# Size bounds for algebraic and semialgebraic proof systems

Thesis, PhD in Computing

Tuomas Hakoniemi
Universitat Politècnica de Catalunya

**Abstract**

This thesis concerns the proof complexity of algebraic and semi-algebraic proof systems Polynomial Calculus, Sums-of-Squares and Sherali-Adams.

The most studied complexity measure for these systems is the degree of the proofs. This thesis concentrates on other possible complexity measures of interest to proof complexity, monomial-size and bit-complexity. We aim to showcase that there is a reasonably well-behaved theory for these measures also.

Firstly we tie the complexity measures of degree and monomial size together by proving a size-degree trade-off for Sums-of-Squares and Sherali-Adams. We show that if there is a refutation with at most $s$ many monomials, then there is a refutation of degree $O(\sqrt{n \log s} + k)$, where $k$ is the maximum degree of the constraints and $n$ is the number of variables. For Polynomial Calculus similar trade-off was obtained in [46].

Secondly we prove a feasible interpolation property for all three systems. We show that for each system there is a polynomial time algorithm that given two sets $Q_1(x, z)$ and $Q_2(y, z)$ of polynomial constraints in disjoint sequences $x, y$ and $z$ of variables, a refutation of $Q_1(x, z) \cup Q_2(y, z)$ and an assignment $a$ to the variables $z$, finds either a refutation of $Q_1(x, a)$ or a refutation of $Q_2(y, a)$.

Finally we consider the relation between monomial-size and bit-complexity in Polynomial Calculus and Sums-of-Squares. We show that there is an unsatisfiable set of polynomial constraints that has both Polynomial Calculus and Sums-of-Squares refutations of polynomial monomial-size, but for which any Polynomial Calculus or Sums-of-Squares refutation requires exponential bit-complexity.

Besides the emphasis on complexity measures other than degree, another unifying theme in all the three results is the use of semantic characterizations of resource-bounded proofs and refutations. All results make heavy use of the completeness properties of such characterizations. All in all, the work on these semantic characterizations presents itself as the fourth central contribution of this thesis.

Aamulle ja Ailille

# Acknowledgements

I'm grateful to my advisor Albert Atserias for his guidance during my doctoral studies. Albert has introduced me to proof complexity and led me towards many interesting problems, some of which have by-products in this thesis.

I want to also thank other members of the AUTAR research project I had the opportunity to discuss and share ideas with: Ilario Bonacina, Michal Garlík, Massimo Lauria, Moritz Müller and Joanna Ochremiak.

Thank you to my fellow PhD students I had the pleasure to get to know during these years: Lucas Machado, Alberto Moreno, Josep Sànchez and Alex Vidal.

Thank you to Juha Kontinen for hosting my visit at the University of Helsinki during the academic year 2019-2020, and to Jonne Iso-Tuisku for all the discussions shared over many cups of coffee.

Last but definitely not least, I want to thank Elina for all the support and encouragement, and for enduring with me our life between different corners of Europe.

The work in this thesis was partially funded by European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme, grant agreement ERC-2014-CoG 648276 (AUTAR) and MICCIN grant TIN2016-76573-C2-1P (TASSAT3).

# Contents

# Chapter 1

# Introduction

Proof theory is a branch of mathematical logic whose objects of study are formal theories and proofs in formal proof calculi. Though the notion of logical calculus can be seen already in Leibniz's *Calculus ratiocinator*, proof theory grew to fruition out of Hilbert's formalist agenda to give finitary foundations for the whole of mathematics. Even if Hilbert's program failed in its most general form, it definitely left a mark on mathematical logic in general, and proof theory in particular.

With the clear understanding of proofs as finite combinatorial objects – strings of symbols from some vocabulary – comes naturally a question about the sizes of such objects. This leads us to propositional proof complexity, which studies the sizes of proofs in different proof calculi for propositional logic(s). The question is certainly interesting by itself, but a stronger motivation for propositional proof complexity comes from the seminal work of Cook and Reckhow [23] that connects propositional proof complexity to major open questions in computational complexity theory.

## 1.1 Propositional proof complexity

In [23] Cook and Reckhow presented a general definition of a propositional proof system as a poly-time computable function onto the set of tautologies. With this definition they made the simple but foundational observation that

there is no propositional proof system for classical propositional logic that has short, i.e. polynomial-sized, proofs for all tautologies unless NP is closed under complementation. The converse implication holds also.

Cook and Reckhow introduced also machinery to compare the relative strengths of different proof systems via so-called p-simulations. A p-simulation is a polynomial-time function that transforms proofs in one system to proofs in another. The existence of such function shows that the proofs in the former system cannot be considerably shorter than in the latter. The main line of research in propositional proof complexity has ever since concerned itself in proving lower bounds for stronger and stronger proof systems in the above definite sense.

Some proof systems for propositional logic familiar for many include Resolution, Hilbert- and Gentzen-style calculi and Natural Deduction. For Resolution we know of many strong lower bounds going back all the way to Tseitin's lower bound for a subsystem of Resolution called Regular Resolution in 1968 [90] and Haken's lower bound for general Resolution in 1985 [43]. The other mentioned systems turn out to be equivalent in their strength [23]. They are jointly called Frege systems as a homage to Frege's Begriffsschrift. Proving superpolynomial lower bounds for Frege systems is a major open question in propositional proof complexity.

## 1.2 (Semi-)algebraic proof systems

Besides logic, different proof calculi can be found also in other parts of mathematics. In this thesis we study calculi arising from algebra and combinatorial optimization that are used to prove the unsatisfiability of a set of polynomial equality and/or inequality constraints. We still retain the point of view of propositional proof complexity, and study these systems as refutation systems for polynomial constraints over Boolean values 0 and 1. We study the algebraic proof system Polynomial Calculus (PC) and the semi-algebraic proof systems Sums-of-Squares (SOS) and Sherali-Adams (SA).

Polynomial Calculus is a proof system based on local inference rules whose correctness is ultimately based on Hilbert's Nullstellensatz. It was introduced by Clegg, Edmonds and Impagliazzo in [22] under the name Gröbner basis proofs. In defining the proof system they drew inspiration from Gröbner basis calculations in computational algebraic geometry, and gave a proof search method for Polynomial Calculus proofs reminiscent of the Buchberger's algorithm for finding a Gröbner basis for a given polynomial ideal. In the Boolean realm Polynomial Calculus was further strengthened to a system called Polynomial Calculus Resolution (PCR) in [1].

Sums-of-Squares on the other hand has its roots in semialgebraic geometry. Central results in semialgebraic geometry are the different forms of Positiv- and Nichtnegativstellensätze, which give necessary and sufficient conditions for the positivity or non-negativity of polynomials on semialgebraic sets, i.e. subsets of the Euclidean space defined by polynomial inequalities and equalities. See [83] for a survey on the different forms of Positiv- and Nichnegativstellensätze.

Based on the most general form of Positivstellensatz by Krivine [57] and Stengle [88], Grigoriev and Vorobjov [40] defined the Positivstellensatz proof system and initiated the study of its proof complexity. Sums-of-Squares proof system on the other hand is based on Putinar's Positivstellensatz [77], which gives a very clean representation of a polynomial positive on a semialgebraic set under an additional technical assumption that holds for semialgebraic sets defined by polynomials over Boolean variables.

Beginning with [9], Sums-of-Squares has amassed considerable amount of attention due to its connections with approximation algorithms and computational complexity through hierarchies of SDP relaxations of combinatorial problems [59, 68, 67, 21, 31, 63, 62]. We refer the reader to [67] and [60] for discussion on these connections.

If Sums-of-Squares has close connection with hierarchies of SDP relaxations, Sherali-Adams proofs arise from the hierarchy of LP relaxations of Sherali and Adams [85], and so Sherali-Adams forms a subsystem of Sums-of-Squares. As a proof system for propositional logic Sherali-Adams was first studied in [26].

## 1.3 Contributions and related work

This thesis has two unifying themes running along the length of the thesis. Firstly, the thesis concentrates on size bounds for the three systems discussed above instead of the most studied complexity measure for the three systems – the degree of the refutations. The second unifying theme is in the techniques we employ to prove our results. We use different semantic characterizations of resource-bounded proofs and refutations to prove the majority of the results below. We rely especially on the completeness properties of such characterizations, when most work in proof complexity employs only the soundness properties of such characterizations. We also introduce novel semantic characterizations tailored directly for size bounds, instead of degree, for the three systems considered.

### 1.3.1 Complexity measures

The most studied complexity measure for all three systems is the degree of a proof. This is of course a very natural complexity measure for proof systems based on polynomials. But for Sums-of-Squares and Sherali-Adams, more importantly, the systems bounded by degree are in one-to-one correspondence with the levels of the Lasserre and Sherali-Adams hierarchies, respectively. Hence the degree upper and lower bounds give immediate algorithmic information about feasibility and infeasibility of combinatorial problems.

In part, the emphasis on degree bounds is also due to the existence of simple proof search algorithms for bounded degree proofs. For Polynomial Calculus proof search can be carried out by an algorithm reminiscent of the Buchberger's algorithm used in Gröbner basis computations, and for Sherali-Adams and Sums-of-Squares proof search for a degree $d$ proof is a linear or semidefinite programming problem of size $n^{O(d)}$. The proof search methods produce always proofs with $n^{O(d)}$ monomials, and unless the coefficients grow too large the algorithms actually find the proofs (up to small additive error in case of SOS) in time $n^{O(d)}$. For Polynomial Calculus over

finite fields and for Sherali-Adams large coefficients do not cause any problems – the systems are degree-automatable – but for Polynomial Calculus over infinite fields and for Sums-of-Squares large coefficients can cause serious problems for the proof search procedures, as is exemplified also in the Chapter 6 of this thesis.

First linear degree lower bounds for Polynomial Calculus were proved by Razborov in [81] for (a version of) the Pigeonhole Principle. The paper also introduced the use of reduction operators to prove degree lower bounds in Polynomial Calculus. This approach has been applied and further developed in many subsequent papers (see e.g. [2, 34, 30, 65]). Another approach based on binomial ideals for degree lower bounds for Polynomial Calculus was used in [20] to prove lower bounds for Tseitin formulas and mod $p$ counting formulas. The work builds on earlier bounds for Nullstellensatz using similar machinary [35]. This approach was used also in [13] to prove degree lower bounds for random CNF's.

Grigoriev proved the first degree lower bounds for Sums-of-Squares in [37] and [36]. The former extended the machinary introduced in [35, 20] to Sums-of-Squares to give lower bounds on Tseitin and parity formulas, while the latter introduced the use of the so-called pseudoexpectations to argue against low degree proofs in Sums-of-Squares. Pseudoexpectations were used, though implicitly, by Schoenebeck in [84] to give linear degree lower bounds for random $k$-CNFs in Sums-of-Squares. The term 'pseudoexpectation' appears only later in [9], where many useful properties of pseudoexpectations were also obtained. We refer the reader to the survey [10] for further discussion on the role and use of pseudoexpectations.

As Sherali-Adams is a subsystem of Sums-of-Squares all the lower bounds mentioned above hold for it also. An important example separating Sherali-Adams from Sums-of-Squares in terms of degree is the Pigeonhole Principle: while there is a constant degree Sums-of-Squares refutation of the Pigeonhole Principle [38], Sherali-Adams requires degree $\Omega(n)$ to refute the Pigeonhole Principle with $n+1$ pigeons and $n$ holes [25].

As stated above, this thesis concentrates on other possible complexity measures that are of interest especially to proof complexity. We consider

the monomial-size of the systems, i.e. the number of monomials in a proof or refutation, and the bit-complexity of the proofs, i.e. the number of bits it actually takes to write down the proofs.

Lower bounds on these size measures are already known for all three systems: one can transform degree lower bounds into lower bounds on the number of monomials by using random restrictions (see [38] for an example of such argument for Sums-of-Squares). Note, however, that such arguments work only when the Boolean values are represented as 0 and 1 as the method of random restrictions relies on a step, where one discards a large number of monomials by mapping them to 0 by some partial assignment. Such attack does not work, when the Boolean values are represented in the Fourier basis with values $\pm 1$. This is in contrast to degree bounds, where one can translate between the two representations with no loss in the degree. Recently Sokolov proved the first strong size lower bounds for Polynomial Calculus and Sums-of-Squares in the $\pm 1$ basis [87]. Note that, by definition, Sherali-Adams system does not make sense in the Fourier basis.

On the other side of things, [8, 61] studied the question whether the $n^{O(d)}$ upper bound on the number of monomials for degree $d$ refutations is the best one can hope for. It was shown that this upper bound is essentially optimal. They constructed for each system examples of CNFs that have degree $d$ refutations, but require $n^{\Omega(d)}$ many monomials to refute.

### 1.3.2 Semantics for resource-bounded proofs and refutations

A second unifying theme in this thesis is the use of semantic arguments to prove the existence or non-existence of resource-bounded proofs or refutations. We aim to showcase that there is a nicely behaved mathematical theory to reason about size bounds directly using tools reappropriated and redefined from the tools traditionally used to prove degree bounds.

A typical way to prove lower bounds in proof complexity is to exhibit a mathematical object whose existence rules out the existence of resource-bounded proofs or refutations. From the point of view of mathematical

logic such objects can be seen as sound semantics for the associated classes of proofs or refutations. More often than not such objects do in fact characterize the associated classes of proofs or refutations, and thus provide us with semantics that is both sound and complete. These include the previously mentioned reduction operators for Polynomial Calculus and pseudoexpectations for Sums-of-Squares, but also d-designs for Nullstellensatz [11, 22, 19], the local and partial Boolean valuations for Extended Frege systems [74, 53, 52], and the game theoretic characterization for Resolution width from [5].

In this thesis we further develop the theory around reduction operators for Polynomial Calculus and pseudoexpectations for Sums-of-Squares and Sherali-Adams. We define variations on the degree bounded versions of these operators that can be used to reason about size bounds directly, and prove the associated soundness and completeness lemmas. Most of our later contributions in this thesis rely especially on the completeness lemmas: we argue for the existence of resource-bounded proofs and refutations from the non-existence of suitable semantic objects, and for the existence of the semantic objects from the non-existence of resource-bounded proofs or refutations.

### 1.3.3 Size-degree trade-offs

We have already noted that one can obtain size lower bounds for the systems using random restrictions. For Polynomial Calculus there is also a more uniform way to translate degree lower bounds into monomial-size lower bounds via the size-degree trade-off of [46].

Our first contribution is proving analoguous results for both Sums-of-Squares and Sherali-Adams. These results show how to transform any refutation with small number of (distinct) monomials into a proof with relatively small degree. Similar results have been also proved between size and width in Resolution [14] and between size and rank in tree-like LS and $\mathrm{LS}_+$ [70].

In more detail we prove that if there is an SOS/SA refutation of a set $Q$ of polynomial constraints of monomial-size $s$, then there is an SOS/SA

refutation of $Q$ of degree of order $\sqrt{n \log s} + k$, where $n$ is the number of variables, and $k$ is the degree of the given constraints $Q$. This gives us a criterion for monomial-size lower bounds from degree lower bounds.

