate a Vandermonde determinant:

$$\mathrm{Van}_{\mathcal{C}_i} := \det \begin{pmatrix} X^0_{\mathcal{C}_j(1)} & \cdots & X^0_{\mathcal{C}_j(k)} \\ \vdots & \ddots & \vdots \\ X^{k-1}_{\mathcal{C}_j(1)} & \cdots & X^{k-1}_{\mathcal{C}_j(k)} \end{pmatrix} = \prod_{i<l} (X_{\mathcal{C}_j(l)} - X_{\mathcal{C}_j(i)}).$$

The *Specht polynomial* s_{t_λ} associated to t_λ is defined as

$$s_{t_\lambda} := \prod_{j=1}^{\nu} \mathrm{Van}_{\mathcal{C}_j} = \sum_{\sigma \in \mathrm{CStab}_{t_\lambda}} \mathrm{sgn}(\sigma)\sigma(X^{t_\lambda}),$$

where $\mathrm{CStab}_{t_\lambda}$ is the column stabilizer of t_λ.

By the $\mathcal{S}_n$-isomorphism $\{t_\lambda\} \mapsto X^{t_\lambda}$, $\mathcal{S}_n$ operates on s_{t_λ} in the same way as on the polytabloid e_{t_λ}. If $t_{\lambda,1}, \ldots, t_{\lambda,k}$ denote all standard Young tableaux associated to λ, then the set of polynomials $s_{t_{\lambda,1}}, \ldots, s_{t_{\lambda,k}}$ are called the *Specht polynomials* associated to λ. The observation implies (see [Spe37]):

Proposition 5.1
The Specht polynomials $s_{t_{\lambda,1}}, \ldots, s_{t_{\lambda,k}}$ span an $\mathcal{S}_n$-submodule of $\mathbb{R}[X]$ which is isomorphic to the Specht module S^λ.

While these polynomials already give a realization of the Specht modules in terms of polynomials, for the construction of the symmetry-adapted moment matrix we need to generalize this construction to realize these modules in terms of polynomials with prescribed exponent vectors. In the following, let $n \in \mathbb{N}$ and $\beta := (\beta_1, \ldots, \beta_n)$ be an n-tuple of non-negative integers, and let $\mathbb{R}\{X^\beta\}$ be the linear span of all monomials $X^{\tilde{\beta}}$ such that $\tilde{\beta}$ and β are permutations of one another. By construction each $\mathbb{R}\{X^\beta\}$ is closed under the action of $\mathcal{S}_n$ and therefore has the structure of an $\mathcal{S}_n$-module.

Denote by $\mathrm{wt}(\beta) = \sum_{i=1}^{n} \beta_i$ the *weight* of β. Let $b_1, \ldots, b_m$ be the distinct components of β (called the *parts* of β), ordered (decreasingly) according to the multiplicity of the

occurrence in β. Further let $I_k = \{j : \beta_j = I_k\}$, $1 \leq k \leq m$; note that the sets $I_1, \ldots, I_m$ define a partition of $\{1, \ldots, n\}$. Setting $\mu_k := |I_k|$, the vector $\mu = (\mu_1, \ldots, \mu_m)$ consists of monotonously decreasing components and thus defines a partition of n. We call $\mu \vdash n$ the *shape* of β. The stabilizer of the monomial X^β is isomorphic to $\mathcal{S}_{\mu_1} \times \ldots \times \mathcal{S}_{\mu_m}$.

Proposition 5.2
For $\beta \in \mathbb{N}_0^n$, the $\mathcal{S}_n$-module $\mathbb{R}\left\{X^\beta\right\}$ is isomorphic to the permutation module M^μ, where μ is the shape of β.

Proof. Recall from Definition 2.21 that M^μ is spanned by the set of all μ-tabloids. For every monomial $X^{\tilde{\beta}}$ and its associated set partition $I_1, \ldots, I_m$ we construct a μ-tableau by placing the indices that correspond to I_k into the k-th row. As the order of the indices in each I_k is arbitrary we get in fact an identification of $X^{\tilde{\beta}}$ with the row equivalence class of the constructed μ-tableau. So each $X^{\tilde{\beta}}$ corresponds uniquely to a μ-tabloid. Since this identification commutes with the action of $\mathcal{S}_n$, we obtain an $\mathcal{S}_n$-isomorphism. □

Now let $\lambda \vdash n$ be another partition of n. In order to construct the realizations of the Specht module S^μ as submodule of $\mathbb{R}\left\{X^\beta\right\}$, we look at pairs (t_λ, T), where t_λ is a fixed λ-tableau and T is a generalized Young tableau with shape λ and content μ. For each pair we construct a monomial $X^{(t_\lambda, T)} \in \mathbb{R}\left\{X^\beta\right\}$ from its parts $b_1, \ldots, b_m$ in the following way:

Let $t_\lambda(i,j)$ and $T(i,j)$ denote the element in the i-th row and j-th column of t_λ and T. Then define

$$X^{(t_\lambda, T)} := \prod_{(i,j)} X_{t_\lambda(i,j)}^{b_{T(i,j)}}.$$

Let $\mathcal{C}_1, \ldots, \mathcal{C}_\nu$ be the columns of t_λ, then we associate to each column $\mathcal{C}_i$ a polynomial

$$\mathrm{Van}_{\mathcal{C}_i, T} := \det \begin{pmatrix} X_{\mathcal{C}_i(1)}^{b_{T(1,i)}} & \ldots & X_{\mathcal{C}_i(k)}^{b_{T(1,i)}} \\ \vdots & \ldots & \vdots \\ X_{\mathcal{C}_i(1)}^{b_{T(k,i)}} & \ldots & X_{\mathcal{C}_i(k)}^{b_{T(k,i)}} \end{pmatrix}.$$

As in Specht's construction we form the product polynomial

$$s_{(t_\lambda, T)} = \prod_{i=1}^{\nu} \mathrm{Van}_{\mathcal{C}_i, T}$$

and set (by summation over the row equivalence class of T)

$$S_{(t_\lambda, T)} := \sum_{S \in \{T\}} s_{(t_\lambda, T)}.$$

Lemma 5.3
Let T be a generalized Young tableau with shape λ and content μ. The generalized Specht polynomial $S_{(t_\lambda,T)}$ generates a cyclic $\mathcal{S}_n$ submodule $\mathbb{R}\left\{S_{(t_\lambda,T)}\right\}$ of $\mathbb{R}\left\{X^\beta\right\}$ which is isomorphic to the Specht module S^λ.

Proof. By Proposition 5.2 we can follow Young's decomposition of M^μ (Theorem 2.29). Therefore we associate to every T with shape λ and content μ an $\mathcal{S}_n$-homomorphism from M^λ to M^μ defined by

$$\Theta_{T,t_\lambda} : \{t_\lambda\} \mapsto \sum_{S\in\{T\}} X^{(t_\lambda,S)}$$

and the cyclic structure of M^λ. If $\bar{\Theta}_{T,t_\lambda}$ denotes the restriction of this homomorphism to the Specht module S^λ we get an element of $\mathrm{Hom}(S^\lambda, M^\mu)$. Let $\mathrm{CStab}_{(t_\lambda)}$ be the column stabilizer associated to the Young tableau t_λ. Then the restriction amounts to say that

$$\bar{\Theta}_{T,t_\lambda}(e_{t_\lambda}) = \bar{\Theta}_{T,t_\lambda}(\sum_{\sigma\in\mathrm{CStab}} \mathrm{sgn}(\sigma)\sigma\{t_\lambda\}) = \sum_{\sigma\in\mathrm{CStab}} \Theta_{T,t_\lambda}(\mathrm{sgn}(\sigma)\sigma\{t_\lambda\}).$$

As we have $s_{(t_\lambda,T)} = \sum_{\sigma\in\mathrm{CStab}_{(t_\lambda)}} \mathrm{sgn}(\sigma)\sigma(X^{(t_\lambda,T)})$ is follows that $S_{(t_\lambda,T)}$ is the image of e_{t_λ} under $\bar{\Theta}_{T,t_\lambda}$. □

Remark 5.4
Note the following connection of the generalized Specht polynomials to the classical Schur polynomials. For a non-negative vector $\lambda = (\lambda_1, \ldots, \lambda_l)$ the generalized Vandermonde determinant

$$a_\lambda \;:=\; \det\left((X_i^{\lambda_j})_{1\le i,j\le l}\right) \tag{5.1}$$

(as a polynomial in $X_1, \ldots, X_l$) is called the *alternant* of λ. Moreover, for a partition λ of length l the *Schur function* s_λ is defined by

$$s_\lambda \;=\; \frac{a_{\lambda+\delta}}{a_\delta},$$

where $\delta := (l-1, l-2, \ldots, 1, 0) \in \mathbb{Z}^l$. It is well known that s_λ is a symmetric polynomial in $X_1, \ldots, X_l$ (also called a *Schur polynomial*). Hence, the alternant (5.1) can be written as

$$a_\lambda \;=\; s_{\lambda-\delta} \cdot a_\delta\,. \tag{5.2}$$

Now the polynomials $\mathrm{Van}_{\mathcal{C}_i,T}$ defined above can be seen as the alternant associated to the numbers $(b_{T(1,i)}, \ldots, b_{T(k,i)})$ and thus by (5.2) as the product of a Schur polynomial with a classical Vandermonde determinant.

Let $\mathcal{T}^0_{\lambda,\mu}$ denote the set of semi standard generalized Young tableaux of shape λ and content μ (see Definition 2.28). To conclude we can summarize the above considerations.

Theorem 5.5
For β of weight d we have

$$\mathbb{R}\left\{X^\beta\right\} = \bigoplus_{\lambda \trianglerighteq \mu} \bigoplus_{T \in \mathcal{T}^0_{\lambda,\mu}} \mathbb{R}\left\{S_{(t_\lambda, T)}\right\}.$$

The multiplicity of the Specht modules S^λ in this $\mathcal{S}_n$-module is equal to the Kostka number $K_{\lambda\mu}$, where $\lambda \vdash n$ is the shape of β (which will be denoted $\mu(\beta)$ in the sequel).

Proof. By Lemma 5.3 each Specht polynomial gives rise to an irreducible component. As from Proposition 5.2 we deduce that $\mathbb{R}\left\{X^\beta\right\}$ is isomorphic to M^λ we can apply Young's rule (Theorem 2.29) in order to identify the number of distinct irreducible components with the Kostka numbers. □

Based on these results, we can construct a symmetry-adapted moment matrix of order k. By (3.3) the blocks are labeled by partitions of n. In order to construct the block for a fixed λ we have to take into account the various $\beta = (\beta_1, \ldots, \beta_n)$ with $wt(\beta) = k$ and shape λ. For a given d, let $c(\lambda, d)$ be the number of $\beta \in \mathbb{N}_0^n$ with $\mathrm{wt}(\beta) = d$ which have shape λ. The decomposition from Theorem 5.5 translates into the moment setting as follows.

Corollary 5.6
For $k \in \mathbb{N}$, the k-th symmetry-adapted moment matrix $M_k^s(y)$ is of the form

$$M_k^s(y) \;=\; \bigoplus_{\lambda \vdash n} M_{k,\lambda}^s(y).$$

With $\kappa_\lambda := \sum_{d=0}^k c(\beta, d) K_{\lambda\mu(\beta)}$ the size of $M_{k,\lambda}^s(y)$ is equal to $\kappa_\lambda \times \kappa_\lambda$.

Proof. The distinct irreducible representations are indexed by partitions of n. Therefore by Remark 3.5 the size κ_λ of the block of $M_k^s(y)$ corresponding to the irreducible component S^λ equals the number of submodules of $\mathbb{R}[X]_{\leq k}$ isomorphic to S^λ. As we have

$$\mathbb{R}[X]_{\leq k} = \bigoplus_{d=0}^{k} \bigoplus_{\beta \in \mathbb{N}_0^n,\, \mathrm{wt}(\beta) = k} \mathbb{R}\left\{X^\beta\right\},$$

Theorem 5.5 implies $\kappa_\lambda = \sum_{d=0}^k c(\beta, d) K_{\lambda\mu(\beta)}$. □

The following remarkable consequence can be seen as a *degree principle for Lasserre's relaxation.*

Theorem 5.7
For all $n \geq 2k$ the symmetry-adapted moment matrix of order k has the same structure,

i.e., the same number and sizes of blocks and variables. In particular, up to the computation of the block decomposition the complexity of the question if a symmetric polynomial of degree $2k$ in n variables is a sum of squares is only depending on k.

Proof. First observe that by Remark 3.5 the number of variables equals the dimension of the $\mathbb{R}$ vector space of symmetric polynomials of degree at most $2k$. Therefore it corresponds to the number of n-partitions of $2k$, which is just the number of partitions of $2k$ for all $n \geq 2k$. So we see that the number of variables does not increase in n once $n \geq 2k$.

Now set $n_0 = 2k$ and let l be the number of partitions of k, $\beta^{(1)}, \ldots, \beta^{(l)} \in \mathbb{N}_0^{n_0}$ the distinct exponent vectors modulo permutation with $\mathrm{wt}(b^{(i)}) = k$, $1 \leq k \leq l$, and $\lambda^{(i)} \vdash n_0$ be the shape of $\beta^{(i)}$. The rest of the proposition follows if we can show that for every $n \geq n_0$ there exist partitions $\tilde{\lambda}^{(1)}, \ldots, \tilde{\lambda}^{(m)}$ of n such that $\kappa_{\tilde{\lambda}^{(i)}} = \kappa_{\lambda^{(i)}}$ for all $1 \leq i \leq m$ and $\kappa_{\tilde{\lambda}} = 0$ for all other $\tilde{\lambda} \vdash n$.