The size-degree trade-offs rely on a zero-gap duality theorem between pseudoexpectation values and provable lower bounds. This was already established in [48], but we present here another proof. Our proof allows us to also prove a small variation on the duality theorem that we actually use in the proofs of the trade-off results.

These results are based on the following paper.

[A] Albert Atserias and Tuomas Hakoniemi. Size-Degree Trade-Offs for Sums-of-Squares and Positivstellensatz Proofs. In Amir Shpilka, editor, *34th Computational Complexity Conference (CCC 2019)*, volume 137 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 24:1–24:20, Dagstuhl, Germany, 2019. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

### 1.3.4 Feasible interpolation

Our second contribution is proving a form of feasible interpolation for the three systems considered here. Feasible interpolation is a framework introduced by Krajíček in [55] and [56] for reducing lower bounds in proof complexity to lower bounds in other computational models. The general idea behind feasible interpolation is to somehow feasibly extract from a refutation an algorithm computing some associated problem, and to use known lower bounds on the computation model to derive lower bounds for the proof system.

The basic form of feasible interpolation takes a refutation of a formula of the form $\varphi(x, z) \wedge \psi(y, z)$ with disjoint sequences $x, y$ and $z$ of variables, and feasibly extracts from it an algorithm computing an interpolant of the formula, i.e. a function that given an assignment $a$ to the $z$-variables outputs 0 only if $\varphi(x, a)$ is unsatisfiable and 1 only if $\psi(y, a)$ is unsatisfiable. Different variations of this basic form depend on the exact notion of feasibility

at hand. The general framework allows also reductions to computational problems different than computing the interpolant – as is done in [33, 45].

The framework was originally used in [56] to prove lower bounds for Resolution from lower bounds on monotone Boolean circuits from [80, 3]. The paper did this by showing that when the given CNF satisfies certain monotonicity conditions, there is a monotone interpolant that can be computed by a monotone Boolean circuit whose size is polynomial in the size of a given refutation.

Another proof system for which the framework has been very succesfully applied is Cutting Planes. Pudlák proved in [76] lower bounds on Cutting Planes refutations showing that given a suitable CNF satifying some monotonicity conditions there is a monotone interpolant that can be computed by a monotone real circuit of size polynomial in the length of the given Cutting Planes refutation. Later [33] and [45] showed independently and concurrently that one can use the general framework to prove lower bounds for random $O(\log n)$-CNFs.

A form of monotone feasible interpolation can also be used to derive degree lower bounds for Nullstellensatz refutation via a reduction to monotone span programs [75]. It has also been shown that Lovász-Schrijver proof system enjoys the feasible interpolation property [72, 27] with respect to polynomial-time computability, and the monotone feasible interpolation property with respect to monotone linear programming circuits [28] – a strong model of monotone computation introduced in [28] strictly stronger than monotone Boolean circuits or monotone span programs.

On the negative side Krajíček and Pudlák showed in [54] that Extended Frege cannot admit feasible interpolation with respect to polynomial-sized Boolean circuits unless RSA is not secure against P/poly. This results was later extended to Frege [18] and to bounded depth Frege [16] under other cryptographic assumptions.

We prove feasible interpolation for all three systems in the following form. We show that for each system there is a polynomial-time algorithm that given two sets $Q_1(x, z)$ and $Q_2(y, z)$ of polynomial constraints in disjoint sequences $x, y$ and $z$ of variables, a refutation of $Q_1(x, z) \cup Q_2(y, z)$ and

an assignment $a$ to the $z$-variables, outputs either a refutation of $Q_1(x, a)$ or a refutation of $Q_2(y, a)$. For Polynomial Calculus we prove this claim only for fixed finite fields – there is a different algorithm for distinct fields.

We prove the claim by first proving that either $Q_1(x, a)$ or $Q_2(y, a)$ has a refutation of size roughly equal to the size of the given refutation of $Q_1(x, z) \cup Q_2(y, z)$. This is called the feasible disjunction property of the proof systems following [73]. The proof is highly non-constructive and uses the semantic characterizations of resource-bounded refutations in an essential way. Only after this existence proof we argue that the small refutation can be actually found in time polynomial in the size of the given refutation of $Q_1(x, z) \cup Q_2(y, z)$. The existence proof narrows down the search space for the refutation in a way that allows us to give a polynomial-time search algorithm within that smaller search space.

A weaker form of feasible interpolation for degree-bounded proofs in the three proof systems can be obtained using the proof search algorithms mentioned above by simply searching for a refutation of $P(x, a)$ for an appropriate amount of time, and then outputting 0 if a refutation is found and 1 otherwise. This argument was noted for Polynomial Calculus in [81] and [75], but a similar argument can be made for Sherali-Adams and Sums-of-Squares. Similarly a weak form of feasible interpolation with respect to size bounds can also be proven using the proof search algorithms presented in Chapter 5. Previously also a form of monotone feasible interpolation for degree-bounded Polynomial Calculus with respect to monotone polynomial programs was given in [75]. This model of computation is unfortunately very strong – over finite fields it is as strong as general Boolean circuits [75]. Very recently [32] showed a form of monotone feasible interpolation for Sherali-Adams with respect to a weaker form of monotone linear programming circuits than what was needed for Lovász-Shrijver in [28].

The work on feasible interpolation for Polynomial Calculus and Sums-of-Squares appeared originally in the following work.

[B] Tuomas Hakoniemi. Feasible Interpolation for Polynomial Calculus and Sums-Of-Squares. In Artur Czumaj, Anuj Dawar, and Emanuela

Merelli, editors, *47th International Colloquium on Automata, Languages, and Programming (ICALP 2020)*, volume 168 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 63:1–63:14, Dagstuhl, Germany, 2020. Schloss Dagstuhl–Leibniz-Zentrum für Informatik.

### 1.3.5 Bit-complexity vs. Monomial-size

We consider also the relationship between the two measures, monomial-size and bit-complexity, and prove separations between the measures in Polynomial Calculus over reals or rationals and Sums-of-Squares. In short, we show that there is a system of polynomial equations that has refutations both in Polynomial Calculus and Sums-of-Squares with only small number of monomials, but for which any proof must have exponential bit-complexity. For Sums-of-Squares we show this by proving a trade-off between the number of monomials and the magnitude of coefficients in Sums-of-Squares refutations. For Polynomial Calculus we prove a three-way trade-off between the number of monomials, the size of coefficients and the height of Polynomial Calculus refutations. It is rather easy to see that for Sherali-Adams these two measures do in fact coincide as a search for Sherali-Adams proofs is a linear programming problem (see Section 5.3.1.1).

The question on bit-complexity of Sums-of-Squares was raised originally by O'Donnell [66] in relation to the degree automatability of Sums-of-Squares. O'Donnell noted that the received wisdom, that a degree $d$ Sums-of-Squares proof can be found using the ellipsoid algorithm in time $n^{O(d)}$ if one exists, is not entirely true. Difficulties may arise if the only proofs of degree $d$ contain exceedingly large coefficients as then the initial ellipsoid cannot be chosen small enough to guarantee polynomial runtime.

Building on [66], Raghavendra and Weitz exhibited in [78] (see also Weitz's PhD thesis [91]) an example of a set $Q$ of polynomial constraints over $O(n^2)$ Boolean variables and a polynomial $p$ that has SOS proofs of non-negativity from $Q$ of degree 2, and thus with polynomially many monomials, but for which any SOS proof of non-negativity from $Q$ of degree $O(n)$

must contain a coefficient of doubly exponential magnitude in $n$.

The example of Raghavendra and Weitz leaves open, however, the possibility that there are SOS proofs of non-negativity of $p$ from $Q$ that can be written with only polynomially many monomials, and with coefficients of polynomial bit-complexity. In other words the example leaves open the possibility that there are SOS proofs of non-negativity of $p$ from $Q$ that can be written down with only polynomially many bits. It follows from our result that this is not the case.

Similarly, Polynomial Calculus is often claimed to be degree automatable. This is certainly true when the underlying field is a fixed finite field as then the problem with large coefficients does not occur. When the underlying field is infinite there is however possibility for significant coefficient blow-up. This phenomenon is recognised also in the Gröbner basis literature, but there the emphasis seems to be more on circumventing the problem rather than in proving lower bounds on the magnitude of the coefficients. See [29, 92, 82, 4] for discussion on ways to circumvent the problem in Gröbner basis computations.

Raghavendra and Weitz proved the lower bound on the magnitude of coefficients in Sums-of-Squares proofs of degree $O(n)$ using the linear degree lower bounds for refutations of Knapsack proved in [36], and the linear degree pseudoexpectations for Knapsack it provides. We on the other hand will use lower bounds on the number of monomials in refutations of Knapsack, and a suitable form of pseudoexpectations tailored for bounds on monomial-size.

To prove our claim for Polynomial Calculus we use the fact – proved originally by Berkholz in [15] – that Sums-of-Squares p-simulates Polynomial Calculus over real numbers. We provide a new semantic proof of this result that gives bounds on the coefficients in the Sums-of-Squares simulation in terms of the size of coefficients and the height of the given Polynomial Calculus refutation.

This work is based on the following paper.

[C] Tuomas Hakoniemi. Monomial size vs. Bit-complexity in Sums-

of-Squares and Polynomial Calculus. In *36th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2021, Rome, Italy, June 29 - July 2, 2021*, pages 1–7. IEEE, 2021.

**Note on Sherali-Adams** The papers listed above mention the Sherali-Adams proof system only in passing. In this thesis – even with a danger of repeating ourselves – we include also the details for Sherali-Adams.

## 1.4 Structure of the thesis

Beginning with Chapter 2 we introduce formally the proof systems we consider in this thesis. We also cover some basic facts on convex cones that admit order units.

In Chapter 3 we formulate semantic objects for resource-bounded proofs and refutations in the three proof systems, and prove the corresponding soundness and completeness results for such objects. This chapter contains some known results, some parts from all three papers mentioned above, and some new observations. The soundness and completeness of reduction operators against degree is implicit in [81], but we give the full details. Reduction operators against sets of monomials appeared originally in [B]. The proof of the Duality theorem for SOS comes from [A], and the work on SOS pseudoexpectations against a set of monomials appears in both [B] and [C]. The arguments for SA are modifications of the ones for SOS. Finally, the semantic proof that SOS p-simulates PCR over reals appears in [C].

In Chapter 4, which is based on [A], we prove a size-degree trade-offs for Sums-of-Squares and Sherali-Adams proof systems.

In Chapter 5 we prove a form of feasible interpolation for all three systems we consider here. This chapter is based on [B].

Chapter 6 considers the the relationship between two complexity measures, bit-complexity and the number of monomials, in Sums-of-Squares and Polynomial Calculus refutations. This chapter is based on [C].

Finally in Chapter 7 we consider future directions for research and pose some open problems related to the work presented in this thesis.

# Chapter 2

# Preliminaries

In this chapter we go through some preliminaries for the thesis. First we fix some notation. Then in Section 2.2 we define the so called Boolean ideal – an ideal of the polynomial ring, whose affine variety corresponds to bit-strings. After that, in Section 2.3 we introduce the proof systems we consider in this thesis and provide for each system a proof search algorithm. Finally in Section 2.4 we recall some basic facts about convex cones admitting order units that are used in this thesis.

## 2.1 On notation

We consider polynomials in a finite sequence $x = \langle x_1, \ldots, x_n \rangle$ of commuting variables. We denote by $\mathbb{F}[x]$ the space of all polynomials over the field $\mathbb{F}$ in variables $x$, in particular $\mathbb{R}[x]$ stands for the set of all real polynomials. For a sequence $\alpha = \langle \alpha_1, \ldots, \alpha_n \rangle$ of natural numbers, we denote by $x^\alpha$ the monomial $\prod_{i \in [n]} x_i^{\alpha_i}$. Depending on situation we write polynomials either in the form $\sum_\alpha a_\alpha x^\alpha$ or $\sum_m a_m m$, where first sum ranges over sequences of natural numbers and the second sum ranges over monomials.

For $p \in \mathbb{R}[x]$, we denote by $\|p\|_\infty$ the maximum coefficient in absolute value appearing in $p$.

For any $d \in \mathbb{N}$, we denote by $\mathbb{F}[x]_d$ the set of all polynomials in $\mathbb{F}[x]$ of degree at most $d$. Note that $\mathbb{F}[x]_d$ is a linear subspace of $\mathbb{F}[x]$. However, it

is not closed under polynomial multiplication.

Given any set $S$ of monomials, we write $\mathbb{F}[S]$ for the set of all linear combinations of elements of $S$, i.e. the set of polynomials where only elements of $S$ appear with non-zero coefficient.

Throughout the thesis we employ the notational convention that upper case $P$ stands for a set of inequality constraints $p \geq 0$, and upper case $Q$ stands for a set of equality constraints $q = 0$. We abuse notation and write $p \in P$ and $q \in Q$ for the polynomials $p$ and $q$ such that the constraints $p \geq 0$ and $q = 0$ are in $P$ and $Q$, respectively.

For polynomial $p$ with rational coefficients, we denote by $\langle p \rangle$ the number of bits needed to represent $p$, when all its coefficients are represented with their reduced fractions written in binary. We also extend the notation for sets of polynomials and write $\langle P \rangle$ for the number of bits needed to represent all polynomials in $P$.

## 2.2 The Boolean ideal and multilinear polynomials

Our primary goal is to study the proof systems from the point of view of proof complexity and combinatorial optimization. Naturally, in these contexts the variables take Boolean values, i.e. they assume values 0 or 1. Accordingly, we will mostly work modulo the Boolean ideal – an ideal whose algebraic variety corresponds to bit-strings – which we define next.

We consider polynomials over $n$ pairs of twin variables $x_i, \bar{x}_i$, $i \in [n]$. The intended meaning is that the variables in a pair take the opposite values, i.e. one assumes value 0 and the other value 1. Define the **Boolean ideal** $I_n$ in $n$ pairs of twin variables to be the ideal generated by the following set of polynomials:

$$B_n := \{x_i^2 - x_i, \bar{x}_i^2 - \bar{x}_i, x_i + \bar{x}_i - 1 : i \in [n]\}. \tag{2.1}$$

It is not hard to see that over any field, the affine variety of $I_n$ consists exactly of the $\{0,1\}$-strings of length $2n$ where any of the pairs have opposite

values. As is usual, we write $p \equiv q \mod I_n$, if $p - q \in I_n$

The Boolean axioms form a Gröbner basis for the ideal $I_n$ with respect to any monomial ordering. This can be easily verified using Buchberger's criterion (see e.g. [24]). This implies that the multivariate division of a polynomial $p$ by $B_n$ leaves an unique remainder, and in particular leaves remainder 0, when $p \in I_n$. For our purposes this has an important consequence that we discuss next. For details on Gröbner bases and multivariate division we refer the reader to [24].

For a polynomial $p$ of degree $d$ in $I_n$, there is always a certificate of degree $d$ of the inclusion. That is, if $p \in I_n$ is of degree $d$, there are $u_i$, $v_i$ and $w_i$ for $i \in [n]$ such that $\deg(u_i), \deg(v_i) \leq d-2$, $\deg(w_i) \leq d-1$ and

$$p = \sum_{i \in [n]} \big( u_i(x_i^2 - x_i) + v_i(\bar{x}_i^2 - \bar{x}_i) + w_i(x_i + \bar{x}_i - 1) \big).$$

This is so because the multivariate division of $p$ by $B_n$ never introduces monomials of higher degrees. It is because of this fact, that when we consider degree bounded proofs, we work exclusively modulo the Boolean ideal and disregard the actual lifts of the Boolean axioms.

Besides considering polynomials modulo the Boolean ideal, at times we consider polynomials modulo multilinearization, i.e. modulo the ideal generated by the axioms $x_i^2 - x_i$ and $\bar{x}_i^2 - \bar{x}_i$. We write

$$p \equiv q \mod J_n,$$

when $p$ and $q$ are equivalent modulo multilinearization, i.e. there are $u_i$ and $v_i$ such that

$$p - q = \sum_{i \in [n]} \big( u_i(x_i^2 - x_i) + v_i(\bar{x}_i^2 - \bar{x}_i) \big).$$

## 2.3 Proof systems

In this section we define the proof systems we consider in this thesis. We do also provide for each system a proof search algorithm. The first section 2.3.1 deals with Polynomial Calculus, the second section 2.3.2 with Sums-of-Squares proofs and the final section 2.3.3 with Sherali-Adams proofs.

### 2.3.1 Polynomial Calculus

Let $\mathbb{F}$ be a field and let $Q$ be a set of equality constraints (over $\mathbb{F}$). A **Polynomial Calculus (PC) proof** over a field $\mathbb{F}$ (or a PC/$\mathbb{F}$ proof) of $p = 0$ from $Q$ is a sequence

$$p_1, \ldots, p_\ell \tag{2.2}$$

of polynomials such that $p_\ell = p$ and for each $i \in [\ell]$ one of the following holds:

- $p_i \in Q$; (2.3)
- there is $j < i$ and a variable $x$ such that $p_i = xp_j$; (2.4)
- there are $j, k < i$ and scalar $a, b \in \mathbb{F}$ such that $p_i = ap_j + bp_k$. (2.5)

A **PC/$\mathbb{F}$ refutation** of $Q$ is a PC/$\mathbb{F}$ proof of $1 = 0$ from $Q$.

In (2.4) the polynomial $p_j$ is the **direct antecedent** of $p_i$ and in (2.5) both $p_j$ and $p_k$ are the direct antecedents of $p_i$. The proof (2.2) is of **degree** at most $d$ if the degree of $p_i$ is at most $d$ for all $i \in [\ell]$. The **height** of the proof is the length of the longest subsequence $p_{i_1}, \ldots, p_{i_k}$ such that $p_{i_j}$ is a direct antecedent of $p_{i_{j+1}}$ for each $j < k$. The **monomial size** of the proof (2.2) is the number of monomials appearing in the proof counted with multiplicity.

When $\mathbb{F} = \mathbb{Q}$ define the **bit-complexity** of the proof (2.2) to be the minimum length of a bit-string representing all the polynomials in the proof and all the scalars used in the linear combination rule, when all the coefficients and scalars are represented with their reduced fractions written in binary.

Let $S$ be a set of monomials, and let $\widehat{S} = S \cup xS$, where $xS = \{xm : m \in S \text{ and } x \text{ is a variable}\}$. A **PC/$\mathbb{F}$ proof** of $p$ from $Q$ **over** $S$ is a PC/$\mathbb{F}$ proof of $p$ from $Q$, where only monomials from the set $\widehat{S}$ appear, and the inference step (2.4) is only applied when $p_i$ is in $\mathbb{F}[S]$.

We write $Q \vdash_d^{\mathbb{F}} p = 0$, if there is a PC/$\mathbb{F}$ proof of $p = 0$ from $Q$ of degree at most $d$, and $Q \vdash_S^{\mathbb{F}} p = 0$ if there is a PC/$\mathbb{F}$ proof of $p = 0$ from $Q$ over $S$. If the field $\mathbb{F}$ is clear from the context, we drop the superscript.

The notion of a PC/$\mathbb{F}$ proof over a set of monomials generalizes the notion of a degree bounded PC/$\mathbb{F}$ proof. A PC/$\mathbb{F}$ proof of degree at most $d$ is just a PC/$\mathbb{F}$ proof over the set of all monomials of degree at most $d-1$.

The above definitions did not require the presence of the Boolean axioms. When the Boolean axioms are included in $Q$, i.e. when $B_n \subseteq Q$, the associated proof system is called **Polynomial Calculus Resolution (PCR)**, and we talk about PCR/$\mathbb{F}$ proofs and refutations.

### 2.3.2 Sums-of-Squares Proofs

Let $P$ and $Q$ be two sets of inequality and equality constraints, respectively, over $\mathbb{R}$ in $n$ pairs of twin variables. Let $r$ be a polynomial. A (Boolean) **Sums-of-Squares (SOS) proof** of non-negativity of $r$ from $P$ and $Q$ is a polynomial equality of the form

$$r = \sum_{i\in[k]} r_i^2 + \sum_{p\in P}\sum_{i\in[k_p]} r_{i,p}^2 p + \sum_{q\in Q} t_q q + \sum_{i\in[n]} \big(u_i(x_i^2 - x_i) + v_i(\bar{x}_i^2 - \bar{x}_i) + w_i(x_i + \bar{x}_i - 1)\big) \quad (2.6)$$

where $r_i$ $r_{i,p}$, $t_q$, $u_i$, $v_i$ and $w_i$ are arbitrary polynomials. An SOS refutation of $P$ and $Q$ is a proof of non-negativity of $-1$ from $P$ and $Q$.

We call the polynomials $r_{i,p}^2$ and $t_q$ the **lifts of the non-logical axioms** and the polynomials $u_i$, $v_i$ and $w_i$ the **lifts of the Boolean axioms.**

When the situation permits we write the proof (2.6) either as an equality modulo the Boolean ideal $I_n$, or modulo multilinearization, i.e.

$$r = \sum_{i\in[k]} r_i^2 + \sum_{p\in P}\sum_{i\in[k_p]} r_{i,p}^2 p + \sum_{q\in Q} t_q q \mod I_n$$

or

$$r = \sum_{i\in[k]} r_i^2 + \sum_{p\in P}\sum_{i\in[k_p]} r_{i,p}^2 p + \sum_{q\in Q} t_q q + \sum_{i\in[n]} w_i(x_i + \bar{x}_i - 1) \mod J_n.$$

The **degree** of the proof (2.6) is at most $d$, when $\deg(r_i^2) \le d$ for any $i \in [k]$; $\deg(r_{i,p}^2 p) \le d$ for any $p \in P$ and $i \in [k_p]$; $\deg(t_q q) \le d$ for any $q \in Q$; and $\deg(u_i x_i^2) \le d$, $\deg(v_i \bar{x}_i^2)$ and $\deg(w_i x_i) \le d$ for any $i \in [n]$.

The **explicit monomials** of the proof (2.6) are all the monomials appearing in the polynomials $r$, $r_i$ for any $i \in [k]$, $r_{i,p}$ and $p$ for any $p \in P$ and $i \in [k_p]$, $t_q$ and $q$ for any $q \in Q$ and $u_i$, $v_i$, $x_i^2 - x_i$ and $x_i + \bar{x}_i - 1$ for any $i \in [n]$. In other words, the explicit monomials of a proof are all the monomials visible in an explicit representation of the proof. The **monomial-size** of the proof is the number of explicit monomials in the proof counted with multiplicity.

Finally we identify an important subset of the explicit monomials. In Chapter 4 we prove a lower bound on the size of this set. We call the monomials appearing in the polynomials $r_i$ for all $i \in [k]$, in the polynomials $r_{i,p}$ for all $p \in P$ and $i \in [k_p]$ and $t_q$ for all $q \in Q$ the **significant monomials** of the proof (2.6).

In the case that the polynomials in the proof (2.6) have only rational coefficients, we define the **bit-complexity** of (2.6) as the minimum length of a bit-string representing the proof when the rational coefficients are represented with their reduced fractions written in binary.

Finally we define a notion of an SOS proof that tries to capture proofs that use only monomials from a fixed set of monomials. Given a set $S$ of monomials, we say that the **proof** (2.6) **is over** $S$ if all the monomials in the polynomials $r_i$, $r_{i,p}$, $t_q$ and $w_i$ are among $S$. Note that we do not restrict the lifts of the Boolean axioms $x_i^2 - x_i$ and $\bar{x}_i^2 - \bar{x}_i$. This choice allows us to still work modulo multilinearization, which makes many things easier later in the thesis.

We write $P, Q \vdash_d^{\text{SOS}} r \geq 0$ if there is an SOS proof of non-negativity of $r$ from $P$ and $Q$ of degree $d$, and $P, Q \vdash_S^{\text{SOS}} r \geq 0$ if there is a proof of non-negativity of $r$ from $P$ and $Q$ over $S$.

### 2.3.3 Sherali-Adams Proofs

Let again $P$ and $Q$ be sets of polynomial inequality and equality constraints, respectively, and let $r$ be any polynomial. A **Sherali-Adams (SA) proof**

of non-negativity of $r$ from $P$ and $Q$ is a polynomial equality of the form

$$r = s + \sum_{p \in P} s_p p + \sum_{q \in Q} t_q q + \sum_{i \in [n]} \big( u_i(x_i^2 - x_i) + v_i(\bar{x}_i^2 + \bar{x}_i) + w_i(x_i + \bar{x}_i - 1) \big) \quad (2.7)$$

where $s$ and $s_p$ for any $p \in P$ are polynomials with non-negative coefficients and $t_q$, $u_i$, $v_i$ and $w_i$ are arbitrary polynomials for any $q \in Q$ and $i \in [n]$. An SA refutation of $P$ and $Q$ is a proof of non-negativity of $-1$ from $P$ and $Q$.

We call the polynomials $s_p$ and $t_q$ the **lifts of the non-logical axioms** and the polynomials $u_i$ and $v_i$ the **lifts of the Boolean axioms.**

Similarly as with Sums-of-Squares, when the situation permits we write the proof as an equality modulo the Boolean ideal or an equality modulo multilinearization.

The **degree** of the proof (2.7) is at most $d$, when when $\deg(s) \leq d$; $\deg(s_p p) \leq d$ for any $p \in P$; $\deg(t_q q) \leq d$ for any $q \in Q$; and $\deg(u_i x_i^2) \leq d$, $\deg(v_i \bar{x}_i^2) \leq d$ and $\deg(w_i x_i) \leq d$ for any $i \in [n]$.

The **explicit monomials** in the proof (2.7) are all the monomials appearing in the polynomials $r$, $s$, $s_p$ and $p$ for any $p \in P$; $t_q$ and $q$ for any $q \in Q$; and $u_i$, $v_i$, $w_i$, $x_i^2 - x_i$, $\bar{x}_i^2 - \bar{x}_i$ and $x_i + \bar{x}_i - 1$ for any $i \in [n]$. In other words, the explicit monomials are all the monomials visible in an explicit representation of the proof (2.7). The **monomial size** of a proof is the number of explicit monomials in the proof counted with multiplicity.

The **significant monomials** of the proof (2.7) are the monomials appearing in the polynomials and $s$, $s_p$ for any $p \in P$ and $t_q$ for any $q \in Q$.

In the case that the polynomials in the proof (2.7) have only rational coefficients, we define the **bit-complexity** of (2.7) as the minimum length of a bit-string representing the proof when the rational coefficients are represented with their reduced fractions written in binary.

Given a set $S$ of monomials, we say that the **proof** (2.7) **is over** $S$ if all the monomials in polynomials $s$, $s_p$, $t_q$ and $w_i$ are among $S$.

We write $P, Q \vdash_d^{\text{SA}} p \geq 0$ if there is a proof of non-negativity of $p$ from $P$ and $Q$ of degree at most $d$, and $P, Q \vdash_S^{\text{SA}} p \geq 0$ if there is a proof of non-negativity of $p$ from $P$ and $Q$ over $S$.

## 2.4 Convex cones and order units

Finally in this section we recall some basic facts about convex cones and order units. We prove a general duality theorem for convex cones admitting an order unit. Lastly we use the general duality theorem to prove a separating hyperplane theorem for convex cones admitting an order unit that is also valid in infinite-dimensional vector spaces. For more on order units and ordered vector spaces we refer the reader to [69].

A subset $C$ of a real vector space $V$ is **convex** if for any $v, w \in C$ and any $\lambda \in [0, 1]$, $\lambda v + (1 - \lambda)w \in C$. A **convex cone** is a convex set satisfying the additional property that $av \in C$ for any $v \in C$ and any $a > 0$. The convex cone $C$ is **pointed** if $0 \in C$.

Any convex cone $C$ gives rise to a transitive relation $<_C$ by $v <_C w$ if $w - v \in C$. The relation moreover respects vector addition and multiplication by a positive scalar, i.e. the following hold:

- if $v_1 <_C w_1$ and $v_2 <_C w_2$, then $v_1 + v_2 <_C w_1 + w_2$; (2.8)
- if $v <_C w$, then $av <_C aw$ for any $a > 0$. (2.9)

It follows also that $v <_C w$ implies $aw <_C av$ for any $a < 0$. Note that, by definition, $v \in C$ if and only if $v >_C 0$.

An **order unit** for a convex cone $C$ is an element $e \in V$ such that for any $v \in V$ there is some $a \in \mathbb{R}_+$ such that $ae - v \in C$, i.e. there is some $a \in \mathbb{R}_+$ such that $ae >_C v$. The following lemma collects some of the basic properties of order units.

**Lemma 2.4.1.** *Let $V$ be a vector space and $C \subseteq V$ a convex cone admitting an order unit $e$. Then the following hold:*

- $e \in C$; (2.10)

- *For every* $v \in V$ *and* $a_1, a_2 \in \mathbb{R}$ *with* $a_1 < a_2$, *if* $a_1 e >_C v$, *then* $a_2 e >_C v$. (2.11)
- *For every* $v \in V$ *there is* $a \in \mathbb{R}$ *such that* $ae >_C v >_C -ae$; (2.12)
- *If* $-e \in C$, *then* $C = V$. (2.13)

*Proof.* (2.10): There is some $a \in \mathbb{R}_+$ such that $ae + e \in C$, i.e. $(r+1)e \in C$, and so $e \in C$.

(2.11): Now $a_2 - a_1 > 0$ and so, by (i), $(a_2 - a_1)e \in C$. Thus $(a_2 - a_1)e + a_1 e - v \in C$, i.e. $a_2 e - v \in C$.

(2.12): Let $a_1$ be such that $a_1 e >_C v$ and let $a_2$ be such that $a_2 e >_C -v$, and let $a = \max\{a_1, a_2\}$. Now, by (ii), $ae >_C v$ and $ae >_C -v$, i.e. $v >_C -ae$.

(2.13): Suppose $-e \in C$, let $v \in V$ and let $a > 0$ be such that $ae >_C v$. Now also $-ae \in C$ and so $a \in C$, i.e. $C = V$. □

Fix a vector space $V$ and a convex cone $C$ admitting an order unit $e$. Let $U$ be a subspace of $V$. A linear functional $L\colon U \to \mathbb{R}$ is **positive** if $L(u) \geq 0$ for all $u \in U \cap C$. Equivalently $L$ is positive if it respects the relation $<_C$ in a sense that $v <_C w$ implies $L(v) \leq L(w)$. A positive linear functional $L$ on $V$ is a **state** for $C$ if $L(e) = 1$. We denote the set of all states for $C$ by $\mathscr{S}(C)$.