First note that the $\tilde{\beta}^{(i)}$ which are exponent vectors come from the $\beta^{(i)}$ by adding $n - n_0$ zeros. As $n \geq n_0 \geq 2k$ this implies that the possible $\tilde{\lambda}^{(i)}$ are of the form $\tilde{\lambda}^{(i)} := (\lambda_1^{(i)} + n - n_0, \lambda_2^{(i)}, \ldots, \lambda_t^{(i)})$. Since $K_{\lambda\mu} = 0$ whenever $\mu \not\trianglerighteq \lambda$ we conclude that the possible $\tilde{\mu}$ we have to consider are of the form $\tilde{\mu} := (\mu_1 + n - n_0, \mu_2, \ldots, \mu_t)$ for one $\mu \geq \lambda^{(i)}$. But in this setting we have $K_{\lambda\mu} = K_{\tilde{\lambda}\tilde{\mu}}$ and the statement follows. □

Example 5.8
We illustrate the techniques for a small example with $n = 3$ and $k = 2$. The moment variables are indexed by partitions of the numbers $1, 2, 3, 4$ with three parts, i.e., $y_1, y_2, y_3, y_4, y_{11}, y_{22}, y_{21}, y_{111}, y_{211}$. The irreducible components are indexed by the partitions $\lambda \vdash (3)$, thus $\lambda \in \{(3), (2,1), (1,1,1)\}$. The β we have to take into account are $(0,0,0), (1,0,0), (2,0,0), (1,1,0)$ with shape $\mu^{(1)} = (3), \mu^{(2)} = (2,1), \mu^{(3)} = (2,1), \mu^{(4)} = (2,1)$. The semi-standard generalized Young tableaux with shape μ and content $\lambda \in \{\lambda^{(1)}, \ldots, \lambda^{(4)}\}$ from Lemma 5.3 are:

- For $\mu = (3)$: $\begin{array}{|c|c|c|}\hline 1&1&1\\\hline\end{array}$, $\begin{array}{|c|c|c|}\hline 1&1&2\\\hline\end{array}$.
- For $\mu = (2,1)$: $\begin{array}{|c|c|}\hline 1&1\\\hline 2\\\cline{1-1}\end{array}$.
- For $\mu = (1,1,1)$: There is no generalized semi-standard Young tableau corresponding to the above $\lambda^{(i)}$.

For $\mu = (3)$, corollary 5.6 yields a 4×4-block, with basis polynomials

$$\left\{1, X_1 + X_2 + X_3, X_1^2 + X_2^2 + X_3^2, X_1X_2 + X_1X_3 + X_2X_3\right\}.$$

Thus

$$M_{(3)} := \begin{pmatrix} 1 & 3\,y_1 & 3\,y_2 & 3\,y_{11} \\ 3\,y_1 & 3\,y_2 + 6\,y_{11} & 3\,y_3 + 6\,y_{21} & 6\,y_{21} + 3\,y_{111} \\ 3\,y_2 & 3\,y_3 + 6\,y_{21} & 3\,y_4 + 6\,y_{22} & 6\,y_{31} + 3\,y_{211} \\ 3\,y_{11} & 6\,y_{21} + 3\,y_{111} & 6\,y_{31} + 3\,y_{211} & 3\,y_{22} + 6\,y_{211} \end{pmatrix} .$$

For $\mu = (2,1)$ we obtain a 3×3-block, with basis polynomials

$$\left\{2X_3 - X_2 - X_1, 2X_3^2 - X_2^2 - X_1^2, -2X_1X_2 + X_2X_3 + X_3X_1\right\} .$$

Thus

$$M_{(2,1)} = \begin{pmatrix} 6\,y_2 - 6\,y_{11} & 6\,y_3 - 6\,y_{21} & 6\,y_{21} - 6\,y_{111} \\ 6\,y_3 - 6\,y_{21} & 6\,y_4 - 6\,y_{22} & -6\,y_{211} + 6\,y_{31} \\ 6\,y_{21} - 6\,y_{111} & -6\,y_{211} + 6\,y_{31} & 6\,y_{22} - 6\,y_{211} \end{pmatrix} .$$

Remark 5.9
We remark that the techniques presented above also provide the tools for some explicitly stated open issues in in the study of unconstrained optimization of symmetric polynomials in Gatermann and Parrilo [GP04] (p. 124) who – mentioning the lack of explicit formulas for the isotypic components – refer to the study of examples and asymptotics.

5.2 Sums of squares-representations for symmetric polynomials

From the dual point of view, the results presented in Section 5.1 imply the following sums of squares decomposition theorem: In the following we let S be a set of monomials and denote $\mathbb{R}\{S\}$ the $\mathbb{R}$–vector space generated by the elements of S. Then $\Sigma(\mathbb{R}\{S\})^2$ will be the shorthand notation for all polynomials that are sums of squares in the elements of $\mathbb{R}\{S\}$.

Theorem 5.10
Let $p \in \mathbb{R}[X_1, \ldots, X_n]$ be symmetric and homogeneous of degree $2d$. If p is a sum of squares then p can be written in the form

$$p \;=\; \sum_{\beta \vdash d} \sum_{\lambda \vdash n} \sum_{T \in \mathcal{T}^0_{\lambda,\mu(\beta)}} \Sigma(\mathbb{R}\left\{S_{(t_\lambda, T)}\right\})^2 ,$$

where β runs over the non-negative partitions of d with n parts.

Proof. The statement follows from dualizing Theorem 5.5. □

Especially for the cases when the notion of non-negativity coincides with the sums of squares decomposition this yields the following corollaries:

Corollary 5.11
Let $p \in \mathbb{R}[X_1, X_2]$ be a symmetric homogeneous form of degree $2d$. If p is non-negative then p can be written in the form

$$p \;=\; \sum_{\alpha_1,\alpha_2\in\mathbb{N}_0,\alpha_1+\alpha_2=d} \Sigma(\mathbb{R}\,\{X_1^{\alpha_1}X_2^{\alpha_2} + X_1^{\alpha_2}X_2^{\alpha_1}\})^2 + \Sigma(\mathbb{R}\,\{X_1^{\alpha_1}X_2^{\alpha_2} - X_1^{\alpha_2}X_2^{\alpha_1}\})^2\,.$$

Corollary 5.12
Let $p \in \mathbb{R}[X_1, \ldots, X_n]$ be symmetric and homogeneous quadratic form. If p is non-negative then p can be written in the form

$$p \;=\; \alpha(X_1 + \cdots + X_n)^2 + \beta\sum_{i<j}(X_j - X_i)^2 = (\alpha + (n-1)\beta)\sum X_i^2 + 2(a-b)\sum_{i\neq j} X_iX_j\,.$$

with some coefficients $\alpha, \beta \geq 0$.

Corollary 5.13
Let $p \in \mathbb{R}[X_1, X_2, X_3]$ be a symmetric and homogeneous of degree 4. If p is non-negative then p can be written in the form

$$p \;=\; (\alpha + 2\delta)M_4 + (2\alpha + 2\varepsilon + \gamma - \delta)M_{22} + (\beta - \omega)M_{31} + (\beta + 2\gamma + 2\omega - 2\varepsilon)M_{211},$$

where

$$M_4 := \sum(X_i^4), M_{22} := \sum_{i\neq j} X_i^2X_j^2, M_{31} := \sum_{i\neq j} X_i^3X_j, \text{ and } M_{211} := \sum_{i\neq j\neq k} X_i^2X_jX_k,$$

such that $\alpha, \gamma, \delta, \varepsilon \geq 0$ and $\alpha\gamma \geq \beta^2$ and $\delta\varepsilon \geq \omega^2$.

5.3 Using the degree principle

As a further way to exploit symmetries in SDP -based relaxations we want to show how to construct a family of low dimensional problems of lower-dimensional relaxations by applying the degree principle (Theorem 4.2). The idea behind this aproach is that the set A_k can be represented as a finite union of k-dimensional linear subspaces. By restricting the initial problem to each of this subspaces individually we arrive at a family of k dimensional polynomial optimization problems.

For $n, k \in \mathbb{N}$ a vector $\omega := (\omega_1 \ldots, \omega_k)$ of positive, non-increasing integers with $n = \omega_1 + \ldots + \omega_k$ is called a *k-partition* of n. Let Ω denote all possible k-partitions of n. Then for each $\omega = (\omega_1 \ldots, \omega_k)$, let

$$f^\omega := f(\underbrace{t_1, \ldots, t_1}_{\omega_1}, \underbrace{t_2, \ldots, t_2}_{\omega_2}, \ldots, \underbrace{t_k, \ldots, t_k}_{\omega_k}) \in \mathbb{R}[t_1, \ldots, t_k]\,.$$

Similarly, let $K^\omega := \big\{(t_1, \ldots, t_k) \in \mathbb{R}^k : {g_1}^\omega(t) \geq 0, \ldots, {g_k}^\omega(t) \geq 0\big\}$. With these notations at hand we can use Theorem 4.2 in order to transform the original optimization problem in n variables into a set of new optimization problems that involve only k variables,

$$\inf_{x \in K} f(x) \;=\; \inf_{\omega \in \Omega} \min_{x \in K^\omega} f^\omega(x)\,. \tag{5.3}$$

Now one can apply the usual relaxation scheme to every of the above k-dimensional problems separately. For each $\omega \in \Omega$ let Q_l^ω be the l-th relaxation (1.15) of $\min_{x \in K^\omega} f_\omega$. Putting these ideas together we obtain:

Theorem 5.14
Let $f, g_1, \ldots, g_m \in \mathbb{R}[X]$ symmetric such that $K := \{x \in \mathbb{R}^n : g_1(x) \geq 0, \ldots, g_m(x) \geq 0\}$ meets Putinar's condition. Let d be the degree of f and set

$$k := \max\left\{\lfloor \frac{d}{2} \rfloor, \deg g_1, \ldots, \deg g_m\right\}.$$

Then the sequence $\inf_\omega Q_k^\omega$ converges to $\inf_{x \in K} f$ for $l \to \infty$.

Proof. By Theorem 4.2 there is a k-partition $\omega \in \Omega$ of n with $\min_{x \in K} f = \min_{x \in K_\omega} f^\omega$. It suffices to show that K^ω also meets Putinar's condition. Since K meets Putinar's condition, there is $u \in \mathbb{R}[X]$ with $u = u_0 + \sum_{j=1}^m u_j g_j$ for some sums of squares polynomials $u_0, \ldots, u_m$ such that the level set of u is compact. This representation carries over to u^ω which also has a compact level set. □

Remark 5.15
At first sight it might not look profitable to replace one initial problem by a family of new problems. However note that for fixed $k \in \mathbb{N}$ the number of k-partitions of any n is bounded by $(n+k)^k$. On the other hand a polynomial optimization problem in n variables yields a moment matrix of size $O(n^{2l})$ in the $l-$th relaxation step of Lasserre's scheme. In view of the polynomial bound (for fixed k) on the number of k-partitions it is therefore profitable to use the degree-principle based relaxation.

The process of building the k-dimensional problems can be related to breaking the symmetries as the resulting problems will in general no longer be invariant to a symmetric group $\mathcal{S}_k$. However as dimensions drop there are situations (in particular for $m = k$) where we will get finite convergence.

Theorem 5.16
Let $f, g_1, \ldots, g_k \in \mathbb{R}[X]$ be symmetric such that the polynomials g_i are of degree at most k, and f is of degree at most $2k$. Further assume that the variety $V(g_1, \ldots, g_k) \subset \mathbb{C}^n$ has codimension k. Then the relaxation sequence $\inf_\omega Q_l^\omega$ will converge to $\inf_{x \in V(g_1,\ldots,g_k)}$ after finitely many steps.

Proof. By Theorem 4.2 the problems that give rise to the sequence of relaxation schemes are k-dimensional. The main observation is that under the circumstances described above each of the resulting varieties $V^\omega := V({g_1}^\omega, \ldots, {g_k}^\omega)$ is zero dimensional and then Laurent's Theorem (1.32) can be applied to deduce the announced statement. To see that these varieties contain only finitely many points we proceed as follows:

It was shown in Corollary 4.11 that every symmetric polynomial g of degree k in n variables can be uniquely written as a polynomial in the first k power sum polynomials $p_1(X), \ldots, p_k(X)$, where $p_i(X) = \sum_{j=1}^n X_j^i$.

Let $\gamma_1 \ldots, \gamma_k \in \mathbb{R}[Z_1 \ldots, Z_k]$ be polynomials such that

$$\gamma_i(p_1(X), \ldots, p_n(X)) = g_i(X).$$

The fact that the polynomials $p_1, \ldots, p_n$ are algebraically independent establishes that $\mathbb{C}^n/\mathcal{S}_n$ is in fact isomorphic to $\mathbb{C}^n$.

As the variety

$$V(g_1, \ldots, g_k)$$

is $\mathcal{S}_n$ invariant, its image in the quotient $\mathbb{C}^n/\mathcal{S}_n$ is given by

$$\tilde{V} := \{z \in \mathbb{C}^n \,:\, \gamma_i(z) = 0 \text{ for all } 1 \leq i \leq k\}.$$

Now as $\mathcal{S}_n$ is a finite group the codimension of $\tilde{V}$ is also k. But this implies that

$$\tilde{V} \cap \{z \in \mathbb{C}^n \,:\, z_{k+1} = \ldots = z_n = 0\}$$

is zero dimensional. Therefore, there are just finitely many $z := (z_1, \ldots, z_k)$ for which $\gamma_i(z) = 0$ holds for all k with $1 \leq i \leq k$.

Now let $\omega = (\omega_1, \ldots, \omega_k)$ be any k-partition of n and consider

$$V^\omega := V({g_1}^\omega, \ldots, {g_k}^\omega) \subset \mathbb{C}^k.$$

Let $\tilde{p}_i := \sum_{j=1}^k \omega_j t_j^k$, then we get ${g_i}^\omega(t) = \gamma_i(\tilde{p}_1(t), \ldots, \tilde{p}_k(t))$. So at the points in $y \in V^\omega$ we have

$$\tilde{p}_1(y) = z_1, ..., \tilde{p}_k(y) = z_k$$

for one of the finitely many $z = (z_1, .., z_k)$, with $\gamma_i(z) = 0$ for all $1 \leq i \leq k$. And thus there are just finitely many points in V^ω. □

Closely related to the question of finite convergence is the description of polynomials that are positive but not sums of squares. By Hilbert's Theorem 1.13, every nonnegative ternary quartic polynomial is a sum of squares. For quartics in more than three variables this is not true in general, not even for symmetric polynomials (see Example 5.18 below). For symmetric polynomials of degree 4, deciding the non-negativity can be reduced to an SOS problem and thus to a semidefinite optimization problem.

Theorem 5.17
Let $f \in \mathbb{R}[X]$ be a symmetric polynomial of degree 4. Then f is non-negative if and only if for all $\omega \in \Omega$ the polynomials f^ω are SOS.