Suppose $U$ contains the order unit and let $v \in V$. By (2.12) the following two sets are non-empty:

$$\downarrow_U \{v\} = \{u \in U : v >_C u\},$$
$$\uparrow_U \{v\} = \{u' \in U : v <_C u'\}.$$

Now if $u \in \downarrow_U \{v\}$ and $u' \in \uparrow_U \{v\}$, then $u <_C u'$ and thus $L(u) \leq L(u')$ for any positive linear functional $L\colon U \to \mathbb{R}$. Hence for any positive $L\colon U \to \mathbb{R}$ both $d_v^L = \sup\{L(u) : u \in \downarrow_U \{v\}\}$ and $u_v^L = \inf\{L(u) : u \in \uparrow_U \{v\}\}$ are real numbers and $d_v^L \leq u_v^L$.

**Lemma 2.4.2.** *Let* $U$ *be a subspace of* $V$ *containing the order unit* $e$, *and let* $L$ *be a positive linear functional on* $U$. *Then for any* $v \in V \setminus U$ *and for*

*any* $\gamma \in \mathbb{R}$ *satisfying* $d_v^L \leq \gamma \leq u_v^L$ *there is a positive linear functional* $L'$ *that is defined on* $\operatorname{span}(\{v\} \cup U)$ *extending* $L$ *such that* $L'(v) = \gamma$.

*Proof.* Every element of $\operatorname{span}(\{v\} \cup U)$ can be written uniquely in form $av + u$, where $a \in \mathbb{R}$ and $u \in U$. Define $L'$ by

$$L'(av + u) = a\gamma + L(u).$$

It is easy to check that $L'$ is linear map. We show that $L'$ is positive by considering a few cases.

Case $a = 0$. If $av+u \in C$ and $a = 0$, then $u \in C$ and, by the positiveness of $L$, $L'(av + u) = L(u) \geq 0$.

Case $a > 0$. Suppose that $av + u \in C$ and $a > 0$. Then $v + u/a \in C$, i.e. $v >_C -u/a$, and so $L(-u/a)) \leq \gamma$, i.e. $0 \leq a\gamma + L(u)$.

Case $a < 0$. Suppose that $av + u \in C$ and $a < 0$. Then $-a > 0$, and so $-v - u/a \in C$, i.e. $-u/a >_C v$. Hence $\gamma \leq L(-u/a)$, and so $0 \leq a\gamma + L(u)$. □

### 2.4.1 Duality theorem

Now we can prove a general duality theorem for convex cones admitting an order unit. For a more general version of this result, see [69].

**Theorem 2.4.3.** *Let* $V$ *be a real vector space and let* $C$ *be a convex cone admitting an order unit* $e$. *For any* $v \in V$ *it holds that*

$$\sup\{a \in \mathbb{R} : v >_C ae\} = \inf\{E(v) : E \in \mathscr{S}(C)\}.$$

*Moreover, if the set* $\mathscr{S}(C)$ *is non-empty, then there is a state achieving the infimum.*

*Proof.* The inequality from left to right is clear. For the inequality from right to left we distinguish two cases: whether $-e \in C$ or not. If $-e \in C$, then $\mathscr{S}(C) = \emptyset$, since $-1 \not\geq 0$, so $\inf\{E(a) : E \in \mathscr{S}(C)\} = +\infty$. On the other hand $\sup\{a \in \mathbb{R} : v > ae \in C\} = +\infty$ by (2.13), and so the claim follows.

If $-e \notin C$, then the map defined by $L_0(ae) = a$ for all $a \in \mathbb{R}$ is a positive linear functional on $U_0 = \text{span}(\{e\})$. Note that $d_v^{L_0} = \sup\{a \in \mathbb{R} : v >_C ae\}$, and so, to prove the theorem, it suffices to show that there is some state $E$ extending $L_0$ such that $E(v) = d_v^{L_0}$.

If $v \in U_0$, then $L_0(v) = d_v^{L_0}$. On the other hand if $v \notin U_0$, then by Lemma 2.4.2, there is a positive linear functional $L'$ extending $L_0$ on $\text{span}(\{e, v\})$ such that $L'(v) = d_v^{L_0}$. Now consider the set $\mathscr{A}$ of all positive linear functionals $L$ that are defined on a subspace $U \subseteq V$ containing both $e$ and $v$, and satisfy $L(e) = 1$ and $L(v) = d_v^{L_0}$. By the argument above $\mathscr{A} \neq \emptyset$. On the other hand $\mathscr{A}$ is closed under unions of chains and so, by Zorn's lemma, there is some maximal $E \in \mathscr{A}$.

Now the domain of $E$ is the whole of $V$, since otherwise we could extend $E$ by using Lemma 2.4.2, contradicting the maximality of $E$. Hence $E$ is the state we are looking for. □

As an application of the above general theorem we prove a hyperplane separation theorem between convex cones admitting an order unit and convex sets. Note that the theorem below holds also for infinite dimensional vector spaces. For infinite dimensional vector spaces the assumption on the existence of an order unit is necessary as otherwise there are examples of disjoint convex cones and sets with no non-trivial separating hyperplanes.

**Lemma 2.4.4.** *Let $V$ be a real vector space, let $C_1$ be a convex cone that admits an order unit $e$ and let $C_2$ be a convex set disjoint from $C_1$. Then there is a linear functional $L\colon V \to \mathbb{R}$ such that $L(e) = 1$, $L(v) \geq 0$ for all $v \in C_1$ and $L(u) \leq 0$ for all $u \in C_2$.*

*Proof.* Let $D$ be the convex cone of all elements of the form $v - au$, where $v \in C_1$, $u \in C_2$ and $a \in \mathbb{R}_+$. Now $0 \notin D$, since $C_1$ and $C_2$ are disjoint. Note also that $e$ is also an order unit for $D$, and so $-e \notin D$. It follows that $\mathscr{S}(D) \neq \emptyset$. Hence there is some $E\colon V \to \mathbb{R}$ such that $E(e) = 1$ and $E(v) \geq E(au)$ for any $v \in C_1$, $u \in C_2$ and $a \in \mathbb{R}_+$. In particular $E(v) \geq 0$ for any $v \in C_1$. On the other hand, since $\varepsilon e \in C_1$ for any $\varepsilon > 0$, we have that $E(u) \leq 0$ for any $u \in C_2$. □

# Chapter 3

# Semantics for resource-bounded proofs and refutations

This chapter is dedicated to semantics for resource-bounded proofs and refutations. Here semantics is understood in the lax sense familiar from mathematical logic as any mathematical object, not inherently syntactic in nature, characterizing a class of purely syntactic objects. The intended application of these objects is of course to simplify proofs of syntactic statements by removing us from combinatorial considerations.

A typical way to prove lower bounds in proof complexity is to exhibit a mathematical object that in a sense fools proofs or refutations with only limited resources to think that the given unsatisfiable set of formulas is actually satisfiable. From the point of view of mathematical logic, such objects give sound semantics for resource-bounded proofs or refutations. More often than not, such objects can actually be used to characterize the resource-bounded classes of proofs and refutations, and thus they give sound and complete semantics for the associated classes.

We feel a need to point out immediately that the semantic objects considered below, and in the rest of this thesis, have appeared previously in the literature, and are not usually conceptualized as we do here, as semantics

for resource-bounded proofs and refutations. However for the applications we have in mind, that are of somewhat metalogical in nature themselves, it is natural to conceptualize these objects from a logical point of view.

We present in this chapter semantic counterparts of resource-bounded PC, SOS and SA proofs, and prove that they do in fact characterize suitable classes of proofs or refutations, by proving the associated soundness and completeness properties of these semantic characterizations. First in Section 3.1 we consider reduction operators for Polynomial Calculus. In Sections 3.2 and 3.3 we consider pseudoexpectations for Sums-of-Squares and Sherali-Adams, respectively. Lastly in Section 3.4 we exemplify the use of semantic arguments for resource-bounded refutations by giving a semantic proof of the fact that SOS p-simulates Polynomial Calculus Resolution over reals, a result originally proved by Berkholz in [15].

## 3.1 Reduction operators for Polynomial Calculus

For Polynomial Calculus the appropriate semantic counterpart is provided by the so called reduction operators. These objects were originally introduced by Razborov in [81] to prove degree lower bounds for PC refutations of the pigeonhole principle. Methods involving reduction operators to prove degree lower bounds were refined by Alekhnovic and Razborov in [2], and further developed in [34, 65, 30].

It turns out that reduction operators can actually be used to characterize the existence of degree bounded refutations. This is implicit in [81], but we give the full details below. Secondly we will repurpose the degree bounded reduction operators to define the reduction operators over a set of monomials, so that we can use those to argue for size upper bounds in Polynomial Calculus later in Chapter 5.

### 3.1.1 Reduction operators against degree

For this section fix a field $\mathbb{F}$ and a set $Q$ of equality constraints of degree at most $k$ over the field $\mathbb{F}$. For $d \geq k$, a degree $d$ **reduction operator** for $Q$ is a linear map $R\colon \mathbb{F}[x]_d \to \mathbb{F}[x]_d$ satisfying the following

- $R(1) = 1$; (3.1)
- $R(q) = 0$ for any $q \in Q$; (3.2)
- $R(p) = R(R(p))$ for any $p \in \mathbb{F}[x]_d$; (3.3)
- $R(xm) = R(xR(m))$ for any variable $x$ and monomial $m$ of degree at most $d$. (3.4)

It is not hard to see that if there is a degree $d$ reduction operator for $Q$, then there cannot be a degree $d$ PC refutation of $Q$. This is the soundness property of reduction operators. The rest of this section is dedicated to proving that the converse, the completeness property, holds. Note that (3.3) is not strictly necessary to prove soundness. However the argument below gives a mapping satisfying also (3.3), and this property actually turns out to be rather useful. For example the lower bound proof in [81] uses the fact that the constructed operator is idempotent in the sense of (3.3).

Let $<$ be a total order on the set of all monomials of degree at most $d$ that respects the degree, i.e. $m < m'$ whenever $\deg(m) < \deg(m')$. The order lifts naturally to the set of all terms by considering the underlying monomials of terms. Given a polynomial $p \in \mathbb{F}[x]_d$, we call the largest term appearing in $p$ with respect to $<$, the **leading term** of $p$, and denote it by $\mathrm{LT}(p)$. The **leading monomial** $p$, denoted $\mathrm{LM}(p)$, is the underlying monomial of the leading term of $p$.

Given a set of polynomials $Q$, and the order $<$, a term $t \in \mathbb{F}[x]_d$ is reducible modulo $Q$, if there is a polynomial $p$ such that $Q \vdash_d p = 0$ and $\mathrm{LT}(p) = t$. Otherwise $t$ is irreducible modulo $Q$. The following lemma shows the important fact that any polynomial can be uniquely decomposed into a PC provable and irreducible component.

**Lemma 3.1.1.** *For any $p \in \mathbb{F}[x]_d$ there are unique $q \in \mathbb{F}[x]_d$ and $r \in \mathbb{F}[x]_d$ such that*

- $p = q + r$*;*
- $Q \vdash_d q = 0$*;*
- $r$ *is a sum of irreducible terms modulo* $Q$*.*

*Moreover* $\mathrm{LT}(p) \geq t$ *for each term* $t$ *in* $r$*.*

*Proof.* To prove the existence of such $q$ and $r$, we construct sequences of elements $p_i, q_i, r_i$ such that

- $p = p_i + q_i + r_i$;
- $Q \vdash_d q_i = 0$;
- $r_i$ is a sum of irreducible terms modulo $Q$;
- $p_m = 0$ for some $m$.

Let $p_1 = p$ and $q_1 = r_1 = 0$. For step $i$, let $\mathrm{LT}(p_i) = t_i$. If $t_i$ is reducible as witnessed by $q$, let $p_{i+1} = p_i - q$, $q_{i+1} = q_i + q$ and $r_{i+1} = r_i$. On the other hand, if $t_i$ is irreducible, let $p_{i+1} = p_i - t_i$, $q_{i+1} = q_i$ and $r_{i+1} = r_i + t_i$.

Now $p_m = 0$ for some $m$, since the rank, i.e. the position in the order $<$, of the leading term of $p_i$ decreases at each step. By construction, $q_m$ and $r_m$ satisfy the conditions of the lemma.

To prove the uniqueness of $q$ and $r$, suppose $p = q + r$ and $p = q' + r'$, i.e. $q - q' = r' - r$. Now $Q \vdash_d q - q' = 0$ and so $Q \vdash_d r' - r = 0$. Hence $\mathrm{LT}(r' - r)$ is not irreducible. However, since both $r$ and $r'$ are sums of irreducible terms, it follows that $\mathrm{LT}(r' - r) = 0$ and so $r = r'$. Hence also $q = q'$. □

Consider now the mapping $R_d^Q \colon \mathbb{F}[x]_d \to \mathbb{F}[x]_d$ that maps each $p$ to the unique sum $r$ of irreducible terms modulo $Q$ such that $Q \vdash_d p - r = 0$. The following lemma gathers five basic properties of the mapping.

**Lemma 3.1.2.** *The following hold.*

- *If there is no PC refutation of $Q$ of degree at most $d$, then $R_d^Q(1) = 1$;* (3.5)
- $R_d^Q(q) = 0$ *for any* $q \in Q$; (3.6)
- $R_d^Q$ *is a linear function;* (3.7)
- $R_d^Q(R_d^Q(p)) = R_d^Q(p)$ *for any polynomial* $p \in \mathbb{F}[x]_d$; (3.8)
- $R_d^Q(xm) = R_d^Q(xR_d^Q(m))$ *for any monomial* $m$ *of degree at most* $d-1$ *and any variable* $x$. (3.9)

*Proof.* To see that (3.5) holds, note first that if there is no refutation of $Q$ of degree $d$ then, the constant polynomial 1 is irreducible modulo $Q$, as 1 is the least monomial with respect to the order $<$. On the other hand $Q \vdash_d 0 = 0$ and so, by the uniqueness of the decomposition, $R_d^Q(1) = 1$.

For (3.6), of course $Q \vdash_d q = 0$ for any $q \in Q$, and 0 is a (empty) sum of irreducible terms modulo $Q$. Hence, by the uniqueness of the decomposition, $R_d^Q(q) = 0$ for any $q \in Q$.

For (3.7), first note that $Q \vdash_d p - R_d^Q(p) = 0$ and $Q \vdash_d q - R_d^Q(q) = 0$, and so $Q \vdash_d p + q - (R_d^Q(p) + R_d^Q(q)) = 0$. Now $R_d^Q(p) + R_d^Q(q)$ is a sum of irreducible terms modulo $Q$ and so, by the uniqueness of the decomposition, $R_d^Q(p+q) = R_d^Q(p) + R_d^Q(q)$. Similarly $Q \vdash_d ap - aR_d^Q(p) = 0$ and so $R_d^Q(ap) = aR_d^Q(p)$.