Proof. As f is of degree 4, all the f^ω are polynomials of degree 4 in two variables. Hence, by Hilbert's theorem every f^ω is non-negative if and only if it is a sum of squares. □

Example 5.18
Choi and Lam [CL78] have shown that the homogenous polynomial of degree 4

$$f \;=\; \sum X_i^2 X_j^2 + \sum X_i^2 X_j X_k - 4X_1X_2X_3X_4$$

in four variables is non-negative, but not a sum of squares. By Theorem 5.17, the non-negativity of f is equivalent to the property that the following two homogeneous polynomials in two variables are sum of squares.

$$\begin{aligned} f_1 &= X_2^4 + 4\,X_2^2X_4^2 + X_4^4 + 2\,X_4^3X_2\,, \\ f_2 &= 4\,X_2^4 + 6\,X_2^2X_4^2 - 2\,X_2^3X_4\,. \end{aligned}$$

However, the SOS property of the polynomials easily follow from their non-negativity of their de-homogenized versions (which are univariate polynomials) and Hilbert's Theorem.

5.4 Lower and upper bounds for power sum problems

For constrained polynomial optimization problems described by power sums, the orbit space approach defined in Chapter 3 can become particularly simple. The following class of optimization problems generalizes a class studied by Brandenberg and Theobald ([BT06])

Definition 5.19
Let $n, m, q \in \mathbb{N}$ with $q \geq m$, $m \leq n+1$, and given some vector $\gamma \in \mathbb{R}^{m-1}$, consider the symmetric global optimization problem

$$\mathrm{P}_{nmq}: \quad \min \sum_{i=1}^{n} X_i^q \qquad \text{s.t.} \quad \sum_{i=1}^{n} X_i^j \;=\; \gamma_k\,, \quad j = 1, \ldots, m-1, \tag{5.4}$$

with optimal value denoted $\min \mathrm{P}_{nmq}$.

In this section, we are going to provide upper and lower bounds for P_{nmq}.

Choose the fundamental invariants $\pi_j = \frac{1}{n} p_j$ $(1 \leq j \leq n)$ where $p_j := \sum_{i=1}^{n} X_i^j$ denotes the power sum of order j.

Then the matrix $M(z)$ in Theorem 3.11 specializes to the Sylvester matrix (see Definition 4.14).

We can exploit the double occurrence of power sums: within the optimization problem and within the Sylvester matrix. To this end we consider the following Hankel matrix.

Definition 5.20
For $z = (z_0, \ldots, z_{2n-2})$ we define the *Hankel-matrix* $H(z)$ to be

$$H(z) \;=\; \begin{pmatrix} z_0 & z_1 & z_2 & \cdots & z_{n-1} \\ z_1 & z_2 & z_3 & \cdots & z_n \\ z_2 & z_3 & z_4 & \cdots & z_{n+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ z_{n-1} & z_n & z_{n+1} & \cdots & z_{2n-2} \end{pmatrix} . \tag{5.5}$$

Now using this notation we can use $H(z)$ in order to define an SDP-based bound. Namely, for $m \leq n+1$ and $m \leq q \leq 2n-2$, consider the following semidefinite optimization problem

$$\mathrm{L}_{nmq} \;=\; \min_{s} \{\, s_q \;\; | \;\; H_n(s) \succeq 0\,;\; s_0 = n\,;\; s_j = \gamma_j, \quad j = 1, \ldots, m-1 \} \,. \tag{5.6}$$

Theorem 5.21
Let $n, m, q \in \mathbb{N}$ with $m \leq n+1$, $m \leq q \leq 2n-2$, and let P_{nmq} be as in (5.4). Then one obtains the following lower bounds on $\min \mathrm{P}_{nmq}$.

(a) $\min \mathrm{P}_{nmq} \geq \mathrm{L}_{nmq}$.

(b) *If $q = m = 2r$ for some r, write*

$$H_{r+1}(s) \;=\; \left(\begin{array}{c|c} H_r(\gamma) & u_r(\gamma) \\ \hline u_r^T(\gamma) & s_{2r} \end{array}\right); \quad u_r(\gamma)^T = (\gamma_r, \ldots, \gamma_{2r-1}),$$

with $\gamma_0 = n$. Then $\min \mathrm{P}_{nmq} \geq u_r(\gamma)^T H_r(\gamma) u_r(\gamma)$.

Proof. (a) Consider the equivalent formulation to problem (5.4) in the orbit space form ((3.5)). With the definition of the Hankel matrix in (5.5) it follows that every solution to the resulting PMI is feasible for the above defined SDP (5.6).

(b) In case $q = m = 2r < 2n$, we observe $r < n$ and

$$H_n(s) \;=\; \left(\begin{array}{c|c} H_{r+1}(s) & U(s) \\ \hline U^T(s) & V(s) \end{array}\right),$$

for some appropriate (possibly empty) matrices

$$U(s) \in \mathbb{R}^{(r+1)\times(n-r-1)} \text{ and } V(s) \in \mathbb{R}^{(n-r-1)\times(n-r-1)}.$$

Therefore, $H_n(s) \succeq 0$ implies $H_{r+1}(s) \succeq 0$, and the final result follows from Schur's complement (Theorem 1.2) applied to the Hankel matrix $H_{r+1}(s)$. □

In certain cases, we can complement this lower bound for problem (1.5) by an upper bound. The idea is to consider potential solutions $x \in \mathbb{R}^n$ of P_{nmq} with at most m non-zero components.

The key will be again to consider a univariate polynomial. Let $f \in \mathbb{R}[t]$ be written

$$f(t) \;:=\; t^m + \sum_{k=0}^{m-1} f_{m-1} t^j \,,$$

and denote $x_1, \ldots, x_m$ the m roots (counting multiplicities) of f. By Theorem 4.15 we have that a necessary and sufficient condition for all roots of f to be real is that that $S(f) \succeq 0$. Now notice that in the power sum bases the first $\lfloor \frac{n}{2} \rfloor$ leading principle minors of $S(f)$ and the Hankel matrix $H_m(s)$, where $H_m(s)$ is the Hankel matrix defined in (5.5) with $s_i = p_i(x_1 \ldots, x_m)$, coincide.

When $q \leq 2m-2$, we investigate the following SDP problem

$$\mathrm{U}_{nmq} \;=\; \min_s \,\{\, s_q \;\;|\;\; H_m(s) \succeq 0\,;\; s_0 = m\,;\; s_j = \gamma_j, \quad j = 1, \ldots, m-1\}\,, \qquad (5.7)$$

which the same as (5.6) except that we now have a Hankel matrix $H_m(s)$ of dimension m instead of $H_n(s)$ of dimension n.

Now by the Newton identities (4.1) it is well known that the power sums $p_k \;=\; \sum_{j=1}^m x_j^k$, $k \geq 0$, of f are known polynomials in its coefficients $\{f_j\}$, and conversely, the coefficients f_j of f are polynomials in the p_j's. i.e., we can write

$$f_j \;=\; P_j(p_0, \ldots, p_{m-1})\,, \qquad j = 0, 1, \ldots$$

for some polynomials $P_j \in \mathbb{R}[p_0, \ldots, p_{m-1}]$.

Hence if one knows p_j for all $j = 1, \ldots, m-1$, then one may compute the f_j's for all $j = 1, \ldots, m-1$, and therefore, we can choose as unknown of our problem the variable f_0 (the only (constant) coefficient of f that we do not know), and write

$$p_j \;=\; P_j(f_0, \ldots, f_{m-1}) \;=\; Q_j(f_0)\,, \qquad j = m, m+1, \ldots$$

for some known polynomials $Q_j \in \mathbb{R}[f_0]$. We claim that Q_j is affine whenever $j \leq 2m-1$. Indeed, this follows from by careful examination of the Newton identities:

$$\begin{aligned}
p_m &= -p_0 f_0 - p_1 f_1 - \cdots - p_{m-1} f_{m-1}\,,\\
p_{m+1} &= -p_1 f_0 - \cdots - p_{m-1} f_{m-2} - p_m f_{m-1}\\
&= -p_1 f_0 - \cdots - p_{m-1} f_{m-2} + f_{m-1}(p_0 f_0 + p_1 f_1 + \cdots + p_{m-1} f_{m-1})\\
&= -f_0(p_1 - p_0 f_{m-1}) - f_1(p_2 - f_{m-1} p_1) - \cdots - f_{m-1}(p_m - f_{m-1} p_{m-1})\,,\\
p_{m+2} &= -p_2 f_0 - \cdots - p_{m-1} f_{m-3} - p_m f_{m-2} - p_{m+1} p_{m-1}\\
&= -p_0(s_2 - p_{m-2} s_0 + p_{m-1} s_1 - s_0 p_{m-1}^2) - \cdots\,,\\
p_{m+3} &= -f_0(p_3 - p_0 f_{m-3} + \cdots) - \cdots
\end{aligned}$$

Therefore, with $q \leq 2m-2$, the SDP problem (5.7) reads

$$\mathrm{U}_{nmq} \;=\; \min_{f_0} \,\{\, Q_q(f_0) \,:\, H_m(s) \succeq 0\} \;, \tag{5.8}$$

where $s_0 = m$ and all the entries s_j of $H_m(s)$ are replaced by their affine expression $Q_j(f_0)$ whenever $m \leq j \leq 2m-2$. This is an SDP with the single variable f_0 only!

Theorem 5.22
Let $n, m, q \in \mathbb{N}$ with $m \leq n$ and $q \leq 2m-2$. Let P_{nmq} be as in (5.4) and let U_{nmq} be as in (5.8). Then

$$\min \mathrm{P}_{nmq} \;\leq\; \mathrm{U}_{nmq}. \tag{5.9}$$

In addition, if P_{nmq} has an optimal solution $x^* \in \mathbb{R}^n$ with at most m non-zero entries, then $\min \mathrm{P}_{nmq} = \mathrm{U}_{nmq}$ and so P_{nmq} has the equivalent convex formulation (5.8).

Proof. Let p_0 be an optimal solution of the SDP (5.8), and consider the monic polynomial $p \in \mathbb{R}[X]$ of degree m which satisfies the Newton identities with $s_j = \gamma_j$, $j = 1, \ldots, m-1$. The vector $x = (x_1, \ldots, x_m)$ of all its roots (counting multiplicities) is real because $H_m(s) \succeq 0$, i.e., its Hankel matrix $H_m(s)$ formed with its Newton sums s_j, $j = 1, \ldots, 2m-2$ (and $s_0 = m$), is positive semidefinite. Let $x^* = (x, 0, \ldots, 0) \in \mathbb{R}^n$. By definition of the Newton sums of p, one has

$$\sum_{i=1}^{n} (x_i^*)^k \;=\; \sum_{i=1}^{m} x_i^k \;=\; \gamma_k, \quad k = 1, \ldots, m-1,$$

which shows that x^* is feasible for P_{nmq}. Therefore, $\mathrm{U}_{nmq} = s_q \geq \min \mathrm{P}_{nmq}$, the desired result. □

Example 5.23
Consider the optimization problem P_{n44}

$$\mathrm{P}_{344}: \quad \min \sum_{i=1}^{3} x_i^4 \quad \text{s.t.} \quad \sum_{i=1}^{3} x_i = 0; \quad \sum_{i=1}^{3} x_i^2 \;=\; 1\,, \quad \sum_{i=1}^{3} x_i^3 \;=\; 0\,,$$

which occurs in the determination of radii of regular simplices (see [BT06]).

It has finitely many solutions; namely $x_1 = 0, x_2 = \frac{1}{\sqrt{2}}$, $x_3 = -\frac{1}{\sqrt{2}}$ and the permutations thereof. Therefore $\min \mathrm{P}_{344} = \frac{1}{2}$. On the other hand,

$$H_3(s) \;=\; \begin{pmatrix} 3 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & s_4 \end{pmatrix}$$

and so by Theorem 5.21(b) we obtain $\min \mathrm{P}_{344} \geq (1,0) \begin{pmatrix} 1/3 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{3}$, a strict lower bound which in this case is also equal to L_{344}. The reason for the gap between L_{344} and P_{344} is that there does not exist a polynomial of degree 3 with Newton sums γ_j and $s_4 = 1/3$. So the positive semidefinite matrix

$$H_3(s) \;=\; \begin{pmatrix} 3 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1/3 \end{pmatrix}$$

is not the Hankel matrix of some polynomial $p \in \mathbb{R}[X]$ of degree 3.

With regard to an upper bound, consider problem P_{n44} with $n \geq m = q = 4$ so that $q \leq 2m - 2 = 6$. There are four coefficients f_0, f_1, f_2 and f_3. Since $p_0 = 4$, $p_1 = 0$, $p_2 = 1$, $p_3 = 0$, the Newton identities allow to compute f_0, f_1, f_2, f_3 via

$$\begin{aligned} f_3 &= -p_1 \;=\; 0\,, \\ f_2 &= (p_1^2 - p_2)/2 = -1/2 \\ f_1 &= (p_1^3 + 2p_3 - 3p_1p_2)/6 \;=\; 0. \end{aligned}$$

Then we can express p_4, p_5, p_6 affinely in terms of f_0 since we have

$$\begin{aligned} p_4 &= -f_3p_3 - f_2p_2 - f_1p_1 - 4f_0 \;=\; 1/2 - 4f_0\,, \\ p_5 &= -f_3p_4 - f_2p_3 - f_1p_2 - f_0p_1 \;=\; 0\,, \\ p_6 &= -f_3p_5 - f_2p_4 - f_1p_3 - f_0p_2 \;=\; 1/4 - 2f_0 - f_0 = 1/4 - 3f_0. \end{aligned}$$

Solving the semidefinite program

$$\min_{p_0} \left\{ \frac{1}{2} - 4f_0 \;:\; \begin{pmatrix} 4 & 0 & 1 & 0 \\ 0 & 1 & 0 & \frac{1}{2} - 4f_0 \\ 1 & 0 & \frac{1}{2} - 4f_0 & 0 \\ 0 & \frac{1}{2} - 4f_0 & 0 & \frac{1}{4} - 3f_0 \end{pmatrix} \succeq 0 \right\}$$

yields the solution $p_0 = 1/16$, showing $\min \mathrm{P}_{n44} \leq 1/16$. Indeed, this solution is optimal.

So when $q \leq 2m-2$, we have obtained lower and upper bounds on $\min \mathrm{P}_{nmq}$ which permits to check the quality of the feasible solution obtained from the upper bound U_{nmq}.

6

SDP based bounds for generalized Hamming distances

> What is the difference between method and device? A method is a device which you used twice.
>
> George Pólya

THIS final chapter discusses the possibilities of bounding sizes of codes using semidefinite programming. In order to obtain numerical results for these SDPs resulting from interesting parameter choices, exploiting symmetries will be an essential step.

A *code* is a subset $\mathcal{C}$ of a finite set X where the elements are called the *words*. These words can be seen as n-tuples over a finite alphabet K. Here the alphabet will consist of the two element set $\{0, 1\}$ and the set of words can be identified with the vector space $\mathbb{F}_2^n$. Given two distinct elements of the code one can assign a distance to the two code words in order to measure how much the words differ from each other. We define this *Hamming distance* $d_H(x, y)$ of two elements $x, y \in \mathbb{F}_2^n$ to be

$$d_H(x, y) := \#\{x_i \neq y_i\},$$

i.e., the number of places where two words x and y are distinct. The *minimal distance* of a code $\mathcal{C}$ then is the minimum of the Hamming distances of all possible pairs of words i.e., $d_{\min}(\mathcal{C}) := \min_{x \neq y \in \mathcal{C}} d_H(x, y)$.

Given this setting an interesting combinatorial question in the construction of good codes is how many distinct words can be combined into a code given that the code has a prescribed *minimal distance*. We will denote by $A(n, d)$ the maximal cardinality that a code $\mathcal{C} \subset \mathbb{F}_2^n$ can have, given that the words in C have at least the prescribed minimal distance d. In the early 1970's Philippe Delsarte [Del72] provided an approach to bound the numbers $A(n, d)$ using linear programming. These linear programming methods have

been until very recently the most powerful tools to estimate $A(n,d)$, and Delsarte's methods were also transferred into other extremal problems as for example the famous sphere packing problem. Already some years later Schrijver [Sch79] and independently McEliece, Rodemich, and Rumsey [MRR78] observed a connection between the Delsarte's bound and the ϑ–number of a graph associated with this problem. However it was not before 2005, when a further developed SDP-based construction was used by Schrijver [Sch05a] in order to obtain better bounds for the numbers $A(n,d)$.

In this chapter we will present an SDP based method in a similar setting. We will consider $H_n := \mathbb{F}_2^n$ the n-dimensional Hamming cube. But instead of the usual Hamming distance we will consider so called *pseudo–distances* that involve k–tuples of points instead of pairs. An example of such a pseudo–distance which is studied in coding theory is the *generalized Hamming distance*.

Definition 6.1
The generalized Hamming distance of k elements of H_n is defined by:

$$\begin{aligned} d_{H,k}(x_1,\ldots,x_k) &= \#\{j,\ 1\le j\le n:\ \#\{(x_1)_j,\ldots,(x_k)_j\}\ge 2\} \\ &= \#\{j,\ 1\le j\le n:\ ((x_1)_j,\ldots,(x_k)_j)\notin\{0^k,1^k\}\} \end{aligned}$$

This notion was introduced in [CLZ94], and takes its origin in the work of Ozarow and Wyner, and of Wei, who studied the generalized Hamming weight of linear codes in view of cryptographic applications. When $k=2$, $d_{H,2}(x_1,x_2)$ is nothing else than the usual Hamming distance. A first systematic treatment of bounds in such cases was provided by Bachoc and Zémor in [BZ10]. The authors there give an SDP–method for 3-tuples distances. In this chapter we aim to generalize their approach to general k–tuples.

6.1 Delsarte's bound

The first linear programming approach to give bounds for codes was introduced by Philippe Delsarte in his thesis. The important observation made by Delsarte was that he could use the distribution of the Hamming distance in a code to design a linear program.

More precisely, Delsarte observed that there is a family of orthogonal polynomials, the so called *Krawtchouk polynomials* $K_k^n(t)$ (see Definition 6.4 below) which satisfy a positivity property, namely for all $C\subset H_n$ we have:

$$\sum_{(x,y)\in H_n^2} K_k^n(d_H(x,y))\ge 0. \tag{6.1}$$

The variables for the linear programming bound are related to the *distance distribution* $(x_i)_{0\le i\le n}$ of a code C defined as

$$x_i := \frac{1}{|C|}|\{(x,y)\in C^2\ :\ d_H(x,y)=i\}|.$$

Using the above positivity condition 6.1 Delsarte concluded that the x_i satisfy the following linear inequalities:

1. $\sum_{i=0}^{n} K_k^n(i)x_i \geq 0$ for all $0 \leq k \leq n$,
2. $x_i \geq 0$,
3. $x_0 = 1$,
4. $\sum_{i=0}^{n} x_i = |C|$.

Furthermore the premise on the minimal distance $d_H(C) \geq d$ implies that $x_i = 0$ for $i = 1, \ldots, d-1$.

These inequalities were used by Delsarte to obtain a linear program in real variables y_i, the optimal value of which gives and upper bound for the number $A(n,d)$ [Del72]:

$$\begin{aligned} \max \Big\{ \textstyle\sum_{i=0}^{n} x_i : \quad & x_i \geq 0, \\ & x_0 = 1, \\ & x_i = 0 \ \text{ if } i = 1, \ldots, d-1 \\ & \textstyle\sum_{i=0}^{n} K_k^n(i)x_i \geq 0 \quad 0 \leq k \leq n \Big\} \end{aligned} \tag{6.2}$$

Later McEliece, Rodemich, and Rumsey and independently Schrijver discovered a fundamental connection between Delsarte's linear programming bound and a strengthening of the ϑ–number defined in Chapter 2. This strengthened parameter ϑ' is obtained by adding a nonnegativity constraint to the original definition of ϑ (see Definition 1.8):

Definition 6.2
For a graph $G = (V, E)$ the parameter $\vartheta'(G)$ is defined by

$$\begin{aligned} \vartheta'(\Gamma_k^n) \quad = \max \Big\{ \textstyle\sum_{i,j} B_{i,j} : \quad & B \in \mathbb{R}^{n \times n}, \ B \succeq 0 \\ & \textstyle\sum_i B_{i,i} = 1, \\ & B_{ij} \geq 0, \\ & B_{i,j} = 0 \quad (i,j) \in E \Big\} \end{aligned} \tag{6.3}$$

The connection of this parameter to Delsarte's approach comes from considering the graph $\Gamma = (H_n, E(d))$ whose vertex set is the Hamming space $H_n = \{x_1, \ldots, \}$ and two vertices $x_i, x_j \in H_n$ are connected by an edge if their Hamming distance is strictly less than d. Now the stability number of Γ is precisely the number $A(n,d)$ and therefore the number $\vartheta'(\Gamma)$ provides an upper bound: Thus we can conclude the following theorem.

Theorem 6.3
The optimal solution of the following SDP provides an upper bound for $A(n,d)$:

$$\begin{aligned} \vartheta'(\Gamma) \quad = \max \Big\{ \textstyle\sum_{i,j} B_{i,j} : \quad & B \in \mathbb{R}^{2^n \times 2^n} \\ & \textstyle\sum_i B_{i,i} = 1, \\ & B_{i,j} = 0 \quad \textit{whenever } 0 < d_H(x_i, X_j) < d \\ & B_{ij} \geq 0, \\ & B \succeq 0 \Big\} \end{aligned} \tag{6.4}$$

At first sight it may seem that the above SDP (6.4) is more complicated than the linear programming bound given by Delsarte. Indeed the size of the matrix B is exponential in n and instead of an LP we have to deal with an SDP. However, the insight of the above mentioned authors was that (6.4) can be symmetrized and brought into the form of a linear program that agrees with the version given by Delsarte.

To see this we consider the group $\mathrm{Aut}(H_n)$ of distance preserving automorphisms of the Hamming cube. This means the elements of $\mathrm{Aut}(H_n)$ are precisely those bijections $\sigma : H_n \to H_n$ which preserve Hamming distances. This group has order $2^n n!$ and is generated by all $n!$ permutations of the n coordinates and all 2^n switches of 0 and 1. The key in order to relate (6.4) with Delsarte's bound now comes by exploiting the symmetry of this very big group.

The first crucial observation to make is that the decomposition into irreducible $\mathrm{Aut}(H_n)$–modules is given by

$$H_n = H_n^0 \oplus H_n^1 \oplus \ldots \oplus H_n^n,$$

where $H_n^i := \{x \in H_n : |x| = i|\}$.

This gives that all irreducible $\mathrm{Aut}(H_n)$-modules involved in the decomposition have multiplicity 1. Recalling the arguments presented in Chapter 2 this observation implies that in fact all $\mathrm{Aut}(H_n)$ invariant matrices can be block diagonalized into matrices decomposing into blocks of size 1×1. Hence the SDP (6.4) will simplify into a linear program.

Further using Fourier analysis on the Hamming cube, one can even more explicitly characterize the invariant matrices. To obtain this description of these matrices, the following family of orthogonal polynomials is important:

Definition 6.4
For $0 \leq k \leq n$ we define the *Krawtchouk polynomial* K_k by

$$K_k^n(t) = \sum_{j=0}^{k} (-1)^j \binom{t}{j} \binom{n-t}{k-j}.$$

With these polynomials the positive semidefinite $\mathrm{Aut}(H_n)$ invariant matrices are characterized as follows:

Theorem 6.5
A matrix $A \in \mathbb{R}^{2^n \times 2^n}$ is $\mathrm{Aut}(H_n)$ invariant and positive semidefinite, if and only if

$$A(x,y) = \sum_{k=0}^{n} f_k K_k^n(d_h(x,y)),$$

for nonnegative numbers $f_0, \ldots, f_n$.

See [Sch79, Val08, CS99] for more details and a proof. Now applying the above characterization to (6.4) we arrive on an alternative way at the classical Delsarte bound.

This viewpoint that connects the formulation of ϑ' to the code problem was later used by Schrijver [Sch05a] in order to derive a strengthening of Delsarte's LP-bounds via semidefinite programming. This way is in fact the route we are about to take in the next section in order to define similar bounds for codes with generalized Hamming distances.

6.2 SDP-bounds via a generalized ϑ'

In this section we aim to give a generalization of Lovasz's ϑ–number to hypergraphs and use this in order to derive bounds for generalized Hamming distances. Instead of pairs of words we will have to deal with k–tuples.

Let $C \subset H_n$ be a subset of the Hamming space such that for all $\underline{z} = (z_1, \ldots, z_k) \in C^k$, we have that $\underline{z}$ belongs to some given set Ω. In the very same way as the graph Γ used in the previous section this situation can be visualized with a combinatorial structure: A *hypergraph* is a set of vertices and hyperedges where each hyperedge can connect more than 2 vertices. Such a hypergraph is said to be k-uniform, if each hyperedge connects exactly k vertices. Thus, by defining hyperedges between a k-tuple of words $(z_1, \ldots, z_k)$ if and only if $(z_1 \ldots, z_k) \notin \Omega$ we naturally associate a k-uniform hypergraph to this situation.

In the context of a pseudo–distance $f(z_1, \ldots, z_k)$ we want to study codes C such that $f(\underline{z})$ is restricted to some range of values, for all $\underline{z} \in C^k$. This leads to the following definition of Ω:

Definition 6.6
For $k \in \mathbb{N}$, $s \leq k$, and $\delta > 0$ set

$$\Omega = \Omega(f, s, \delta) = \{\underline{z} \in H_n^k : f(z_{i_1}, \ldots, z_{i_s}) \geq \delta \text{ for all } 1 \leq i_1 < \cdots < i_s \leq k \text{ and } z_{i_l} \neq z_{i_m}\}.$$

Following the standard notation in coding theory, the maximal number of elements of a code C such that $C^k \subset \Omega$ is denoted $A(n, \Omega)$. In this section we show how to obtain an upper bound for $A(n, \Omega)$ by means of a semidefinite program.

Now to give bounds $A(n, \Omega)$ we start from the same ideas as were used in the definition of the ϑ-parameter. We consider the following function $F_C : H_n^k \to \mathbb{R}$:

$$F_C(z_1, \ldots, z_k) := \frac{1}{|C|} \mathbb{1}_C(z_1) \cdots \mathbb{1}_C(z_k),$$

where $\mathbb{1}_C$ is the characteristic function of the set C.

The analogy to the definition of ϑ becomes clearer by observing that F_C has following properties:

1. We have $F_C(z_1, \ldots, z_k) = F_C(z'_1, \ldots, z'_k)$ for all $\{z_1, \ldots, z_k\} = \{z'_1, \ldots, z'_k\}$. This in turn implies that $F_C(\underline{z})$ only depends on the set $\{z_1, \ldots, z_k\}$ rather than on the k-tuple $(z_1, \ldots, z_k)$.
2. For all $k-2$ tuples $(z_1, \ldots, z_{k-2}) \in H_n^{k-2}$, the application
$$(x, y) \mapsto F_C(z_1, \ldots, z_{k-2}, x, y)$$
is positive semidefinite.
3. $F_C(z_1, \ldots, z_k) \geq 0$.
4. $F_C(z_1, \ldots, z_k) = 0$ if $(z_1, \ldots, z_k) \notin \Omega$.
5. $\sum_{x \in H_n} F_C(x) = 1$.
6. $\sum_{(x,y) \in H_n^2} F_C(x, y) = |C|$.

Remark 6.7
Note that with (1) it makes sense to define $F_C(z_1, \ldots, z_s)$ for $s < k$ being the value of χ at any k-tuple $(y_1, \ldots, y_k)$ with $\{y_1, \ldots, y_k\} = \{z_1, \ldots, z_s\}$, e.g., $(y_1, \ldots, y_k) = (z_1, \ldots, z_s, z_s, \ldots, z_s)$.

A closer analysis of condition (2) shows that an even stronger condition holds:

Proposition 6.8
The function $F_C(z_1, \ldots, z_k)$ defined above satisfies:
(2') For all $(z_1, \ldots, z_{k-2}) \in H_n^{k-2}$, and all $I \subset \{1, \ldots, k-2\}$,
$$(x, y) \mapsto \sum_{I \subset J \subset \{1, \ldots, k-2\}} (-1)^{|J|-|I|} F_C(z_{j(j \in J)}, x, y) \succeq 0 \text{ and } \geq 0.$$

Proof. Since the last expression equals
$$\prod_{i \in I} \mathbb{1}_C(z_i) \prod_{i \notin I} (1 - \mathbb{1}_C(z_i))\, \mathbb{1}_C(x)\, \mathbb{1}_C(y),$$
the above proposition is immediate. □

These conditions now can be used to define two cones of functions $F : H_n^k \to \mathbb{R}$ which will lead to a semidefinite program which will be used to derive bounds on the numbers $A(n, \Omega)$.