For (3.8) we have that $Q \vdash_d p - R_d^Q(p) = 0$ and $Q \vdash_d R_d^Q(p) - R_d^Q(R_d^Q(p)) = 0$ and so also $Q \vdash_d p - R_d^Q(R_d^Q(p)) = 0$, where $R_d^Q(R_d^Q(p))$ is a sum of irreducible terms modulo $Q$. Hence, again by the uniqueness of the decomposition, $R_d^Q(p) = R_d^Q(R_d^Q(p))$.

Finally for (3.9) we have again that $Q \vdash_d m - R_d^Q(m) = 0$. Now, by Lemma 3.1.4, each term $t$ in $R_d^Q(m)$ satisfies $t \leq m$. Hence, by the degree-monotonicity condition of $<$, each $t$ in $R_S^Q(m)$ is of degree at most $d-1$. Hence also $Q \vdash_d xm - xR_d^Q(m) = 0$. It follows by the uniqueness of the decomposition that $R_d^Q(xm) = R_d^Q(xR_d^Q(m))$. □

In other words, the previous lemma shows that the linear map $R_d^Q$ constructed is a degree $d$ reduction operator if there is no degree $d$ PC refutation of $Q$. In conclusion, we have the following soundness and completeness theorem for degree $d$ reduction operators.

**Theorem 3.1.3** (Soundness and Completeness)**.** *There is a PC refutation of $Q$ of degree at most $d$ if and only if there is no degree $d$ reduction operator for $Q$.*

### 3.1.2 Reduction operators against sets of monomials

In this section we restate the definitions and results of the previous section for proofs over a set of monomials. These constructions will be used later to prove the feasible interpolation property for Polynomial Calculus in Section 5.1.

For this section fix again a field $\mathbb{F}$ and a set $Q$ of equality constraints. Fix also a set $S$ of monomials containing all the monomials in $Q$ and the empty monomial 1. Recall the definition of a PC proof over a set of monomials $S$ from section 2.3.1, and the definition of the set $\widehat{S}$,

$$\widehat{S} := S \cup \{xm : x \text{ is a variable and } m \in S\}.$$

We call a linear function $R\colon \mathbb{F}[\widehat{S}] \to \mathbb{F}[\widehat{S}]$ a **reduction operator for $Q$ over $S$** if it satisfies the following conditions:

- $R(1) = 1$; (3.10)
- $R(q) = 0$ for any $q \in Q$; (3.11)
- $R(p) = R(R(p))$ for any $p \in \mathbb{F}[\widehat{S}]$; (3.12)
- $R(xm) = R(xR(m))$ for any variable $x$ and $m \in S$. (3.13)

Again it is easy to see that if there is a refutation of $Q$ over $S$, then there cannot be a reduction operator for $Q$ over $S$. This is the soundness property reduction operators over a set of monomials. We prove below that the converse, the completeness, also holds. Note again that (3.12) is not strictly necessary for soundness. The proof below however produces a mapping

having this property, and moreover this property is actually needed later in the proof of Theorem 5.1.1.

We proceed with the proof. Let $<$ be a total order on $\widehat{S}$ satisfying the following two conditions:

- $1 \leq m$ for any $m \in \hat{S}$; (3.14)
- if $m \in S$ and $m' \in \widehat{S} \setminus S$, then $m < m'$. (3.15)

Again the order lifts to the set of all terms built from the monomials in $\hat{S}$. The leading term of a polynomial $p \in \mathbb{F}[\hat{S}]$, denoted $\mathrm{LT}(p)$, is the largest term in $p$ with respect to $<$, and the leading monomials, denoted $\mathrm{LM}(p)$, is its underlying monomial.

We say that a term $t \in \mathbb{F}[\hat{S}]$ is $S$-reducible modulo $Q$ if there is $p \in \mathbb{F}[\widehat{S}]$ such that $Q \vdash_S p = 0$ and $t = \mathrm{LT}(p)$. Otherwise the term is $S$-irreducible modulo $Q$. The following lemma shows that any polynomial in $\mathbb{F}[\hat{S}]$ can be uniquely decomposed into a provable and an $S$-irreducible component. We omit the proof, since it is exactly the same as the proof of Lemma 3.1.1

**Lemma 3.1.4.** *For any polynomial $p \in \mathbb{F}[\hat{S}]$ there are unique $q \in \mathbb{F}[\hat{S}]$ and $r \in \mathbb{F}[\hat{S}]$ such that*

- $p = q + r$; (3.16)
- $Q \vdash_S q = 0$; (3.17)
- *$r$ is a sum of $S$-irreducible terms modulo $Q$.* (3.18)

*Moreover* $\mathrm{LT}(p) \geq t$ *for each term $t$ in $r$.*

Consider now the mapping $R_S^Q \colon \mathbb{F}[\widehat{S}] \to \mathbb{F}[\widehat{S}]$ that maps each $p$ to the unique sum $r$ of $S$-irreducible terms modulo $Q$ such that $Q \vdash_S p - r = 0$. The following lemma gathers the basic properties of such mapping.

**Lemma 3.1.5.** *The following hold.*

- *If there is no refutation of $Q$ over $S$, then $R_S^Q(1) = 1$;* (3.19)

- $R^Q_S(q) = 0$ *for any* $q \in Q$*;* (3.20)
- $R^Q_S$ *is a linear function;* (3.21)
- $R^Q_S(R^Q_S(p)) = R^Q_S(p)$ *for any polynomial* $p \in \mathbb{F}[\widehat{S}]$*;* (3.22)
- $R^Q_S(xm) = R^Q_S(xR^Q_S(m))$ *for any* $m \in S$ *and any variable* $x$*.* (3.23)

*Proof.* For (3.19) note first that there is no refutation of $Q$ over $S$, then, by (3.14), the constant polynomial 1 is $S$-irreducible modulo $Q$. On the other hand $Q \vdash_S 0 = 0$ and so, by the uniqueness of the decomposition, $R^Q_S(1) = 1$.

For (3.20), of course $Q \vdash_S q = 0$ for any $q \in Q$. On the other hand the constant polynomial 0 is vacuously a sum of $S$-irreducible terms, and so, by the uniqueness of the decomposition, $R^Q_S(q) = 0$ for any $q \in Q$.

For (3.21) first note that $Q \vdash_S p - R^Q_S(p) = 0$ and $Q \vdash_S q - R^Q_S(q) = 0$, and so $Q \vdash_S p+q-(R^Q_S(p)+R^Q_S(q)) = 0$. Now $R^Q_S(p)+R^Q_S(q)$ is a sum of $S$-irreducible terms modulo $Q$ and so, by the uniqueness of the decomposition, $R^Q_S(p+q) = R^Q_S(p) + R^Q_S(q)$. Similarly $Q \vdash_S ap - aR^Q_S(p) = 0$ and so $R^Q_S(ap) = aR^Q_S(p)$.

For (3.22) we have that $Q \vdash_S p - R^Q_S(p) = 0$ and $Q \vdash_S R^Q_S(p) - R^Q_S(R^Q_S(p)) = 0$ and so also $Q \vdash_S p - R^Q_S(R^Q_S(p)) = 0$, where $R^Q_S(R^Q_S(p))$ is a sum of $S$-irreducible terms modulo $Q$. Hence, again by the uniqueness of the decomposition, $R^Q_S(p) = R^Q_S(R^Q_S(p))$.

Finally for (3.23) we have that $Q \vdash_S m - R^Q_S(m) = 0$. Now, by Lemma 3.1.4, each term $t$ in $R^Q_S(m)$ satisfies $t \leq m$. Hence, by (3.15), each $t$ in $R^Q_S(m)$ is in $S$, and so $R^Q_S(m) \in \mathbb{F}[S]$. Hence also $Q \vdash_S xm - xR^Q_S(m) = 0$. It follows that $R^Q_S(xm) = R^Q_S(xR^Q_S(m))$. □

In other words, the lemma above shows that if there is no refutation of $Q$ over $S$, then the operator $R^Q_S$ constructed is a reduction operator for $Q$ over $S$. In conclusion, we have the following soundness and completeness theorem for reduction operators over a set of monomials.

**Theorem 3.1.6** (Soundness and Completeness)**.** *There is a PC refutation of* $Q$ *over* $S$ *if and only if there is no reduction operator for* $Q$ *over* $S$*.*

## 3.2 Pseudoexpectations for Sums-of-Squares

Secondly we consider pseudoexpectations for Sums-of-Squares. Pseudoexpectations are linear functionals that fool resource-bounded SOS to think that the set of constraints is satisfiable by mapping anything provably non-negative with limited resources to a non-negative value. Probably the first instance of this idea to prove degree lower bounds for SOS appears in [36, 37], however the term 'pseudoexpectation' appears for the first time in [9].

As with reduction operators we will think of pseudoexpectations mainly as semantics for resource-bounded SOS refutations and proofs. Another point of view, much more common in combinatorial optimization, is to view the pseudoexpectations as the dual objects to levels of the Sums-of-Squares hierarchy of SDP relaxations. Indeed, these are the primary objects in the Lasserre hierarchy of SDP relaxations [59].

We conceptualize pseudoexpectations differently since our emphasis and goals differ slightly from those of optimization. First of all we are much more interested in refutations than proofs of non-negativity. But more importantly the applications we have in mind are of rather metalogical character, i.e. we aim to prove structural statements about the SOS proof system itself.

We will first define pseudoexpectations against bounded degree SOS proofs. We prove a strong duality theorem between pseudoexpectation values and provable lower bounds using the general duality theorem 2.4.3. This was originally proved in [48] using duality of semidefinite programming. Soundness and completeness theorem for pseudoexpectations will be an immediate consequence of the duality theorem. We will also give a characterization for pseudoexpectations for sets of equality constraints and as consequence give a normal form for SOS proofs from sets of equality constraints.

Secondly we will again introduce a suitable generalization of pseudoex-

pectations that can be used to argue against monomial size of SOS proofs rather than only degree. Finally we consider a form of pseudoexpectations that also takes into account the size of the coefficients that appear in purported SOS refutations.

### 3.2.1 Pseudoexpectations against degree

For this section fix a sets $P$ and $Q$ of inequality and equality constrains, respectively. A **degree $d$ SOS pseudoexpectation** for $P$ and $Q$ is a linear functional $E\colon \mathbb{R}[x]_d \to \mathbb{R}$ such that

- $E(1) = 1$; (3.24)
- $E(p) \geq 0$ if $P, Q \vdash_d^{\text{SOS}} p \geq 0$. (3.25)

We denote the set of all degree $d$ SOS pseudoexpectations for $P$ and $Q$ by $\mathscr{E}_d^{\text{SOS}}(P, Q)$.

The following lemma is key in obtaining the duality theorem for SOS pseudoexpectations. It shows that the constant polynomial 1 is an order unit for the cone of polynomials provable in SOS in degree $2d$.

**Lemma 3.2.1.** *For any $p \in \mathbb{R}[x]_{2d}$,*

$$\emptyset \vdash_{2d}^{\text{SOS}} \|p\|_1 \geq p,$$

*where $\|p\|_1 = \sum_\alpha |a_\alpha|$, when $p = \sum a_\alpha x^\alpha$.*

*Proof.* We prove that $\vdash_{2d}^{\text{SOS}} |a| \geq am$ for any monomial $m$ of degree at most $2d$, and any $a \in \mathbb{R}$. The claim follows then immediately.

We show first that $\vdash_{2d}^{\text{SOS}} |a| \geq am$ for any monomial $m$ of degree at most $d$, and any $a \in \mathbb{R}$. If $a \geq 0$, then $a - am \equiv (\sqrt{a} - \sqrt{a}m)^2 \mod I_n$, and so $\vdash_{2d}^{\text{SOS}} |a| \geq am$. If on the other hand $a < 0$, then $-am \equiv (\sqrt{-a}m)^2 \mod I_n$, and so $\vdash_{2d}^{\text{SOS}} 0 \geq am$.

Finally we show using the above paragraph that $\vdash_{2d}^{\text{SOS}} |a| \geq am$ for any monomial $m$ of degree at most $2d$ and $a \in \mathbb{R}$. Let $m_1$ and $m_2$ be two monomials of degree at most $d$ such that $m = m_1 m_2$. Now if $a \geq 0$, then

$am_1 - 2am_1m_2 + am_2 \equiv (\sqrt{a}m_1 - \sqrt{a}m_2)^2 \mod I_n$. Now, by previous paragraph, $\vdash_{2d}^{\text{SOS}} |a| \geq am_1$ and $\vdash_{2d}^{\text{SOS}} |a| \geq am_2$. Now $\vdash_{2d}^{\text{SOS}} 2|a| \geq 2am_1m_2$ and so $\vdash_{2d}^{\text{SOS}} |a| \geq am_1m_2$. If $a < 0$, then $-am_1 - 2am_1m_2 - am_2 \equiv (\sqrt{-a}m_1 + \sqrt{-a}m_2)^2 \mod I_n$. Again, $\vdash_{2d}^{\text{SOS}} |a| \geq -am_1$ and $\vdash_{2d}^{\text{SOS}} |a| \geq -am_2$, and so $\vdash_{2d}^{\text{SOS}} |a| \geq am_1m_2$. □

By the above lemma, degree $2d$ SOS pseudoexpectations for $P$ and $Q$ are exactly the states for the convex cone of all polynomials in $\mathbb{R}[x]_{2d}$ provably non-negative in degree $2d$ from $P$ and $Q$. Hence, by Theorem 2.4.3, we obtain the following Duality Theorem for SOS.

**Theorem 3.2.2** (Duality theorem)**.** *For any $p \in \mathbb{R}[x]_{2d}$,*

$$\sup\{r \in \mathbb{R} : P, Q \vdash_{2d}^{\text{SOS}} p \geq r\} = \inf\{E(p) : E \in \mathscr{E}_{2d}^{\text{SOS}}(P, Q)\}.$$

*Moreover, if $\mathscr{E}_{2d}^{\text{SOS}}(P, Q) \neq \emptyset$, the infimum is attained by some $E \in \mathscr{E}_{2d}^{\text{SOS}}(P, Q)$.*

An immediate corollary to the above theorem is the following soundness and completeness theorem.

**Theorem 3.2.3** (Soundness and Completeness)**.** *There is a degree $2d$ SOS refutation of $P$ and $Q$ if and only if there is no degree $2d$ SOS pseudoexpectation for $P$ and $Q$.*

### 3.2.2 Characterization of pseudoexpectations and a normal form for SOS refutations

In this section we prove a characterization of the pseudoexpectations for sets of equality constraints, and obtain a normal form for SOS refutation as a corollary.

**Lemma 3.2.4.** *Let $Q$ be a set of equality constraints of degree at most $k$, and let $d \geq k$. Then a linear functional $E\colon \mathbb{R}[x]_{2d} \to \mathbb{R}$ is a degree $2d$ pseudoexpectation for $Q$ if and only if it satisfies the following conditions:*

- $E(1) = 1$; (3.26)

- $E(p) = E(q)$ *if* $p \equiv q \mod I_n$; (3.27)
- $E(p^2) \geq 0$ *for any* $p \in \mathbb{R}[x]_d$; (3.28)
- $E(q^2) = 0$ *for any* $q \in Q$. (3.29)

*Proof.* For the non-trivial direction let $E$ be a linear functional satisfying the conditions (3.26)-(3.29). We need to prove that $E(mq) = 0$ for any $q \in Q$ and any monomial $m$ such that the degree of $mq$ is at most $2d$.

Let $q \in Q$ be of degree $k_0$, and let $m$ be a monomial of degree at most $2d - k_0$. Let $m_1$ and $m_2$ be monomials of degree at most $d - k_0$ and $d$, respectively, such that $m = m_1 m_2$.

We prove first that $E((m_1 q)^2) = 0$. We have that

$$q^2 - (m_1 q)^2 \equiv (q - m_1 q)^2 \mod I_n,$$

and so $E((m_1 q)^2) \leq E(q^2)$ by (3.27) and (3.28). On the other hand $E((m_1 q)^2) \geq 0$ by (3.26) and $E(q^2) = 0$ by (3.29), and thus $E((m_1 q)^2) = 0$.

Secondly

$$(m_1 q)^2 \pm 2a m_1 m_2 q + a^2 m_2 \equiv (m_1 q \pm a m_2)^2 \mod I_n$$

for any $a > 0$, and so, by (3.27), (3.28) and the above paragraph,

$$|E(2m_1 m_2 q)| \leq E(m_1 q^2)/a + E(a m_2) \leq E(a m_2) = a E(m_2)$$

for any $a > 0$. Hence $E(m_1 m_2 q) = 0$. □

As a corollary for the characterization above we get the following normal form for Sums-of-Squares refutations of a set of equality constraints.

**Lemma 3.2.5.** *Let $Q$ be a set of equality constraints of degree at most $k$, and let $d \geq k$. If there is a degree $2d$ SOS refutation of $Q$, then there is a sum of squares $s$ of degree at most $2d$ and $a_q \in \mathbb{R}$ for every $q \in Q$ such that*

$$-1 \equiv s + \sum_{q \in Q} a_q q^2 \mod I_n.$$

*Proof.* Let $\mathcal{C}$ be the convex cone of all the polynomials $p$ of degree at most $2d$ such that

$$p \equiv s + \sum_{q \in Q} a_q q^2 \mod I_n,$$

for some sum of squares $s$ of degree at most $2d$ and $a_q \in \mathbb{R}$ for $q \in Q$, and suppose towards a contradiction that $-1 \notin \mathcal{C}$. By Lemma 3.2.1, $\mathcal{C}$ is a convex cone that admits an order unit, namely the constant polynomial 1, and so, by Lemma 2.4.4, there is some linear functional $L \colon \mathbb{R}[x]_{2d} \to \mathbb{R}$ such that $L(1) = 1$ and $L(p) \geq 0$ for every $p \in \mathcal{C}$. In particular $L(q^2) = 0$ for every $q \in Q$, and so, by Lemma 3.2.4, $L$ is a degree $2d$ pseudoexpectation for $Q$. □

### 3.2.3 Pseudoexpectations against a set of monomials

In this section we define the appropriate counterpart of SOS proofs over some set $S$ of monomials, and obtain analogues of the results above for bounded degree SOS proofs and pseudoexpectations.

Fix again for this section sets $P$ and $Q$ of equality and inequality constraints, respectively, and a set $S$ of monomials containing the empty monomial 1. An SOS pseudoexpectation for $P$ and $Q$ over $S$ is a linear functional $E \colon \mathbb{R}[S^2] \to \mathbb{R}$ such that

- $E(1) = 1$; (3.30)
- $E(p) \geq 0$, when $P, Q \vdash_S^{\text{SOS}} p \geq 0$. (3.31)

We denote by $\mathscr{E}_S^{\text{SOS}}(P, Q)$ the set of all SOS pseudoexpectations for $P$ and $Q$ over $S$.

Again, using Theorem 2.4.3, we obtain a strong duality theorem for SOS pseudoexpectations over a set of monomials via the following lemma, and the soundness and completeness theorem as a consequence of the duality theorem.

**Lemma 3.2.6.** *For any $p \in \mathbb{R}[S^2]$,*

$$\vdash_S^{\text{SOS}} \|p\|_1 \geq p,$$

*where* $\|p\|_1 = \sum |a_\alpha|$, *when* $p = \sum a_\alpha x^\alpha$.

*Proof.* We prove that for any $m \in S^2$ and $a \in \mathbb{R}$,

$$\vdash_S^{\text{SOS}} |a| \geq am.$$

First suppose that $m \in S$, and let $a \in \mathbb{R}$. If $a \geq 0$, then $a - am \equiv (\sqrt{a} - \sqrt{a}m)^2 \mod J_n$, and so $\vdash_S^{\text{SOS}} a \geq am$. If on the other hand $a < 0$, then $-am \equiv (\sqrt{-a}m)^2 \mod J_n$, and so $\vdash_S^{\text{SOS}} 0 \geq am$. Hence also $\vdash_S^{\text{SOS}} |a| \geq am$.

Let then $m_1, m_2 \in S$, and let $a \in \mathbb{R}$. If $a \geq 0$, then $am_1 - 2am_1m_2 + am_2 \equiv (\sqrt{a}m_1 - \sqrt{a}m_2)^2 \mod J_n$. Now, by previous paragraph, $\vdash_S^{\text{SOS}} |a| \geq am_1$ and $\vdash_S^{\text{SOS}} |a| \geq am_2$. Now $\vdash_S^{\text{SOS}} 2|a| \geq 2am_1m_2$ and so $\vdash_S^{\text{SOS}} |a| \geq am_1m_2$. If $a < 0$, then $-am_1 - 2am_1m_2 - am_2 \equiv (\sqrt{-a}m_1 + \sqrt{-a}m_2)^2 \mod J_n$. Again, $\vdash_S^{\text{SOS}} |a| \geq -am_1$ and $\vdash_S^{\text{SOS}} |a| \geq -am_2$, and so $\vdash_S^{\text{SOS}} |a| \geq am_1m_2$. □

**Theorem 3.2.7** (Duality theorem)**.** *For any* $p \in \mathbb{R}[S^2]$,

$$\sup\{r \in \mathbb{R} : P, Q \vdash_S^{\text{SOS}} p \geq r\} = \inf\{E(p) : E \in \mathscr{E}_S^{\text{SOS}}(P, Q)\}.$$

*Moreover, if* $\mathscr{E}_S^{\text{SOS}}(P, Q) \neq \emptyset$, *then there is* $E \in \mathscr{E}_S^{\text{SOS}}(P, Q)$ *that achieves the infimum.*

**Theorem 3.2.8** (Soundness and Completeness)**.** *There is an SOS refutation of* $P$ *and* $Q$ *over* $S$ *if and only if there is no SOS pseudoexpectation for* $P$ *and* $Q$ *over* $S$.

Finally, for a set $Q$ of equality constraints we obtain a characterization of SOS pseudoexpectations for $Q$ over $S$ and a normal form for SOS refutations over $S$ as corollary.

**Lemma 3.2.9.** *Let* $Q$ *be a set of equality constraints and let* $S$ *be a set of monomials containing all the monomials in* $Q$, *all variables and the empty monomial* 1. *A linear functional* $E \colon \mathbb{R}[S^2] \to \mathbb{R}$ *is an SOS pseudoexpectation for* $Q$ *over* $S$ *if and only if the following conditions hold:*

- $E(1) = 1$; (3.32)

- $E(p) = E(q)$ *if* $p \equiv q \mod J_n$; (3.33)
- $E(p^2) \geq 0$ *for any* $p \in \mathbb{R}[S]$; (3.34)
- $E(q^2) = 0$ *for any* $q \in Q$; (3.35)
- $E((x_i + \bar{x}_i - 1)^2) = 0$ *for any* $i \in [n]$. (3.36)

*Proof.* For the non-trivial direction assume that $E\colon \mathbb{R}[S^2] \to \mathbb{R}$ is a linear functional satisfying the conditions (3.32)-(3.36). We show that $E(mq) = 0$ for every $m \in S$ and $q \in Q$. By (3.34), $E((am \pm q/a)^2) \geq 0$ for every $a > 0$, and so,$|E(2mq)| \leq E(a^2m^2) + E(q^2/a^2)$. By (3.35), $E(q^2/a^2) = 0$, and so $|E(2mq)| \leq E(a^2m^2)$ for any $a > 0$. It follows that $E(mq) = 0$. With a similar argument one obtains that $E(m(x_i + \bar{x}_i - 1)) = 0$ for any $m \in S$ and $i \in [n]$. □

**Lemma 3.2.10.** *Let $Q$ be a set of equality constraints and let $S$ be a set of monomials that contains all the monomials in $Q$, all variables and the empty monomial 1. If there is an SOS refutation of $Q$ over $S$, then there is a sum of squares $s$ of polynomials in $\mathbb{R}[S]$ and $a_q \in \mathbb{R}$ for $q \in Q$ and $b_i \in \mathbb{R}$ for $i \in [n]$ such that*

$$-1 \equiv s + \sum_{q \in Q} a_q q^2 + \sum_{i \in [n]} b_i (x_i + \bar{x}_i - 1)^2 \mod J_n.$$

*Proof.* Let $\mathcal{C}$ be the convex cone of all the polynomials $p \in \mathbb{R}[S^2]$ such that

$$p \equiv s + \sum_{q \in Q} a_q q^2 + \sum_{i \in [n]} b_i (x_i + \bar{x}_i - 1)^2 \mod J_n,$$

for some sum of squares $s$ of polynomials in $\mathbb{R}[S$, some $a_q \in \mathbb{R}$ for $q \in Q$ and some $b_i \in \mathbb{R}$ for $i \in [n]$, and suppose towards a contradiction that $-1 \notin \mathcal{C}$. By Lemma 3.2.6, $\mathcal{C}$ is a convex cone that admits an order unit, namely the constant polynomial 1, and so, by Lemma 2.4.4, there is some linear functional $L\colon \mathbb{R}[S^2] \to \mathbb{R}$ such that $L(1) = 1$ and $L(p) \geq 0$ for every $p \in \mathcal{C}$. In particular $L(q^2) = 0$ and $L((x_i + \bar{x}_i - 1)^2) = 0$ for every $q \in Q$ and $i \in [n]$, and so, by Lemma 3.2.9, $L$ is a pseudoexpectation for $Q$ over $S$. □

### 3.2.4 Pseudoexpectations against bounded refutations

Finally we formulate pseudoexpectations in a form that takes also into account the size of the coefficients appearing in purported refutations. Later in Section 5.2.2 when we consider the proof search problem for SOS, we need to consider SOS refutations with a given bound on the size of the coefficients in order to give a polynomial time proof search algorithm. Hence we also need a semantic characterization for SOS refutations that carries information about the size of the coefficients. We formulate such objects only for sets of equality constraints. It is not immediately clear how to extend the definitions meaningfully to the situation with inequality constraints.

Fix for this section a set $Q$ of equality constraints and a set $S$ of monomials containing all the monomials in $Q$, all the variables and the empty monomial 1. We say that an SOS proof

$$p \equiv \sum_{i\in[k]} r_i^2 + \sum_{q\in Q} t_q q + \sum_{i\in[n]} u_i(x_i + \bar{x}_i - 1) \mod J_n \tag{3.37}$$

is **$R$-bounded** if $\|t_q\|_\infty \leq R$ for any $q \in Q$ and $\|u_i\|_\infty \leq R$ for any $i \in [n]$. Note that we do not bound the size of the coefficients in the polynomials $r_i$ or in the lifts of the axioms of the form $x^2 - x$ in an $R$-bounded SOS proof. This is for the simplicity of the semantic characterization below. Moreover we will see later in Section 5.2.2 that a bound on the polynomials $t_q$ and $u_i$ suffice for an efficient proof search.

For $\epsilon > 0$, an **$\varepsilon$-pseudoexpectation for $Q$ over $S$** is a linear functional $E\colon \mathbb{R}[S^2] \to \mathbb{R}$ satisfying the following:

- $E(1) = 1$; (3.38)
- $E(p) = E(q)$ if $p \equiv q \mod J_n$; (3.39)
- $E(p^2) \geq 0$ for any $p \in \mathbb{R}[S]$; (3.40)
- $|E(mq)| \leq \varepsilon$ for any $m \in S$ and $q \in Q$. (3.41)
- $|E(m(x_i + \bar{x}_i - 1))| \leq \varepsilon$ for any $m \in S$ and $i \in [n]$. (3.42)

The following two lemmas give the correspondence between $R$-bounded refutations of $Q$ over $S$ and $\varepsilon$-pseudoexpectations for $Q$ over $S$.

**Lemma 3.2.11** (Soundness)**.** *If there is an $\varepsilon$-pseudoexpectation for $Q$ over $S$, then there is no $R$-bounded refutation of $Q$ over $S$ for $R$ less than $1/\varepsilon|S|(|Q|+n)$.*

*Proof.* Let $E$ be an $\varepsilon$-pseudoexpectation for $Q$ over $S$, and suppose that

$$-1 \equiv s + \sum_{q\in Q} t_q q + \sum_{i\in[n]} u_i(x_i + \bar{x}_i - 1) \mod J_n$$

is a refutation over $S$ with $\|t_q\|_\infty, \|u_i\|_\infty < 1/\varepsilon|S|(|Q|+n)$ for any $q \in Q$ and $i \in [n]$. Now $|E(amq)| \leq |a|\varepsilon$ for each $m \in S$, $q \in Q$ and $a \in \mathbb{R}$. Hence $|E(t_q q)| < 1/(|Q|+n)$ for each $q \in Q$. Similarly $|E(u_i(x_i + \bar{x}_i - 1))| < 1/(|Q|+n)$ for each $i \in [n]$. Hence

$$\left| E\left( \sum_{q\in Q} t_q q + \sum_{i\in[n]} u_i(x_i + \bar{x}_i - 1) \right) \right| < 1.$$

Now applying $E$ to both sides of the refutation we obtain that

$$-1 \geq \sum_{q\in Q} E(t_q q) + \sum_{i\in[n]} E(u_i(x_i + \bar{x}_i - 1)) > -1;$$

a contradiction. □

**Lemma 3.2.12** (Completeness)**.** *If there is no $R$-bounded refutation of $Q$ over $S$, then there is a $(1/R)$-pseudoexpectation for $Q$ over $S$.*

*Proof.* Suppose there is no $R$-bounded refutation of $Q$ over $S$, and consider the following two sets

$$A := \{p \in \mathbb{R}[S^2] : \emptyset \vdash_S^{\text{SOS}} p \geq 0\}$$

and

$$B := \{-1 + \sum_{q\in Q} t_q q + \sum_{i\in[n]} u_i(x_i + \bar{x}_i - 1) : \\ t_q, u_i \in \mathbb{R}[S] \text{ and } \|t_q\|_\infty, \|u_i\|_\infty \leq R \text{ for every } q \in Q \text{ and } i \in [n]\}.$$

Now, by assumption, $A$ and $B$ are disjoint, $A$ is a convex cone and $B$ is a convex set. Moreover, by Lemma 3.2.6, $A$ admits an order unit, the constant polynomial 1. Now, by Lemma 2.4.4, there is a linear functional $E\colon \mathbb{R}[S^2] \to \mathbb{R}$ such that $E(1) = 1$, $E(p) \geq 0$ for every $p \in A$, and $E(p') \leq 0$ for every $p' \in B$.