Definition 6.9
For $k \in \mathbb{N}$ we define the set $\mathcal{C}_k^0$, respectively $\mathcal{C}_k$, to be the functions
$$F : H_n^k \to \mathbb{R}$$

such that

$$F(z_1,\dots,z_k) = F(\{z_1,\dots,z_k\}) \text{ for all } (z_1,\dots,z_k) \in H_n^k,\ F(z_1,\dots,z_k) \geq 0,$$

and

$$(x,y) \mapsto F(z_1,\dots,z_{k-2},x,y) \succeq 0,$$

respectively

$$(x,y) \mapsto \sum_{I\subset J\subset\{1,\dots,k-2\}} (-1)^{|J|-|I|} F(z_{j_{(j\in J)}},x,y) \succeq 0,$$

and takes nonnegative values for all $(z_1,\dots,z_{k-2}) \in H_n^{k-2}$, and all $I \subset \{1,\dots,k-2\}$.

Example 6.10
Let us work out the positive semidefinite conditions in the definition of $\mathcal{C}_k$ for small k.

1. For $k = 2$, it is clear that it agrees with the standard notion of the cone of two variable positive definite functions on H_n.
2. For $k = 3$, the positive semidefinite conditions on F are
$$\begin{cases} (x,y) \mapsto F(z_1,x,y) \succeq 0 \\ (x,y) \mapsto F(x,y) - F(z_1,x,y) \succeq 0. \end{cases}$$
3. For $k = 4$, we have the following three positive semidefinite conditions:
$$\begin{cases} (x,y) \mapsto F(z_1,z_2,x,y) \succeq 0 \\ (x,y) \mapsto F(z_1,x,y) - F(z_1,z_2,x,y) \succeq 0 \\ (x,y) \mapsto F(x,y) - F(z_1,x,y) - F(z_2,x,y) + F(z_1,z_2,x,y) \succeq 0. \end{cases}$$

Now we can define a semidefinite program whose optimal value provides an upper bound for the number of elements of any code C such that $C^k \subset \Omega$.

$$\max\Big\{ \textstyle\sum_{(x,y)\in H_n^2} F(x,y) : \begin{array}{l} F : H_n^k \to \mathbb{R}, \\ F \in \mathcal{C}_k^0 \\ F(z_1,\dots,z_k) = 0 \text{ if } (z_1,\dots,z_k) \notin \Omega \\ \sum_{x\in H_n} F(x) = 1 \Big\}. \end{array} \qquad \boxed{P_k^0}$$

Similarly, a program $\boxed{P_k}$ is defined by the same conditions except $F \in \mathcal{C}_k$.

Theorem 6.11
The optimal values of the above defined semidefinite programs, denoted $\vartheta_k(\Omega)$ and $\vartheta_k^0(\Omega)$, satisfy:

$$A(n,\Omega) \leq \vartheta_k(\Omega) \leq \vartheta_k^0(\Omega). \qquad \boxed{6.5}$$

Let $2 \leq s \leq k$ and let $\Omega \subset H_n^s$. Then Ω obviously induces subsets $\Omega(k) \subset H_n^k$, and we have

$$A(n,\Omega) \leq \cdots \leq \vartheta_k(\Omega(k)) \leq \vartheta_{k-1}(\Omega(k-1)) \leq \cdots \leq \vartheta_s(\Omega). \tag{6.6}$$

The same inequalities hold for ϑ_k^0.

Proof. The inequality $\vartheta_k \leq \vartheta_k^0$ is obvious by the inclusion $\mathcal{C}_k \subset \mathcal{C}_k^0$. Together with the above discussion, we have (6.5). It is clear that $A(n,\Omega) = A(n,\Omega(k))$ thus $A(n,\Omega) \leq \vartheta_k(\Omega(k))$ for all $k \geq s$. If F is a feasible solution for the program defining $\vartheta_k(\Omega(k))$, then $F(z_1, z_2, \ldots, z_{k-1})$ provides a feasible solution for $\vartheta_{k-1}(\Omega(k-1))$ with the same objective value, thus the inequality $\vartheta_k(\Omega(k)) \leq \vartheta_{k-1}(\Omega(k-1))$. □

6.3 Exploiting symmetries

The sizes of the above defined SDPs are out of reach for current SDP–solvers for interesting choices of n. Therefore it is necessary to exploit the action of the group of automorphisms of H_n in order to reduce the complexity of the SPD (P_k) and (P_k^0). Recall that this group of automorphisms $\mathrm{Aut}(H_n)$ is the semi–direct product of the group of translations by elements of H_n with the group of permutations on the n coordinates.

For the sake of simplicity of the exposition we deal in the remaining with the weaker but simpler to expose version (P_k^0). The block diagonalization of the matrices in $\mathcal{C}_k$ then follows the same line of ideas.

By its definition the set Ω is invariant under the action of $G := \mathrm{Aut}(H_n)$. From this it follows that the SDP (P_k^0) is G–invariant thus by the arguments provided in Chapter 2 we can restrict in (P_k^0) to the G-invariant functions F. Therefore we need a characterization of those elements of the cone $\mathcal{C}_k^0$ which are G-invariant.

In what follows we will look at a k-tuple $\underline{z}$ of points $z_1, \ldots, z_k$ in H_n and we want to first characterize its stabilizer under G. Without loss of generality we can choose the k-tuple in such a way that z_1 is the zero word and the k-tuple is ordered lexicographically and we need to study the action of G on k-tuples $(z_1, \ldots, z_k) \in H_n^k$.

This has already been done in [BZ10]. The orbits can be characterized using the following notation:

Definition 6.12
For $\underline{z} = (z_1, \ldots, z_k) \in H_n^k$, and for $u \in \mathbb{F}_2^k$, let

$$n_u(\underline{z}) := \#\{\ j,\ 1 \leq j \leq n : ((z_1)_j, \ldots, (z_k)_j) = u\}$$

and let the *weight distribution* of $\underline{z}$ be defined by

$$\mathcal{W}(\underline{z}) := (n_u(\underline{z}))_{u \in \mathbb{F}_2^k}.$$

In order to understand the above definition it is useful to visualize $\underline{z}$ using the (k, n) matrix $M(\underline{z})$ whose i-th line equals z_i. In this view the number $n_u(\underline{z})$ corresponds to the number of columns of $\underline{z}$ which are equal to u:

$$M(\underline{z}) = \begin{pmatrix} z_1 & = 000\ldots0 & \ldots\ldots \\ z_2 & = 111\ldots1 & \ldots\ldots \\ \vdots & = \quad \vdots \quad \vdots & \\ z_k & = \underbrace{111\ldots1}_{n_u(\underline{x})} & \ldots\ldots \end{pmatrix}.$$

With this notation Bachoc and Zémor characterized the action of $Aut(H_n)$ on $k-$tuples:

Proposition 6.13 (Bachoc-Zémor)
Let $\underline{z}, \underline{y} \in H_n^k$. Then we have

$$\underline{z} \sim_{\mathrm{Aut}(H_n)} \underline{y} \text{ if and only if } \mathcal{W}(\underline{z}) = \mathcal{W}(\underline{y}).$$

Now a natural number n will be associated with its *binary representation* $\mathrm{bin}(n)$. This notation alows to define the number t_i as $t_i = n_{\omega_i}(\underline{z})$ where $\omega_i = \mathrm{bin}(2i)$ for every i in $[0 \ldots 2^{k-1} - 1]$. Now the following proposition which characterizes the stabilizer of $\underline{z}$ is straight forward:

Proposition 6.14
Let $G_{\underline{z}} < Aut(H_n)$ be the stabilizer of a k-tuple $\underline{z}$. Then

$$G_{\underline{z}} \cong S_{t_0} \times S_{t_1} \times \ldots \times S_{t_{2^{k-1}-1}}.$$

In order to calculate the zonal matrices for a block diagonalization, we need to decompose the space $\mathcal{C}(H_n)$ of functions $F : H_n \to \mathbb{R}$ into irreducible $G_{\underline{z}}$–modules. We start with the decomposition into irreducibles for $\mathcal{S}_n$. This is rather classical (see [Val08] and the references therein):

As obviously each of the sets $H_n^i := \{x \in H_n : |x| = i|\}$ is closed under the action of $\mathcal{S}_n$, a first orbit decomposition will give us

$$\mathcal{C}(H_n) = \mathcal{C}(H_n^0) \perp \mathcal{C}(H_n^1) \perp \ldots \perp \mathcal{C}(H_n^n).$$

We follow the notation provided in Chapter 2 and denote $M^{(n-i,i)}$ the module corresponding to $\mathbf{1}\uparrow_{\mathcal{S}_{n-i}\times\mathcal{S}_i}^{\mathcal{S}_n}$. Now we study the action of $\mathcal{S}_n$ on $\mathcal{C}(H_n^i)$. As each element in $\mathcal{C}(H_n^i)$ is stabilized by a group isomorphic to $\mathcal{S}_{n-i} \times \mathcal{S}_i$ we can conclude that as an $\mathcal{S}_n$ module $\mathcal{C}(H_n^i)$ is isomorphic to $M^{(n-i,i)}$ when $i \leq \frac{n}{2}$ and to $M^{(i,n-i)}$ otherwise.

Now using Young's Rule (see Theorem 2.29) this characterization immediately yields the decomposition of $\mathcal{C}(H_n^i)$ into irreducibles:

$$\mathcal{C}(H_n^m) = \begin{cases} W_{0,m}^n \perp \ldots \perp W_{m,m}^n, & \text{when } 0 \leq m \leq \lfloor n/2 \rfloor, \\ W_{0,m}^n \perp \ldots \perp W_{n-m,m}^n, & \text{otherwise,} \end{cases}$$

where $W_{k,m}^n$ are irreducible S_n-modules isomorphic to $\mathfrak{S}^{(n-k,k)}$. The dimension of $W_{k,m}^n$ i.e., the number of standard Young tableaux for $(n-k,k)$ is $d_k^n = \binom{n}{k} - \binom{n}{k-1}$.

Furthermore, the corresponding zonal matrices $E_k(x,y)$ have been explicitly characterized by several authors (see for example [Sch05a, Val08] and the references therein) using the so called Hahn polynomials.

The Hahn polynomials associated with the parameters n, s, t with $0 \leq s \leq t \leq n$ are the polynomials $Q_k(n,s,t;x)$ with $0 \leq k \leq \min(s, n-t)$ uniquely determined by the properties:

1. The degree of Q_k in the variable x is k.
2. They are orthogonal polynomials for the weights

$$0 \leq i \leq s \quad w(n,s,t;i) = \binom{s}{i}\binom{n-s}{t-s+i}.$$

3. $Q_k(0) = 1$.

Theorem 6.15 (Schrijver, Vallentin)
If $k \leq s \leq t \leq n-k$, $wt(x) = s$, $wt(y) = t$,

$$E_{k,s,t}(x,y) = |X| \frac{\binom{t-k}{s-k}\binom{n-2k}{t-k}}{\binom{n}{t}\binom{t}{s}} Q_k(n,s,t; s - |x \cap y|).$$

If $wt(x) \neq s$ or $wt(y) \neq t$, $E_{k,s,t}(x,y) = 0$.

In order to relate the decomposition for the group $G_{\underline{z}}$ with the above decomposition we will need some notations:

For $x \in H_n$ and $i \in [0, \ldots, 2^{k-1}-1]$ we define $x(i)$ to be a word in H_{t_i} such that the concatenation of all $x(i)$ equals x. Further for every weight distribution $\omega := (\omega_0, \ldots \omega_{2^{k-1}-1})$ we can define the set

$$H_n^\omega := \{x \in H_n : |x(i)| = w_i\}.$$

These sets give rise to the following decomposition

$$\mathcal{C}(H_n) = \bigoplus_\omega \mathcal{C}(H_n^\omega),$$

which is exactly the decomposition into the various orbits.
Furthermore we have the decomposition of $\mathcal{S}_{t_i}$-modules:

$$\mathcal{C}(H_{t_i}) = \bigoplus_{\omega_i=0}^{\omega_i=t_i} \mathcal{C}(H_{t_i}^{\omega_i}).$$

Now we can use the decomposition of $x \in H_n$ into $(x(1), x(2), \ldots, x(2^{k-1}-1))$ to define

$$\begin{array}{rcl} \phi : \bigotimes \mathcal{C}(H_{t_i}^{\omega_i}) & \longrightarrow & \mathcal{C}(H_n^{\omega}) \\ \otimes f_i & \longmapsto & f(x) = \prod_i f(x(i)) \end{array}.$$

As ϕ preserves the group action we only need to decompose each S_{t_i}-module $\mathcal{C}(H_{t_i}^{\omega_i})$. Again using Young's Rule for the group $\mathcal{S}_{t_i}$ we get:

$$\mathcal{C}(H_{t_i})^{\omega_i} = \begin{cases} W_{0,\omega_i}^{t_i} \perp \ldots \perp W_{\omega_i,\omega_i}^{t_i}, & \text{when } 0 \leq \omega_i \leq \lfloor t_i/2 \rfloor, \\ W_{0,\omega_i}^{t_i} \perp \ldots \perp W_{t_i-\omega_i,\omega_i}, & \text{otherwise.} \end{cases}$$

Putting all this together we see that the irreducible representations of

$$\mathcal{S}_{t_0} \times \cdots \times \mathcal{S}_{t_{2^{k-1}-1}}$$

that will appear in the decomposition are indexed by

$$K = (k_0, \ldots, k_{2^{k-1}-1}) \text{ with } 0 \leq k_i \leq \lfloor t_i/2 \rfloor$$

and we can announce the following theorem.

Theorem 6.16
Let $T = (t_0, \ldots, t_{2^{k-1}-1})$ such that $\sum_{i=0}^{2^{k-1}-1} t_i = n$ and let

$$S_T = S_{t_0} \times S_{t_1} \times \ldots \times S_{t_{2^{k-1}-1}}.$$

Then the following holds:

1. *The decomposition into irreducible S_T spaces is given by*

$$\mathcal{C}(H_n) = \bigoplus_{\omega} \bigotimes_{k_i \leq \min(\omega_i, t_i-\omega_i)} W_{k_i,\omega_i}^{t_i}.$$

2. *The dimension of an irreducible component belonging to K is given by $\prod_i d_i^{k_i}$.*
3. *The corresponding zonal matrices are given by*

$$E_K^T(x,y) = \bigotimes_i E_{k_i}^{t_i}(x(i), y(i)).$$

Proof. The first and second statement follow directly from the above argumentation and (3) can be deduced from these. □

Now in order to characterize the elements of $\mathcal{C}_k^0$ we let $\underline{z} := (z_1, \ldots, z_{k-2}) \in H_n^{k-2}$. The orbit $o_G(\underline{z})$ of such a $k-2-$tuple $\underline{z}$ under the action of G is characterized by a sequence of non negative integers $T = (t_0, \ldots, t_{2^{k-3}-1})$ as described above.