We claim that $E$ has the desired properties. We prove (3.41), and leave others to the reader. By definition, $-1 \pm Rmq \in B$, and so $E(-1 \pm Rmq) \leq 0$ for any $m \in S$ and $q \in Q$. Hence $|E(mq)| \leq 1/R$. □

In the proof of the completeness lemma we needed the fact that the size of the coefficients in the squares or in the lifts of the Boolean axioms of the form $x^2 - x$ were not restricted in the definition of an $R$-bounded refutation in order to guarantee that the set $A$ is actually a convex cone of the space $\mathbb{R}[S^2]$ that admits an order unit.

Finally we prove a version of the normal form lemma 3.2.10 that takes into account the size of coefficients appearing in the refutations. This version of the lemma together with the proof search algorithm in Section 5.2.2 show that one can p-simulate arbitrary SOS refutations from sets of equality constraints almost completely inside the squares.

**Lemma 3.2.13.** *Let $Q$ be a set of equality constraints and let $S$ be a set of monomials that contains all the monomials in $Q$, all the variables and the empty monomial 1. If there is an $R$-bounded SOS refutation of $Q$ over $S$, then there is a sum of squares $s$ of polynomials in $\mathbb{R}[S]$ and $a_q, b_i \in \mathbb{R}$ for $q \in Q$ and $i \in [n]$ such that*

$$-1 \equiv s + \sum_{q \in Q} a_q q^2 + \sum_{i \in [n]} b_i (x_i + \bar{x}_i - 1) \mod J_n,$$

*and $|a_q|, |b_i| \leq R_0^2$ for every $q \in Q$ and $i \in [n]$ where $R_0 = R|S|(|Q|+n)+1$.*

*Proof.* Suppose towards a contradiction that the conclusion of the lemma does not hold, and consider the following two sets

$$A := \{p \in \mathbb{R}[S^2] : \emptyset \vdash_S^{\mathrm{SOS}} p \geq 0\}$$

and

$$B := \{-1 + \sum_{q \in Q} a_q q^2 + \sum_{i \in [n]} b_i(x_i + \bar{x}_i - 1) : |a_q|, |b_i| \leq R_0^2\}.$$

Now, by assumption, $A$ and $B$ are disjoint, and, by construction, $A$ is a convex cone that admits an order unit 1 and $B$ is a convex set. By Lemma 2.4.4 there is a linear functional $L \colon \mathbb{R}[S^2] \to \mathbb{R}$ such that $L(1) = 1$, $L(p) \geq 0$ for every $p \in P$ and $L(q) \leq 0$ for every $q \in B$.

Now for every $q \in Q$, we have that $-1 \pm R_0^2 q^2 \in B$ holds, and thus $|L(q^2)| \leq 1/R_0^2$. Now let $m \in S$. We show that $|L(mq)| \leq 1/R_0$.

First assume that $L(m) = 0$. Then

$$L(m^2 \pm 2amq + a^2 q^2) \geq 0$$

for any $a > 0$. Thus $|L(mq)| \leq L(m/(2a)) + L((aq^2)/2) = L((aq^2)/2)$ for any $a > 0$. Hence $L(mq) = 0$. Similarly if $L(q^2) = 0$, then $L(mq) = 0$.

Assume then that $L(m) > 0$ and $L(q^2) > 0$. Now

$$\frac{m}{2L(m)} \pm \frac{mq}{\sqrt{L(m)L(q^2)}} + \frac{q^2}{2L(q^2)} \equiv \left( \frac{m}{\sqrt{2L(m)}} \pm \frac{q}{\sqrt{2L(q^2)}} \right)^2 \mod J_n$$

Hence

$$1 \pm \frac{L(mq)}{\sqrt{L(m)L(q^2)}} \geq 0,$$

and so $|L(mq)| \leq \sqrt{L(m)L(q^2)} \leq 1/R_0$, since $L(m) \leq 1$ for every $m \in S$.

By a similar argument we obtain that $|L(m(x_i + \bar{x}_i - 1))| \leq 1/R_0$ for every $m \in S$ and $i \in [n]$. Now it is easy to see that $L$ satisfies the other conditions of an $1/R_0$-pseudoexpectation for $Q$ over $S$. Now, by the soundness lemma above, there is no $R'$-bounded refutation of $Q$ over $S$ for $R'$ less than $R_0/(|S|(|Q| + n))$. But this contradicts the assumption that there is an $R$-bounded SOS refutation of $Q$ over $S$. □

## 3.3 Pseudoexpectations for Sherali-Adams

Lastly we consider pseudoexpectations for Sherali-Adams. The basic ideas and principles behind these are the same as with Sums-of-Squares. We consider first pseudoexpectations against degree and prove the duality theorem

for SA. Secondly we introduce the notion of pseudoexpectations over a set of monomials for SA.

### 3.3.1 Pseudoexpectations against degree

For this section fix again sets $P$ and $Q$ of inequality and equality constraints. A **degree $d$ SA pseudoexpectation** for $P$ and $Q$ is a linear functional $E\colon \mathbb{R}[x]_d \to \mathbb{R}$ such that

- $E(1) = 1$; (3.43)
- $E(p) \geq 0$ when $P, Q \vdash_d^{\mathrm{SA}} p \geq 0$. (3.44)

We denote the set of all degree $d$ SA pseudoexpectations for $P$ and $Q$ by $\mathscr{E}_d^{\mathrm{SA}}(P, Q)$. The duality theorem for SA pseudoexpectations will be again a consequence of the following lemma.

**Lemma 3.3.1.** *For any $p \in \mathbb{R}[x]_d$,*

$$\emptyset \vdash_d^{\mathrm{SA}} \|p\|_1 \geq p,$$

*where $\|p\|_1 = \sum_\alpha |a_\alpha|$, when $p = \sum a_\alpha x^\alpha$.*

*Proof.* We prove that $\vdash_d^{\mathrm{SA}} |a| \geq am$ for any monomial $m$ of degree at most $d$ and any $a \in \mathbb{R}$, by induction on the degree of $m$.

If $\deg(m) = 0$, then the claim is clear. If $\deg(m) = 1$, then $m = x$ for some basic or twin variable $x$. If $a < 0$, then $\vdash_d^{\mathrm{SA}} -a - am \geq 0$, and so $\vdash_d^{\mathrm{SA}} |a| \geq am$. If on the other hand $a \geq 0$, then $\vdash_d^{\mathrm{SA}} a\bar{x} \geq 0$, i.e. $\vdash_d^{\mathrm{SA}} a - ax \geq 0$, and so $\vdash_d^{\mathrm{SA}} a \geq am$.

Suppose then that $\deg(m) > 1$, let $a \in \mathbb{R}$ and write $m = xm'$ for some variable $x$ and monomial $m'$. Now, by induction assumption, $\vdash_d^{\mathrm{SA}} |a| \geq am'$, and so $\vdash_d^{\mathrm{SA}} |a|x \geq am$. Now, by previous paragraph, $\vdash_d^{\mathrm{SA}} |a| \geq |a|x$, and so we obtain $\vdash_d^{\mathrm{SA}} |a| \geq am$. □

By the above lemma, degree $d$ SA-pseudoexpectations for $P$ and $Q$ are exactly the states in $\mathbb{R}[x]_d$ for the convex cone of all polynomials provably in Sherali-Adams non-negative in degree $d$ from $P$ and $Q$. Hence, by Theorem

2.4.3, we obtain the following Duality Theorem for degree bounded Sherali-Adams.

**Theorem 3.3.2** (Duality theorem)**.** *For any $p \in \mathbb{R}[x]_d$,*

$$\sup\{r \in \mathbb{R} : P, Q \vdash_d^{\mathrm{SA}} p \geq r\} = \inf\{E(p) : E \in \mathscr{E}_d^{\mathrm{SA}}(P, Q)\}.$$

*Moreover, if $\mathscr{E}_d^{\mathrm{SA}}(P, Q) \neq \emptyset$, the infimum is attained by some $E \in \mathscr{E}_d^{\mathrm{SA}}(P, Q)$.*

An immediate corollary to the above theorem is again the following soundness and completeness theorem.

**Theorem 3.3.3** (Soundness and Completeness)**.** *There is a degree $d$ SA refutation of $P$ and $Q$ if and only if there is no degree $d$ SA-pseudoexpectation for $P$ and $Q$.*

To end this subsection we prove an analogue of Lemma 3.2.5 for Sherali-Adams. For Sherali-Adams we can only prove the lemma for sets of equality constraints of a special form. Importantly, however, this includes the multiplicative encoding of CNFs, where we encode a clause $\ell_1 \vee \ldots \vee \ell_k$ as the equality constraint $\prod_{i \in [k]} \bar{\ell}_i = 0$.

**Lemma 3.3.4.** *Let $Q$ be a set of equality constraints of the form $q = 0$, where $q$ is a positive linear combination of monomials. If there is a degree $d$ SA refutation of $Q$, then there is a positive linear combination $s$ of monomials of degree at most $d$, and $a_q \in \mathbb{R}$ for each $q \in Q$ such that*

$$-1 \equiv s + \sum_{q \in Q} a_q q \mod I_n.$$

*Proof.* Suppose towards a contradiction that the conclusion does not hold, and let $\mathcal{C}$ be the convex cone of all polynomials $p$ of degree at most $d$ such that

$$p \equiv s + \sum_{q \in Q} a_q q \mod I_n,$$

where $s$ is a positive linear combination of monomials of degree at most $d$ and $a_q \in \mathbb{R}$ for every $q \in Q$. By assumption $-1 \notin \mathcal{C}$. Then, by Lemma

2.4.4, there is some linear functional $L\colon \mathbb{R}[x]_d \to \mathbb{R}$ such that $L(1) = 1$ and $L(p) \geq 0$ for every $p \in \mathcal{C}$.

Our aim is to prove that $L(mq) = 0$ for every monomial $m$ such that the degree of $mq$ is at most $d$. This shows that $L$ is a degree $d$ SA-pseudoexpectation for $Q$, and thus we reach contradiction by the soundness theorem.

So fix an arbitrary $q \in Q$, and write $q = \sum a_\alpha x^\alpha$, and let $m$ be a monomial so that the degree of $mq$ is at most $d$. First note that $L(x^\alpha) = 0$ for any $\alpha$. This follows, since $q$ is a positive linear combination of monomials, and $L(q) = 0$. On the other we have that $x^\alpha - mx^\alpha \in \mathcal{C}$ by a simple telescoping sum: write $m = \prod_{i\in[k]} \ell_i$ and note that

$$x^\alpha - x^\alpha \prod_{i\in[k]} \ell_i \equiv x^\alpha \bar{\ell}_1 + x^\alpha \ell_1 \bar{\ell}_2 + \cdots + x^\alpha \prod_{i\in[k-1]} \ell_i \bar{\ell}_k \mod I_n.$$

Hence $L(x^\alpha) \geq L(mx^\alpha)$. Moreover, since $mx^\alpha \in \mathcal{C}$, we have that $L(mx^\alpha) \geq 0$. Hence $L(mx^\alpha) = 0$ for any $\alpha$, and so also $L(mq) = 0$. □

### 3.3.2 Pseudoexpectations against sets of monomials

Secondly we define SA pseudoexpectations over a set of monomials. Fix again for this section sets $P$ and $Q$ of inequality and equality constraints. An **SA pseudoexpectation** for $P$ and $Q$ **over** $S$ is a linear functional $E\colon \mathbb{R}[S] \to \mathbb{R}$ such that

- $E(1) = 1$; (3.45)
- $E(p) \geq 0$, when $P, Q \vdash_S p \geq 0$. (3.46)

We denote by $\mathscr{E}_S^{\mathrm{SA}}(P, Q)$ the set of all SA-pseudoexpectations for $P$ and $Q$ over $S$.

We need to impose some restrictions to the set $S$ in order to prove the duality theorem for SA pseudoexpectations over $S$. We say that the set $S$ is **closed** if it satisfies the following two conditions:

- if $S$ contains a variable $x$, it contains also its twin $\bar{x}$; (3.47)

- for any $m \in S$, there is some variable $x$ and $m' \in S$ such that $xm' = m$ and $\bar{x}m' \in S$. (3.48)

Note that it follows from the definition, that if a closed set $S$ of monomials is non-empty, then $1 \in S$. With this definition at hand, we can prove the analogue of Lemma 3.3.1.

**Lemma 3.3.5.** *If $S$ is a closed set of monomials, then for any $p \in \mathbb{R}[S]$,*

$$\vdash_S^{\mathrm{SA}} \|p\|_1 \geq p.$$

*Proof.* We prove that $\vdash_S^{\mathrm{SA}} |a| \geq am$ for any $m \in S$ and $a \in \mathbb{R}$. If $a < 0$, then by definition, $\vdash_S^{\mathrm{SA}} -a - am \geq 0$, and so $\vdash_S^{\mathrm{SA}} |a| \geq am$.

Suppose then that $a \geq 0$. We argue by induction on the degree of $m$. If $\deg(m) = 0$, the claim is clear. If $\deg(m) = 1$, then $m = x$ for some variable $x$. Now, by condition (3.47), $\bar{x} \in S$, and so $\vdash_S^{\mathrm{SA}} a\bar{x} \geq 0$, and so also $\vdash_S^{\mathrm{SA}} a - ax \geq 0$. Hence $\vdash_S^{\mathrm{SA}} a \geq ax$.

Suppose then that $\deg(m) > 1$. By condition (3.48) there is a variable $x$ and $m' \in S$ such that $m = xm'$. By induction assumption $\vdash_S^{\mathrm{SA}} a \geq am'$. On the other hand, again by condition (3.48), $\bar{x}m' \in S$, and so

$$am' - axm' = a\bar{x}m' - am'(x + \bar{x} - 1)$$

is a proof over $S$ of non-negativity of $am' - axm'$. Hence $\vdash_S^{\mathrm{SA}} am' \geq axm'$, and so also $\vdash_S^{\mathrm{SA}} a \geq am$. □

**Theorem 3.3.6** (Duality theorem)**.** *If $S$ is a closed set of monomials, then for any $p \in \mathbb{R}[S]$,*

$$\sup\{r \in \mathbb{R} : P, Q \vdash_S^{\mathrm{SA}} p \geq r\} = \inf\{E(p) : E \in \mathscr{E}_S^{\mathrm{SA}}(P, Q)\}.$$

*Moreover, if $\mathscr{E}_S^{\mathrm{SA}}(P, Q) \neq \emptyset$, then there is $E \in \mathscr{E}_S^{\mathrm{SA}}(P, Q)$ that achieves the infimum.*

**Theorem 3.3.7** (Soundness and Completeness)**.** *Let $S$ be a closed set of monomials. There is an SA refutation of $P$ and $Q$ over $S$ if and only if there is no SA-pseudoexpectation for $P$ and $Q$ over $S$.*

Finally we prove an analogue of Lemma 3.2.10 for Sherali-Adams. The lemma does not take as nice form as the same lemma for SOS.