Each t_i is associated to a set of indices I_i such that $t_i = |I_i|$ and the columns of $M(\underline{z})$ with these indices equal either $\mathrm{bin}(2i)$ or $\mathrm{bin}(2^{k-2} - 1 - 2i)$. For $x \in H_n$, let $x(i)$ denote the restriction of x to the indices in I_i. Let, for $0 \leq k_i \leq \lfloor t_i/2 \rfloor$,

$$E_K^T(z_1, \ldots, z_{k-2}, x, y) := \otimes E_{k_i}^{t_i}((x - z_1)(i), (y - z_1)(i)). \tag{6.7}$$

It is clear that $E_K^T(z_1, \ldots, z_{k-2}, x, y)$ is invariant under the action of G, in other words that

$$E_K^T(g(z_1), \ldots, g(z_{k-2}), g(x), g(y)) = E_K^T(z_1, \ldots, z_{k-2}, x, y) \text{ for all } g \in G.$$

Thus we can conclude that the matrices

$$E_K^T(\underline{z}, x, y) := E_K^T(z_1, \ldots, z_{k-2}, x, y) \text{ where } K = (k_0, \ldots) \text{ varies,}$$

characterize the cone of $G_{\underline{z}}$-invariant positive definite functions, where $G_{\underline{z}}$ denotes the stabilizer of $\underline{z}$ in G, namely we have:

Proposition 6.17
Let $f : H_n^2 \to \mathbb{R}$ be $G_{\underline{z}}$-invariant. Then $f \succeq 0$ if and only if, for all K,

$$\sum_{(x,y) \in H_n^2} f(x, y) E_K^T(\underline{z}, x, y) \succeq 0.$$

Using this characterization we can go back to the G-invariant functions F and we obtain the following characterization for the elements in $\mathcal{C}_k^0$.

Theorem 6.18
Let $f : H_n^k \to \mathbb{R}$ be G invariant. Then we have $F \in \mathcal{C}_k^0$ if and only if, for all $\underline{z} \in H_n^{k-2}$, with $T = o_G(\underline{z})$, and all K,

$$\sum_{(x,y) \in H_n^2} F(\underline{z}, x, y) E_K^T(\underline{z}, x, y) \succeq 0. \tag{6.8}$$

With these thoughts at hand we can construct the simplified version which exploits the symmetry.

In order to avoid confusion, we adopt the notation

$$U = (u_0, u_1, \ldots, u_{2^k-1-1})$$

for the sequence of integers associated with an orbit of G acting on H_n^k, and we denote by $\mathcal{O}_k$ the set of these orbits.

We freely identify the sequence U and the element of $\mathcal{O}_k$ which is represented by U. Since F and E_K^T are G-invariant, they define functions on $\mathcal{O}_k$, that we continue to denote respectively $F(U)$ and $E_K^T(U)$. Let $|U|$ denotes the number of elements in the orbit represented by U. Then define the variables

$$X_U := |U|F(U). \tag{6.9}$$

Further define the mapping $\tau : \mathcal{O}_k \to \mathcal{O}_{k-2}$ that sends

$$U = o_G((z_1, \ldots, z_k)) \text{ to } \tau(U) = o_G((z_1, \ldots, z_{k-2})).$$

Then with this definitions (6.8) is equivalent to

$$\sum_{U \in \mathcal{O}_k \,:\, \tau(U)=T} X_U E_K^T(U) \succeq 0. \tag{6.10}$$

The reduction of the SDP (P_k^0) will be completed by also taking the property

$$F(z_1, \ldots, z_k) = F(\{z_1, \ldots, z_k\})$$

into account. This just implies that F is in fact a function on the orbits of G on $\mathfrak{P}_k(H_n)$, the set of subsets of H_n with at most k elements. This set of orbits will be denoted $\mathcal{O}_k^s$. The obviously defined mapping

$$\text{set} : \mathcal{O}_k \to \mathcal{O}_k^s \text{ sends } o_G((z_1, \ldots, z_k)) \text{ to } o_G(\{z_1, \ldots, z_k\}).$$

Note that it is not true that $E_K^T(U) = E_K^T(U')$ if $\text{set}(U) = \text{set}(U')$.

For $V \in \mathcal{O}_k^s$, $V \neq \emptyset$, let

$$S_K^T(V) := \sum_{U \,:\, \tau(U)=T,\, \text{set}(U)=V} E_K^T(V).$$

With this we obtain

Theorem 6.19
The optimal value of the SDP (P_k^0) agrees with the optimal value of the following:

$$\max \Big\{ \textstyle\sum_{V \in \mathcal{O}_2} X_V : \begin{array}{l} (X_V)_{V \in \mathcal{O}_k^s} \in \mathbb{R}, \\ \displaystyle\sum_V X_V S_K^T(V) \succeq 0, \\ X_V \geq 0, \\ X_V = 0 \text{ if } V \notin \overline{\Omega}, \\ X_1 = 1 \Big\} \end{array} \tag{P_k'}$$

where the semidefinite constraint is required for all $T = (t_i) \in \mathcal{O}_{k-2}$, *and all* $K = (k_i)$, $0 \leq k_i \leq \lfloor t_i/2 \rfloor$, *where* $\overline{\Omega} := \{\mathrm{set}(o_G(\underline{z})), \underline{z} \in \Omega\}$ *and where* $1 \in \mathcal{O}_k^s$ *denotes the unique* G*-orbit of singleton.*

6.4 Final remarks and numerical results

In this last section we will provide a link to a general framework introduced by Laurent. Her *combinatorial moment matrix* can be seen as a generalization of all types of hierarchies which have been defined for combinatorial problems so far. Secondly we are presenting the list of numerical results which were obtained using the approach described above for the generalized hamming distance.

6.4.1 The general framework

The hierarchy proposed in this chapter can be seen as a specific instance of a more general approach. This *combinatorial moment matrix*-approach was introduced by Laurent (see Laurent [Lau09]). Let V be a finite set and consider its power set $\mathfrak{P}(V)$. Given a sequence $(y)_\alpha$ of real numbers indexed by the elements of $\mathfrak{P}(V)$ (i.e., by the subsets of V) we define the combinatorial moment matrix as follows:

Definition 6.20
Let (y_α) be a sequence as defined above. The combinatorial moment matrix $M(y)$ is the $\mathfrak{P}(V) \times \mathfrak{P}(V)$-matrix matrix given by

$$[M(y)]_{S,T} = y_{S \cup T}.$$

Take any subset $C \subseteq V$ and consider the characteristic function $\mathbb{1}_C$ of C, which leads naturally to a sequence $y \in \{0,1\}^{\mathfrak{P}(V)}$ by setting

$$y_S = \prod_{v \in S} \mathbb{1}_C(v) \text{ for all } S \in \mathfrak{P}(V).$$

This construction implies that the moment matrix $M(y)$ is positive semidefinite since $M(y) = yy^T$. Now the following theorem of Laurent naturally provides a general framework into which the SDP-approach used in this chapter fits.

Theorem 6.21 (Laurent)
Let $M(y)$ *be a moment matrix with* $y_\emptyset = 1$ *and* $M(y) \succeq 0$. *Then* $M(y)$ *is a convex combination of moment matrices* $M(y_1), \ldots, M(y_k)$, *where* y_i *is obtained from lifting a vector in* $\{0,1\}^V$.

For any graph $\Gamma = (V, E)$ with vertex set V the above Theorem 6.21 yields that the independence number can be calculated by the following:

$$\alpha(\Gamma) = \max\Big\{ \sum_{v\in V} y_{\{v\}} : y_\emptyset = 1, y_S = 0 \text{ if } S \text{ contains an edge}, \\ M(y) \succeq 0\Big\}. \tag{6.11}$$

Although this shows that the independence number is actually given by an SDP, this exponential size of the combinatorial moment matrix makes it impossible to actually calculate it. So one has to restrict to suitable sub matrices.

For example, to recover the SDP given in (P_k^0) define $\mathfrak{P}_k(H_n)$ to be the set of subsets of H_n of cardinality at most k. Then for all $S \in \mathfrak{P}_k(H_n)$ of size $|S| = k-2$ consider the sub matrix of $M_S(y)$ of elements $y_{X\cup Y}$, where X, Y run over the elements of $\mathfrak{P}_k(H_n)$, containing S, and of a size such that $|X \cup Y| \leq k$. If $k = 2$, this agrees exactly the SDP-bounds proposed by Schrijver in [Sch05a].

After the research that led to this chapter had been carried out, Gijswijt, Mittelmann and Schrijver [GMS10] presented a semidefinite bound to improve the current bounds related to the ordinary Hamming distance. Their work in fact generalizes our approach to all $S \subset \mathfrak{P}_4(H_n)$. Albeit their SDPs contain far more constrains, some numerical comparison for small values of $n \leq 12$ suggest that the results that can be obtained using the approach presented in this chapter applied to the classical Hamming distance, do not differ too much.

6.4.2 Numerical results for the generalized Hamming distance

Finally we present numerical results. The following table gives bounds for codes with prescribed minimal generalized Hamming distance $d_{H,4}$. Mostly we were using the weaker constraints resulting from $\mathcal{C}_4^0$ as it turned out that the SDPs coming from the $\mathcal{C}_4$ are already for $n \geq 14$ very hard to solve and numerically unstable with the solvers used to obtain the results. However, for small $n \leq 13$ we found that the optimal value of the two SDPs differs only marginally.

The numerical results were obtained by using first a MAGMA program to generate the SDPs in the form (P_k'). Then the SDPA online solver [FFK$^+$10] was used to calculate the resulting SDPs for $n \leq 17$. The SDPs resulting for $n = 18, 19$ were calculated by Hans Mittelmann [Mit10]. In Table 6.1 we list our results. Every column corresponds to a choice of n. In each row we have collected the corresponding value of the SDP in bold versus the best known bounds as presented by Bachoc and Zémor in [BZ10].

Table 6.1. Bounds on $A(n, d_4, m)$

$m\backslash n$	8	9	10	11	12	13	14	15	16	17	18	19
4	**90** *96*	**179** *192*	**355** *384*	**706** *768*	**1402** *1536*	**2740** *3072*	**5495** *6144*	**6529** *12288*				
5	**45** *48*	**89** *96*	**177** *192*	**342** *384*	**665** *768*	**1264** *1536*	**2370** *3072*	**4959** *6144*	**5381** *11565*			
6	**24** *24*	**44** *48*	**87** *96*	**169** *192*	**307** *384*	**569** *768*	**1072** *1536*	**2068** *3072*	**3797** *6144*	**5950** *12288*		
7	**12** *12*	**24** *24*	**43** *48*	**84** *96*	**167** *192*	**299** *384*	**541** *768*	**1025** *1536*	**1612** *3072*	**3645** *6144*	**4771** *12288*	
8		**12** *12*	**24** *24*	**41** *48*	**79** *96*	**151** *192*	**290** *384*	**520** *768*	**975** *1536*	**1612** *3072*	**3521** *6144*	**3765** *12288*
9			**12** *12*	**24** *24*	**40** *48*	**75** *96*	**142** *192*	**269** *384*	**479** *768*	**879** *1536*	**1660** *3072*	**3123** *6144*
10				**12** *12*	**24** *24*	**39** *48*	**72** *96*	**136** *192*	**258** *384*	**479** *768*	**859** *1536*	**1568** *3072*
11					**12** *12*	**21** *24*	**38** *48*	**70** *96*	**131** *192*	**243** *384*	**460** *768*	**817** *1536*
12						**10** *12*	**21** *24*	**37** *48*	**68** *96*	**126** *192*	**237** *384*	**445** *768*
13							**10** *12*	**20** *24*	**36** *48*	**66** *96*	**121** *192*	**225** *384*
14								**10** *12*	**20** *24*	**36** *48*	**64** *96*	**117** *192*
15									**10** *12*	**20** *24*	**35** *48*	**60** *96*
16										**10** *11*	**20** *24*	**35** *48*
17											**10** *11*	**20** *24*
18												**9** *10*

7

Some open problems and future prospect

In the following we present some open problems, that arose during the preparation of this thesis and will be the ground for further research.

A conjecture on the asymptotic geometry of the symmetric SOS cone

The introduction of this thesis explained the great importance of the two cones $\mathcal{P}_n$ and Σ_n for the freshly emerged paradigms in polynomial optimization. The fact that in general polynomial optimization is hard is reflected on the difference of these two cones. In [Ble06] Blekherman was able to provide deep insight in the geometry of the difference of these two objects. He could show that for fixed degree and growing number of variables asymptotically there are by far more positive polynomials than polynomials that are sums of squares. In chapter five we studied the geometry of the sums of squares cone for fixed degree. Here we have that the dimension of the space of symmetric polynomials of degree $2d$ equals exactly the number of partitions of $2d$ – denoted by $p(2d)$. Hence we see that for $n \geq 2d$ each of the cones $\Sigma_{n+1,2d}^{\mathcal{S}_n}$ of symmetric sums of squares of degree $2d$ and $\mathcal{P}_{n,2d}^{\mathcal{S}_n}$ of positive symmetric polynomials of degree $2d$ is in fact a cone in $\mathbb{R}^{p(2d)}$. Furthermore, a main result was, that the decomposition into semi-invariants is independent of the number of variables once $n \geq 2d$. This in turn implies that every $f \in \Sigma_{n,2d}^{\mathcal{S}_n}$ naturally corresponds to a polynomial $\tilde{f} \in \Sigma_{n+1,2d}^{\mathcal{S}_{n+1}}$. On the other hand the number of constraints that the the coefficients of a symmetric polynomial in fixed degree has to verify in order to be positive grows with the number of variables. Thus the cone $\mathcal{P}_{n,2d}^{\mathcal{S}_n}$ gets more and more constraint.

These two observations combined give rise to the following conjecture:

Conjecture 7.1
Asymptotically for d fixed and $n \to \infty$ the difference of the two cones $\mathcal{P}_{n,2d}^{\mathcal{S}_n}$ and $\Sigma_{n,2d}^{\mathcal{S}_n}$ gets smaller.

Very recently this conjecture was verified for the special case $d = 4$. Together with

Blekherman we show in [BR11b] that actually

$$\lim_{n\to\infty} \mathcal{P}_{n,4}^{\mathcal{S}_n} = \lim_{n\to\infty} \Sigma_{n,4}^{\mathcal{S}_n}$$

holds. So the more variables we allow the more unlikely it gets that a positive symmetric polynomial is not a sum of squares.

Topology of symmetric real varieties

The topology of real varieties is described by the so called Betti numbers. Their sum can be seen as a measure of complexity and therefore bounding these numbers has implications to complexity theory. For general real varieties given by polynomials the best known bounds on the betti numbers are exponential in the number of variables. In the view of Theorem 4.2 and its implications on the complexity of deciding if a given symmetric real variety of fixed degree is empty (Corollary 4.26) Saugata Basu asked whether the presence of symmetry makes better bounds possible. Following Milnor's classical approach [Mil64] this could be done by Morse theory. The classical Morse-lemma (see for example [BPR06]) states that the sum over all Betti numbers of $S := \{x \in \mathbb{R}^n : F(X) = 0\}$ is in fact bounded by the number of critical points of a *Morse function* on S. Now if one considers the critical points of a symmetric polynomial F of degree d it follows from chapter 4 that its critical points lie in "small" orbits, i.e. the critical points lie in a set $A_{\lfloor \frac{d}{2} \rfloor}$. However as it turned out the problem is that some of the points in $A_{\lfloor \frac{d}{2} \rfloor}$ in fact have asymptotically large orbits: Indeed, consider the simple case of points not having more than two distinct components. For every n the point

$$x := (\underbrace{t, t, \ldots, t}_{\lfloor n/2 \rfloor}, \overbrace{s, s, s, \ldots, s}^{\lceil n/2 \rceil})$$

clearly lies in $A_2 \subset \mathbb{R}^n$. However if x is a critical point of F then also all points in the orbit of x are critical points. This in turn implies that the number of critical points behaves asymptotically like the central binomial coefficients, thus exponential in n. So either a finer analysis of the arguments used in chapter 4 can provide ways to exclude such points as critical points or the answer to Basu's question is negative.

Generalizing the degree principle

One of the main motivations to study the original proof of Timofte for the degree and half degree principle was to obtain ways to generalize these beautiful statements to the case of other invariant polynomials. Besides the immediate generalization to even symmetric polynomials this is an open question. However the new proof given in this thesis made it clearer which two properties of symmetric functions are mainly responsible:

1. Independence of the generators: This allowed us to derive the statement on the polynomial G, i.e. we could exclude some of the generators due to their degree.
2. Compactness of the level set: The fact that each set $p_2(X) = a$ is either empty or compact also played a very big role in order to conclude that the minimizers coincide with the critical points.

By a famous Theorem of Chevalley, Shephard, and Todd the first will generalize to all groups which are generated by pseudo reflections. Further even in the case that the generators cannot be chosen to be independent, one could still hope to use other information from the original polynomial F in addition to the degree to deduce a desired representation of the resulting polynomial in the generators. The compactness of the levelsets however seems harder to replace.

Bibliography

[Arm88] M. A. Armstrong. *Groups and symmetry.* Undergraduate Texts in Mathematics. New York: Springer, 1988.

[Art26] E. Artin. Über die Zerlegung definiter Funktionen in Quadrate. *Abhandlungen Hamburg*, 5:100–115, 1926.

[Baca] C. Bachoc. Applications of semidefinite programming to coding theory. Proceedings of ITW, Dublin 2010.

[Bacb] C. Bachoc. Semidefinite programming, harmonic analysis and coding theory. Lecture notes of a course given at the CIMPA summer school Semidefinite Programming in Algebraic Combinatorics, 2009.

[BCR98] J. Bochnak, M. Coste, and M.-F. Roy. *Real algebraic geometry.* Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge 36. Berlin: Springer, 1998.

[BGSV10] C. Bachoc, D. C. Gijswijt, A. Schrijver, and F. Vallentin. Invariant semidefinite programs. arXiv:1007.2905, 2010.

[Ble06] G. Blekherman. There are significantly more nonnegative polynomials than sums of squares. *Isr. J. Math.*, 153:355–380, 2006.

[Ble10] G. Blekherman. Nonnegative polynomials and sums of squares. *preprint*, 2010.

[BNdOFV09] C. Bachoc, G. Nebe, F. M. de Oliveira Filho, and F. Vallentin. Lower bounds for measurable chromatic numbers. *Geom. Funct. Anal.*, 19(3):645–661, 2009.

[Bos07] H. Bosse. Positive polynomials that are not sums of squares. *preprint*, 2007.

[Bou54] V. Bouniakovsky. Note sur les maxima et les minima d'une fonction symetrique entiere de plusieurs variables [note on the maxima and minima of a symmetric function in several variables]. *Bull. Classe Phys.-Math. Acad. Imper. Sci.*, 12:351–361, 1854.

[BPR06] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in real algebraic geometry. 2nd ed.* Algorithms and Computation in Mathematics 10. Berlin: Springer, 2006.

[BR11a] C. Bachoc and C. Riener. On k-tuple bounds for generalized hamming distances. *in preparation*, 2011.

[BR11b] G. Blekherman and C. Riener. On positive symmetric polynomials in degree four. *in preparation*, 2011.

[Brö98] L. Bröcker. On symmetric semialgebraic sets and orbit spaces. *Banach Center Publ.*, 44:37–50, 1998.

[BT06] R. Brandenberg and T. Theobald. Radii minimal projections of polytopes and constrained optimization of symmetric polynomials. *Adv. Geom.*, 6:71–83, 2006.

[BV89] A. I. Barvinok and A. M. Vershik. The representation theory methods in combinatorial optimization problems. *Soviet J. Comput. Systems Sci.*, 27:1–7, 1989.

[BV08] C. Bachoc and F. Vallentin. New upper bounds for kissing numbers from semidefinite programming. *J. Amer. Math. Soc*, 21:909–924, 2008.

[BV09] C. Bachoc and F. Vallentin. Semidefinite programming, multivariate orthogonal polynomials, and codes in spherical caps. *Eur. J. Comb.*, 30(3):625–637, 2009.

[BZ10] C. Bachoc and G. Zémor. Bounds for binary codes relative to pseudo-distances of k points. *Adv. Math. Com.*, 4(4):547–565, 2010.

[CF96] R. Curto and L. A. Fialkow. *Solution of the truncated complex moment problem for flat data.*, volume 568. Mem. Am. Math. Soc., 1996.

[CKS09] J. Cimprič, S. Kuhlmann, and C. Scheiderer. Sums of squares and moment problems in equivariant situations. *Trans. Am. Math. Soc.*, 361(2):735–765, 2009.

[CL78] M. D. Choi and T. Y. Lam. Extremal positive semidefinite forms. *Math. Ann*, 231:1–18, 1978.

[CLO07] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms.* Undergraduate Texts in Mathematics. New York: Springer, 2007.

[CLR87] M. D. Choi, T. Y. Lam, and B. Reznick. Even symmetric sextics. *Math. Z.*, 195:559–580, 1987.

[CLZ94] G. Cohen, S. Litsyn, and G. Zémor. Upper bounds on generalized Hamming distances. *IEEE Trans. Inform. Theory*, 40:2090–2092, 1994.

[CS99] J. H. Conway and N. J. A. Sloane. *Sphere packings, lattices and groups. 3rd ed.* Grundlehren der Mathematischen Wissenschaften. 290. New York: Springer, 1999.

[Del72] P. Delsarte. Bounds for unrestricted codes, by linear programming. *Philips Research Reports*, 27:272–289, 1972.

[Del73] P. Delsarte. An algebraic approach to the association schemes of coding theory. *Philips Research Reports*, 10, 1973.

[Die38] J. Dieudonné. *La théorie analytique des polynômes d'une variable (a coefficients quelconques).* Mem. Sci. Math. Fasc. 93. Paris: Gauthier-Villars, 1938.

[dKPS07] E. de Klerk, D. V. Pasechnik, and A. Schrijver. Reduction of symmetric semidefinite programs using the regular $*$-representation. *Math. Program., Ser. B*, 109:613–624, 2007.

[dOF09] F. M. de Oliveira Filho. *New Bounds for Geometric Packing and Coloring via Harmonic Analisys and Optimization*. PhD thesis, Universiteit van Amsterdam, 2009.

[Dun76] C. F. Dunkl. A krawtchouk polynomial addition theorem and wreath product of symmetric groups. *Indiana Univ. Math. J.*, 25:335–358, 1976.

[FFK+10] K. Fujisawa, M. Fukuda, K. Kobayashi, M. Kojima, K. Nakata, M. Nakata, and M. Yamashita. SDPA: Online for your future. `http://sdpa.indsys.chuo-u.ac.jp/sdpa/`, 2010.

[FH91] W. Fulton and J. Harris. *Representation Theory*. Graduate Texts in Mathematics. 129. New York: Springer, 1991.

[For87] T. H. Foregger. On the relative extrema of a linear combination of elementary symmetric functions. *Linear Multilinear Algebra*, 20:377–385, 1987.

[FS92] A. Fässler and E. Stiefel. *Group theoretical methods and their applications. Transl. from the German by Baoswan Dzung Wong.Rev. transl. Rev. transl.* Boston, MA etc.: Birkhäuser, 1992.

[FW93] F. Fagnani and J. Willems. Representations of symmetric linear dynamical systems. *SIAM J. Control Optim.*, 31:1267–1293, September 1993.

[Gij05] D. C. Gijswijt. *Matrix Algebras and Semidefinite Programming Techniques for Codes.* PhD thesis, Universiteit van Amsterdam, 2005.

[GMS10] D. C. Gijswijt, H. Mittelmann, and A. Schrijver. Semidefinite code bounds based on quadruple distances. *arXiv:1005.4959*, 2010.

[GP04] K. Gatermann and P. Parrilo. Symmetry groups, semidefinite programs, and sums of squares. *J. Pure Appl. Algebra*, 192:95–128, 2004.

[Gri05] D. Grimm. Positivität symmetrischer Polynome [positivity of symmetric polynomials]. Diplomarbeit, Universität Konstanz, 2005.

[Gru07] P. M. Gruber. *Convex and discrete geometry.* Grundlehren der Mathematischen Wissenschaften 336. Berlin: Springer, 2007.

[GSS88] M. Golubitsky, I. Stewart, and D. G. Schaeffer. *Singularities and Groups in Bifurcation Theory II.* Applied Mathematical Sciences. 69. New York: Springer, 1988.

[GW98] R. Goodman and N. R. Wallach. *Symmetry, representations, and invariants. Based on the book 'Representations and invariants of the classical groups*. Graduate Texts in Mathematics 255. New York: Springer, 1998.

[Hav36] E. K. Haviland. On the momentum problem for distribution functions in more than one dimension. II. *Am. J. Math.*, 58:164–168, 1936.

[Hil88] D. Hilbert. Über die Darstellung definiter Formen als Summe von Formenquadraten. *Math. Ann*, 32:342–350, 1888.

[Hil00] D. Hilbert. Mathematische Probleme. Vortrag, gehalten auf dem internationalen Mathematiker-Kongreß zu Paris 1900. *Gött. Nachr.*, pages 253–297, 1900.

[HL03] D. Henrion and J. B. Lasserre. GloptiPoly: Global Optimization over Polynomials with Matlab and SeDuMi. *ACM Trans. Math. Soft*, 29:165–194, 2003.

[HL05] D. Henrion and J. B. Lasserre. Detecting global optimality and extracting solutions in GloptiPoly. In D Henrion and A Garulli, editors, *Positive Polynomials in Control*, volume 312 of *Lecture Notes on Control and Information Sciences*, pages 293–310. Berlin: Springer, 2005.

[HL06] D. Henrion and J. B. Lasserre. Convergent relaxations of polynomial matrix inequalities and static output feedback. *IEEE Trans. Autom. Control*, 51:192–202, 2006.

[Hum92] J. E. Humphreys. *Reflection groups and Coxeter groups.* Cambridge Studies in Advanced Mathematics. 29. Cambridge: Cambridge University Press., 1992.

[JK81] G. James and A. Kerber. *The Representation Theory of the Symmetric Group.* Reading: Addison-Wesley, 1981.

[JLRT06] L. Jansson, J. B. Lasserre, C. Riener, and T. Theobald. Exploiting symmetries in SDP-relaxations for polynomial optimization. *Optimization online, Report*, 1466, 2006.

[Kar84] N. Karmarkar. A new polynomial-time algorithm for linear programming. *Combinatorica*, 4:373–395, 1984.

[Kat84] T. Kato. *Perturbation theory for linear operators. 2nd corr. print. of the 2nd ed.* Grundlehren der Mathematischen Wissenschaften, 132. Berlin: Springer, 1984.

[Ker71] A. Kerber. *Representations of permutation groups. Part I.* Lecture Notes in Mathematics. 240. Berlin: Springer, 1971.

[Kha79] L. G. Khachiyan. A polynomial algorithm in linear programming. *Dokl. Akad. Nauk SSSR*, 244:1093–1096, 1979.

[KK10] S. Kuhlmann and A. Kovačec. Private communication, 2010.

[KKR11] S. Kuhlmann, A. Kovačec, and C. Riener. A note on extrema of linear combinations of elementary symmetric functions. *to appear in Linear and Multilinear Algebra*, 2011.

[KL78] G. A. Kabatiansky and V. I. Levenshtein. Bounds for packings on a sphere and in space. *Problems of Information Transmission*, 14:1–17, 1978.

[KOMK01] Y. Kanno, M. Ohsaki, M. Murota, and N. Katoh. Group symmetry in interior-point methods for semidefinite programming. *Optimization and Engineering*, 2:293–320, 2001.

[KS89] M. Knebusch and C. Scheiderer. *Einführung in die reelle Algebra. [Introduction to real algebra—].* Vieweg Studium, 63: Aufbaukurs Mathematik. Braunschweig: Friedrich Vieweg & Sohn, 1989.

[Las01] J. B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM J. Optim*, 11:796–817, 2001.

[Las04] J. B. Lasserre. Characterizing polynomials with roots in a semi-algebraic set. *IEEE Trans. Autom. Control*, 49:727–730, 2004.

[Las10] J. B. Lasserre. *Moments, positive polynomials and their applications.* Imperial College Press Optimization Series 1, 2010.

[Lau05] M. Laurent. Revisiting two theorems of Curto and Fialkow on moment matrices. *Proc. Amer. Math. Soc.*, 133:2965–2976, 2005.

[Lau07a] M. Laurent. Semidefinite representations for finite varieties. *Math. Program.*, 109:1–26, 2007.

[Lau07b] M. Laurent. Strengthened semidefinite programming bounds for codes. *Math. Program.*, 109:239–261, 2007.

[Lau09] M. Laurent. Sums of squares, moment matrices and optimization over polynomials. In M. Putinar and S. Sullivant, editors, *Emerging Applications of Algebraic Geometry*, volume 149, pages 157–270. IMA Volumes in Mathematics and its Applications, 2009.

[Law76] E. L. Lawler. A note on the complexity of the chromatic number problem. *Inf. Process. Lett.*, 5:66–67, 1976.

[Lov79] L. Lovász. On the Shannon capacity of a graph. *IEEE Trans. Inform. Theory*, 25:1–5, 1979.

[Mar08] M. Marshall. *Positive polynomials and sums of squares.* Mathematical Surveys and Monographs 146. Providence, RI: American Mathematical Society (AMS), 2008.

[Mea92] D. G. Mead. Newton's identities. *Am. Math. Mon.*, 99(8):749–751, 1992.

[Meg87] N. Megiddo. On the complexity of linear programming. in: Advances in economic theory. In T Bewley, editor, *Fifth world congress*, pages 225–268. Cambridge: Cambridge University Press, 1987.

[Mev08] M. Mevissen. Introduction to concepts and advances in polynomial optimization. Tutorial at the ETH Zürich summer school *New Algorithmic Paradigms in Optimization*, 2008.

[Mil64] J. W. Milnor. On the Betti numbers of real varieties. *Proc. Am. Math. Soc.*, 15:275–280, 1964.

[Mit10] H. Mittelmann. Private communication, 2010.

[MRR78] R. J. McEliece, E. R. Rodemich, and H. C. jun. Rumsey. The Lovász bound and some generalizations. *J. Comb. Inf. Syst. Sci.*, 3:134–152, 1978.

[MS85] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes. Parts I, II. (3rd repr.).* North-Holland Mathematical Library, Vol. 16. Amsterdam: North- Holland (Elsevier), 1985.

[Mus93] C. Musili. *Representations of finite groups.* Texts and Readings in Mathematics. New Delhi: Hindustan Book Agency, 1993.

[Obr63] N. Obreschkoff. *Verteilung und Berechnung der Nullstellen reeller Polynome.* Hochschulbücher für Mathematik. 55. Berlin: VEB Deutscher Verlag der Wissenschaften, 1963.

[OW84] L. H. Ozarow and A. D. Wyner. Wire tap channel ii. *Bell System Technical Journal*, 63:2135–2157, 1984.

[Par03] P. Parrilo. Semidefinite programming relaxations for semialgebraic problems. *Math. Program.*, 96:293–320, 2003.

[PD01] A. Prestel and C. N. Delzell. *Positive polynomials. From Hilbert's 17th problem to real algebra.* Springer Monographs in Mathematics. Berlin: Springer., 2001.

[Pro78] C. Procesi. Positive symmetric functions. *Adv. Math.*, 29:219–225, 1978.

[PRSS04] V. Powers, B. Reznick, C. Scheiderer, and F. Sottile. A new approach to Hilbert's theorem on ternary quartics. *C. R., Math., Acad. Sci. Paris*, 339(9):617–620, 2004.

[PS14] G. Pólya and I. Schur. Über zwei Arten von Faktorenfolgen in der Theorie der algebraischen Gleichungen. *J. für Math.*, 144:89–113, 1914.

[PS85] C. Procesi and G. Schwarz. Inequalities defining orbit spaces. *Invent. Math.*, 81:539–554, 1985.

[PS98] G. Pólya and G. Szegő. *Problems and theorems in analysis II. Theory of functions, zeros, polynomials, determinants, number theory, geometry. Transl. from the German by C. E. Billigheimer. Reprint of the 1976 English translation.* Classics in Mathematics. Berlin: Springer, 1998.

[PS10] A. Pfister and C. Scheiderer. An elementary proof of Hilbert's theorem on ternary quartics. *preprint*, 2010.

[Put93] M. Putinar. Positive polynomials on compact semi-algebraic sets. *Indiana Univ. Math. J.*, 42:969–984, 1993.

[PW98] V. Powers and T. Wörmann. An algorithm for sums of squares of real polynomials. *J. Pure Appl. Algebra*, 127(1):99–104, 1998.

[Raj93] A. R. Rajwade. *Squares.* London Mathematical Society Lecture Note Series. 171. Cambridge: Cambridge University Press, 1993.

[Rie10] C. Riener. On the degree and half degree principle for symmetric polynomials. *to appear in J. Pure Appl. Algebra, arXiv:1001.4464*, 2010.

[Ros09] P. Rostalski. *Algebraic Moments - Real Root Finding and Related Topics.* PhD thesis, ETH Zürich, 2009.

[Roy00] M.-F. Roy. The role of Hilbert problems in real algebraic geometry. Camina, Rachel (ed.) et al., European women in mathematics. Proceedings of the 9th general meeting (EWM'99), Loccum, Germany, August 30 - September 4, 1999. Stony Brook, NY: Hindawi Publishing Corporation, 2000.

[RS02] Q. I. Rahman and G. Schmeisser. *Analytic theory of polynomials.* London Mathematical Society Monographs. New Series 26. Oxford: Oxford University Press, 2002.

[RT08] C. Riener and T. Theobald. Positive Polynome und semidefinite Optimierung [Positive polynomials and semidefinite programming]. *Jahresber. Dtsch. Math.-Ver.*, 110, No. 2:57–76, 2008.

[Sag01] B. Sagan. *The Symmetric Group.* Graduate Texts in Mathematics. 203. New York: Springer, 2001.

[Sch79] A. Schrijver. A comparaison of the Delsarte and Lovász bound. *IEEE Trans. Inform. Theory*, 25:425–429, 1979.

[Sch91] K. Schmüdgen. The K-moment problem for compactsemi-algebraic sets. *Math. Ann.*, 289:203–206, 1991.

[Sch05a] A. Schrijver. New code upper bounds from the Terwilliger algebra and semidefinite programming. *IEEE Trans. Inform. Theory*, 51:2859–2866, 2005.

[Sch05b] M. Schweighofer. Optimization of polynomials on compact semialgebraic sets. *SIAM J. Optim.*, 15:805–825, 2005.

[Sch10] C. Scheiderer. Hilbert's theorem on positive ternary quartics: a refined analysis. *J. Algebr. Geom.*, 19(2):285–333, 2010.

[Ser01] J.-P. Serre. *Linear Representations of Finite Groups.* Graduate Texts in Mathematics. 42. New York: Springer, 2001.

[Sho87] N. Z. Shor. Class of global minimum bounds of polynomial functions. *Cybernetics*, 23(6):731–734, 1987.

[Spe37] W. Specht. Zur Darstellungstheorie der symmetrischen Gruppe. *Math. Z.*, 42:774–779, 1937.

[Sta79] R. P. Stanley. Invariants of finite groups and their applications to combinatorics. *Bulletin Am. Math. Soc.*, pages 475–511, 1979.

[Ste73] G. Stengle. A Nullstellensatz and a Positivstellensatz in semialgebraic geometry. *Math. Ann.*, 207:87–97, 1973.

[Stu93] B. Sturmfels. *Algorithms in invariant theory.* Texts and Monographs in Symbolic Computation. Wien: Springer, 1993.

[Stu98] J. F. Sturm. Using sedumi 1.02, a matlab toolbox for optimization over symmetric cones. *Optimization Methods and Software*, 11–12:625–653, 1998.

[Syl53] J. Sylvester. On a theory of the syzygetic relations of two rational integral functions, comprising an application to the theory of sturm's functions, and that of the greatest algebraical common measure. *Phil. Trans. Royal Soc. London*, 143:407–548, 1853.

[Ter40] O. Terquem. Démonstration de deux propositions de M. Cauchy. *J. Math. Pures Appl. (Liouville)*, 5, 1840.

[Tim03] V. Timofte. On the positivity of symmetric polynomial functions. part i: General results. *J. Math. Anal. Appl.*, 284:174–190, 2003.

[Val08] F. Vallentin. Symmetry in semidefinite programs. *Linear Algebra Appl.*, 430:360–369, 2008.

[Wey39] H. Weyl. *The classical groups, their invariants and representations.* Princeton: Princeton University Press, 1939.

[Wey52] H. Weyl. *Symmetry.* Princeton: Princeton University Press, 1952.

SDG

Cordian B. Riener

Curriculum Vitæ

Luginslandweg 6
88299 Leutkirch

Personal Information

Date of Birth	April 9th, 1981
Place of Birth	Memmingen, Germany
Nationalities	austrian, german

Education

2007–2011	**Ph.D. in Mathematics**, *Goethe-Universität*, Frankfurt.
Title of Ph.D. thesis	Symmetries in Semidefinite and Polynomial Optimization – Relaxations, Combinatorics, and the Degree Principle –
Ph.D. advisor	Prof. Dr. T. Theobald
Graduation	2011
2006	**PreDoc-Course "Optimization Methods in Discrete Geometry"**, *TU Berlin*.
2004–2005	**Master Mathématiques**, *Université de Bordeaux 1*.
Title of Master thesis	*Réseaux extremes*
supervisor	Prof. Dr. C. Bachoc
2000–2006	**Diplom Economical Mathematics**, *Universität Ulm*.
Title of Diploma thesis	*Extreme Gitter*
supervisors	Prof. Dr. G. Nebe and Prof. Dr. W. Lütkebohmert
2002–2007	**Bachelor of Arts in Philosophy**, *Universität Ulm*.
Title of Bachelor thesis	*Der Geist des Kapitalismus aus wirtschaftsethischer Sicht*
supervisor	PD. Dr. J. Wernecke

Scholarships

2009 **DAAD Scholarship for a research project at Université de Bordeaux 1**.

2006 **Scholarship for a PreDoc Course at TU Berlin**.

2002-2005 **Scholarship of the Konrad-Adenauer-Foundation**.

Experience

since 04/2011 **PostDoc**, *Zukunftskolleg*, Universität Konstanz.

01/2007–03/2011 **Research assistant**, *Goethe-Universität*, Frankfurt.

08/2007 **Teaching assistant**, *IMA Summer program on Applicable Algebraic Geometry*.

10/2005–12/2005 **Internship**, *West LB Mellon AM*, Düsseldorf.
Portfolio Optimization

10/2003–07/2004 **Mathematics tutor**, *Universität Ulm*.
Tutoring for maths courses for engineers

10/2001–07/2003 **Computer science tutor**, *Universität Ulm*.
Supervision of practical sessions for the introduction courses in computer sciences

Teaching

Fall 10/11 Exercises for "Kombinatorische Optimierung"

Spring 10 Seminar "Advanced discrete and computational mathematics" (with T. Theobald)

Fall 09/10 Exercises for "Einführung in die computerorientierte Mathematik"

Spring 09 Exercises for "Diskrete Mathematik"

Fall 08/09 Seminar "Diskrete Mathematik" (with T. Theobald)

Spring 08 Seminar "Ausgewählte Kapitel der Philosophie der Mathematik" (with W. Essler and T. de Wolff)

Spring 08 Exercises for "Kombinatorische Optimierung"

Fall 07/08 Seminar "Diskrete Mathematik" (with T. Theobald)

Spring 07 Exercises for "Diskrete Mathematik"

Supervised Bachelor Theses

2009 **Sadik Iliman**, *Der Satz von Pólya*.

2009 **Elzbieta Lescevska**, *Semidefinite Schranken für Codes*.

Research interests

Optimization SDP-relaxations, polynomial optimization, symmetries in optimization

Discrete geometry Sphere packing, lattices, t-designs

Invited Conferences and workshops

2010 **Core member of special semester**, *Modern Trends in Optimization and Its Application*, IPAM, University of California, Los Angeles.

2009 **Oberwolfach Seminar**, *New trends in algorithms for real algebraic geometry*.

2008 **Hausdorff Center**, *Extreme Geometric Structures*.

2007 **Oberwolfach Workshop**, *Tropical Geometry*.

2005 **Oberwolfach Seminar**, *Sphere Packings: Exceptional Geometric Structures and Connections to other Fields*.

2005 **Oberwolfach Workshop**, *Gitter und Anwendungen*.

Selected talks

2010 **Symmetric sums of squares in degree four**, *Universität Konstanz*.

2010 **Optimizing with Symmetric Polynomials**, *IPAM, UC Los Angeles*.

2010 **Positive Symmetric Polynomials**, *Universität Konstanz*.

2010 **Positive Symmetric Polynomials**, *UC Berkeley*.

2008 **Landkarten, Postboten, Sudokus: Mathematik mit dem diskreten Blick**, *Tag der Naturwissenschaften Goethe-Universität Frankfurt*.

2007 **SDPs und polynomiale Optimierung**, *RWTH Aachen*.

2007 **Extreme Gitter**, *Goethe-Universität Frankfurt*.

2005 **L'optimisation linéaire dans la théorie des réseaux**, *A2X Bordeaux*.

Activities in university committees

since 2009 **Fachbereichsrat**, *FB Mathematik und Informatik*, Goethe-Universität.

since 2008 **Direktoriumsmitglied**, *Institut für Mathematk*, Goethe-Universität.

2002–2004 **StuVe**, *Student's parliament*, Universität Ulm.

Languages

German **Native**

English **Very good**

French **Very good**

Hungarian **Elementary**

Hebrew **Elementary**

Computer skills

OS Linux, Windows

programming JAVA, C/C++, Pascal

scientific Matlab, Maple, Magma, Singular

Publications

Appeared

[1] Positive Polynome und semidefinite Optimierung. In: *Jahresbericht der DMV* 110 (2008), p. 57–76 (with T. Theobald)

[2] On extreme forms in dimension 8. In: *Journal de Théorie des Nombres de Bordeaux* 18 (2006), p. 677–682
`http://jtnb.cedram.org/item?id=JTNB_2006__18_3_677_0`

Preprints

[1] *Exploiting Symmetries in SDP-relaxations for polynomial optimization*
(with L. Jansson, J.B. Lasserre, and T. Theobald)
`arXiv:1103.0486`

[2] *On the degree and half degree principle for symmetric polynomials*
submitted to Journal of Pure and Applied Algebra `arXiv:1001.4464`

[3] *A note on extrema of linear combinations of elementary symmetric functions*
(with S. Kuhlmann and A. Kovačec)
to appear in Linear and Multilinear Algebra

In preparation

[1] *SDP bounds for generalized Hamming distances*.
(with C. Bachoc)

[2] *Positive symmetric polynomials of degree 4*.
(with. G. Blekherman)