**Lemma 3.3.8.** *Let $Q$ be a set of equality constraints of the form $q = 0$, where $q$ is a positive linear combination of monomials, and let $S$ be a set of monomials containing all the monomials appearing in $Q$, all the variables and the empty monomial 1. If there is an SA refutation of $Q$ over $S$, then there is a positive linear combination $s$ of $\mathrm{poly}(|S|)$ many monomials, and $a_q \in \mathbb{R}$ for any $q \in Q$ such that*

$$-1 \equiv s + \sum_{q \in Q} a_q q \mod I_n.$$

*Moreover the monomial size of the proof above is $\mathrm{poly}(|S|)$.*

*Proof.* Consider the convex cone $\mathcal{C}$ of all polynomials $p \in \mathbb{R}[S^2]$ such that

$$p \equiv s + \sum_{q \in Q} a_q q \mod I_n,$$

where $s$ is a positive linear combination of monomials from $S^2$ and binomials of the form $m - m'$, where both $m$ and $m'$ are from $S^2$ and $m$ is a submonomial of $m'$. Note that each binomial in this term has an SA proof of size $\mathrm{poly}(n)$ from $\emptyset$.

Assume towards a contradiction that $-1 \notin \mathcal{C}$. Then, by Lemma 2.4.4, there is some linear functional $L \colon \mathbb{R}[S^2] \to \mathbb{R}$ such that $L(1) = 1$ and $L(p) \geq 0$ for every $p \in \mathcal{C}$.

Our aim is to prove that $L(mq) = 0$ for any $m \in S$. This suffices to prove our: applying $L$ on both sides of the given SA refutation over $S$ yields an immediate contradiction of the form $-1 \geq 0$.

So let $q \in Q$ be arbitrary, write $q = \sum a_\alpha x^\alpha$, and let $m \in S$. Firstly $L(x^\alpha) = 0$ for any $\alpha$, since $q$ is a positive linear combination of monomials and $L(q) = 0$. Secondly, as $x^\alpha - mx^\alpha \in \mathcal{C}$ and $mx^\alpha \in \mathcal{C}$ for any $\alpha$, we have that $0 = L(x^\alpha) \geq L(mx^\alpha) \geq 0$ for any $\alpha$. Hence $L(mq) = 0$. □

## 3.4 Sums-of-Squares p-simulates Polynomial Calculus Resolution over reals – a semantic proof

Finally, we end this chapter by giving a semantic proof of the fact that Sums-of-Squares polynomially simulates PCR/$\mathbb{R}$, Polynomial Calculus Resolution over the reals. This simulation was first proved by Berkholz in [15] via a syntactic proof. Our proof is conceptually rather different and thus might be of independent interest.

We will prove that if there is a PCR/$\mathbb{R}$ refutation of $Q$ using only monomials from a set $S$, then there is an SOS refutation of $Q$ over $S$. We will first prove a version that does not take into account the size of the coefficients in the SOS refutation. This proof highlights the main ideas of the proof, but does not yield the polynomial time simulation. Afterwards we will prove a version that takes also into account the size of the coefficients. The second version will yield the p-simulation of PCR/$\mathbb{R}$ by SOS.

We note that, in a similar manner, one could also prove that SOS, and actually even SA, simulates Resolution. However these proofs have very much the taste of being the known syntactic proofs (see [25, 8]) in new clothes to be of novel interest.

**Lemma 3.4.1.** *Let $Q$ be a set of equality constraints over reals, and suppose there is a PCR/$\mathbb{R}$ refutation of $Q$ using only monomials from a set $S$. Then there is an SOS refutation of $Q$ over $S$.*

*Proof.* Suppose towards a contradiction that there is no SOS refutation of $Q$ over $S$. Then, by Theorem 3.2.8, there is an SOS pseudoexpectation $E$ for $Q$ over $S$. Let $p_1, \ldots, p_\ell$ be a PCR/$\mathbb{R}$ refutation of $Q$ using only monomials from the set $S$. We prove by induction on the structure of the PCR/$\mathbb{R}$ refutation that $E(p_i^2) = 0$ for every $i \in [\ell]$.

The claim is clear for any $q \in Q$, and for any Boolean axiom. Suppose then that $p_i = xp_j$ for some $j < i$ and some variable $x$. Now $p_j^2 - (xp_j)^2 \equiv$

$(p_j - xp_j)^2 \mod J_n$ and so $E((xp_j)^2) \leq E(p_j^2)$. However, by induction assumption $E(p_j^2) = 0$, and so also $E((xp_j)^2) = 0$.

Suppose finally that $p_i = ap_j + bp_k$ for some $j, k < i$, and $a, b \in \mathbb{R}$. Now, by induction assumption, $E(p_j^2) = E(p_k^2) = 0$. Moreover, since $p_j^2 \pm 2p_jp_k + p_k^2 = (p_j \pm p_k)^2$, we have that $|E(2p_jp_k)| \leq E(p_j^2) + E(p_k^2)$, and so $E(p_jp_k) = 0$. Now $E(p_i^2) = E(a^2p_j^2) + E(2abp_jp_k) + E(b^2p_k^2) = 0$.

Now $E(1) = 0$, against the definition of an SOS pseudoexpectation over $S$. Hence there is an SOS refutation of $Q$ over $S$. □

Now we incorporate bounds on the coefficients into the proof. However we lose some of the elegance of the above proof in doing so. We say that a PCR/$\mathbb{R}$ refutation is **$R$-bounded** if all the coefficients appearing in the proof are bounded by $R$ in absolute value and the scalars $a$ and $b$ in the inference step from $p_j$ and $p_k$ to $ap_j + bp_k$ are also bounded by $R$ in absolute value.

We give a bound on the magnitude of the coefficients in the SOS refutation in terms of a bound on the size of coefficients in the given PCR/$\mathbb{R}$ refutation and the height of the refutation. Recall that the height of a PCR/$\mathbb{R}$ proof $p_1, \ldots, p_\ell$ from $Q$ is the length of the longest subsequence $p_{i_1}, \ldots, p_{i_k}$ such that $p_{i_j}$ is a direct antecedent of $p_{i_{j+1}}$ for any $j < k$. Given a PCR/$\mathbb{R}$ proof $p_1, \ldots, p_\ell$ from $Q$, we define the **height of a polynomial** $p_i$ in the proof as follows: if $p_i \in Q$, then $p_i$ is at height 0. If $p_i$ is obtained from some $p_j$ for $j < i$ by a lift with a variable $x$, i.e. $p_i = xp_j$ for some variable $x$, and $p_j$ is at height $h$, then $p_i$ is at height $h + 1$. Finally if $p_i$ is obtained from $p_j$ and $p_k$ for $j, k < i$ by linear combination, i.e. there are some $a, b \in \mathbb{R}$ such that $p_i = ap_j + bp_k$, and $p_j$ and $p_k$ are at heights $h$ and $h'$, respectively, then $p_i$ is at height $\max\{h, h'\} + 1$.

**Lemma 3.4.2.** *Let $Q$ be a set of equality constraints, let $R \geq 2$ and suppose there is an $R$-bounded PCR/$\mathbb{R}$ refutation of $Q$ of height $h$ using only monomials from a set $S$. Then there is an $R^{4h+5}$-bounded SOS refutation of $Q$ over $S$.*

*Proof.* We prove that there is a sum of squares $s$ of polynomials in $\mathbb{R}[S]$ and

$a_q, b_i \in \mathbb{R}$ for every $q \in Q$ and $i \in [n]$ such that $|a_q|, |b_i| \leq R^{4(h+1)}$ and

$$-1 \equiv s + \sum_{q \in Q} a_q q^2 + \sum_{i \in [n]} b_i (x_i + \bar{x}_i - 1)^2 \mod J_n. \tag{3.49}$$

Now (3.49) is an $R^{4h+5}$-bounded SOS refutation of $Q$, since, by assumption, $\|q\|_\infty \leq R$ for any $q \in Q$.

Suppose towards a contradiction that the above claim does not hold. Then the following sets are disjoint:

$$A := \{p \in \mathbb{R}[S^2] : \emptyset \vdash_S^{\text{SOS}} p \geq 0\}$$

and

$$B := \{-1 + \sum_{q \in Q} a_q q^2 + \sum_{i \in [n]} b_i (x_i + \bar{x}_i - 1)^2 : |a_q|, |b_i| \leq R^{4(h+1)}\}.$$

Now $A$ is a convex cone admitting an order unit 1 and $B$ is a convex set. By Theorem 2.4.4 there is a non-trivial linear functional $E \colon \mathbb{R}[S^2] \to \mathbb{R}$ such that $E(1) = 1$ and $E(p) \geq 0$ for every $p \in A$ and $E(q) \leq 0$ for every $q \in B$.

Let $p_1, \ldots, p_\ell$ be an $R$-bounded PCR/$\mathbb{R}$ refutation of $Q$ of height $h$ using only monomials from a set $S$. We prove by induction on the structure of the refutation that for any $p_i$ at height $h'$ we have $E(p_i^2) \leq 1/R^{4(h-h'+1)}$.

The claim holds for any $q \in Q$, since any $q \in Q$ is at height 0 and we have that $-1 + R^{4(h+1)} q^2 \in \mathcal{B}$, and thus $E(-1 + R^{4(h+1)} q^2) \leq 0$, i.e. $E(q^2) \leq 1/R^{4(h+1)}$. Similarly, the claim holds for any Boolean axiom.

Suppose that $p_i$ at height $h' + 1$ is obtained from $p_j$ via a lift with a variable $x$, i.e. $p_i = x p_j$ for some $x$. Now $E((x p_j)^2) \leq E(p_j^2)$, since $p_j^2 - (x p_j)^2 \equiv (p_j - x p_j)^2 \mod J_n$. Now $p_j$ is at height $h'$, and so by induction assumption, $E(p_j^2) \leq 1/R^{4(h-h'+1)}$. Hence $E((x p_j)^2) \leq 1/R^{4(h-h')}$.

Suppose then that $p_i$ at height $h'+1$ is obtained from $p_j$ and $p_k$ via linear combination, i.e. that there are some $a, b \in \mathbb{R}$ such that $p_i = a p_j + b p_k$. Now both $p_j$ and $p_k$ are at most at height $h'$, and so, by induction assumption, $E(p_j^2), E(p_k^2) \leq 1/R^{4(h-h'+1)}$. Secondly, by assumption, $|a|, |b| \leq R$, and so $a^2, b^2 \leq R^2$. Hence $E(a^2 p_j^2), E(b^2 p_k^2) \leq R^2/R^{4(h-h'+1)}$. Thirdly

$$a^2 p_j^2 - 2ab p_j p_k + b^2 p_k^2 = (a p_j - b p_k)^2,$$

and so $E(2abp_jp_k) \leq E(a^2p_j^2) + E(b^2p_k^2)$. Now

$$\begin{aligned} E(p_i^2) &= E(a^2p_j^2) + E(2abp_jp_k) + E(b^2p_k^2) \\ &\leq 2\big(E(a^2p_j^2) + E(b^2p_k^2)\big) \\ &\leq 4R^2/R^{4(h-h'+1)} \\ &\leq R^4/R^{4(h-h'+1)} \\ &= 1/R^{4(h-h')}, \end{aligned}$$

where the fourth line follows, since $R^2 \geq 4$.

Now $E(1) \leq 1/R$ against the assumption that $E(1) = 1$. □

The above lemma together with the proof search algorithm in Section 5.2.2 show that we can find the SOS refutation whose existence is guaranteed by the above lemma in time polynomial in $\langle Q \rangle$, $|S|$, $\log R$ and $h$. Hence we obtain the following corollary.

**Corollary 3.4.3.** *Sums-of-Squares p-simulates Polynomial Calculus Resolution over reals.*

The argument above is clearly not as computationally efficient as the simulation given by the syntactic proof of [15]. However it is a nice illustration of the use of semantic arguments to prove properties of resource-bounded refutations.

# Chapter 4

# Size-degree trade-offs for Sherali-Adams and Sums-of-Squares proofs

In this chapter we prove a size-degree trade-off for SOS and SA refutations. Our results match their analogues for other proof systems that were considered before. Building on the work of [12] and [22] a size-width trade-off theorem was established for Resolution: a Resolution refutation with $s$ many clauses can be converted into one in which all clauses have width $O(\sqrt{n \log s} + k)$, where $k$ is the size of the largest initial clause [14]. The same type of trade-off was also concurrently established for monomial size and degree for the Polynomial Calculus in [46], and later for proof length and rank for LS and LS$^+$ [70], i.e., the proof systems that come out of the Lovász-Schrijver LP and SDP hierarchies [64][1].

Our proof of the trade-off theorem for SA and SOS follows the standard pattern of the previous proofs with one new key ingredient. Suppose $P$ and $Q$ are a sets of inequality and equality constraints that admit a SA/SOS

[1] Besides the proofs of the trade-off results for LS and LS$^+$, the conference version of [70] claims the result for the stronger Sherali-Adams and Lasserre/SOS proof systems, but the claim is made without proof. The very last section of the journal version [70] includes a sketch of a proof that, unfortunately, is an oversimplification of the LS/LS$^+$ argument that cannot be turned into a correct proof. The forthcoming discussion clarifies how our proof is based on, and generalizes, the one for LS/LS$^+$ in [70].

refutation of monomial size $s$. Going back to the main idea from [22], the argument for getting a degree $d$ refutation goes in four steps: (1) find a variable $x$ that appears in many large monomials, (2) set it to a value $b \in \{0,1\}$ to kill all monomials where it appears, (3) induct on the number of variables to get a refutation of $P[x/b]$ and $Q[x/b]$, and a refutation of $P[x/1-b]$ and $Q[x/1-b]$ which, if $s$ is small enough, are of degrees $d-1$ and $d$, respectively, and (4) compose these refutations together to get a degree $d$ refutation of $P$ and $Q$. The main difficulty in making this work for SA and SOS is step (4).

The main difficulty is that, unlike Resolution and the other proof systems which are **deductive** proof systems based on inference rules, the SA and SOS proofs are **formal polynomial identities**. Such proof systems also known as **static** systems. This means that, for SA and SOS, the reasoning it takes to refute $P$ and $Q$ from the degree $d-1$ refutation of $P[x/b]$ and $Q[x/b]$ and the degree $d$ refutation of $P[x/1-b]$ and $Q[x/1-b]$ needs to be witnessed through a single polynomial identity, without exceeding the bound $d$ on the degree. This is challenging because the general simulation of a deductive proof by a static one incurs a degree loss.

In order to overcome this difficulty we turn to pseudoexpectations. One of the key insights of this chapter is that the duality theorem for SA and SOS is instrumental in completing the step (4) in the proof of the trade-off theorem. We reached this conclusion from trying to generalize the proofs for LS and $\text{LS}_+$ from [70] to SA and SOS. In those proofs, the corresponding zero-gap duality theorems are required only for the very special case where $d = 2$ and for deriving linear inequalities from linear constraints. The fact that these hold goes back to the work of Lovász and Schrijver [64].

In Section 4.6 we list some of the applications of the size-degree trade-off for SOS that follow from known degree lower bounds. Among these we include exponential size SOS lower bounds for Tseitin formulas, Knapsack formulas, and optimal integrality gaps for sparse random instances of MAX-3-XOR and MAX-3-SAT. Except for Knapsack formulas, for which size lower bounds follow from an easy random restriction argument applied to the degree lower bounds in [36, 38], these size lower bounds for SOS appear

to be new.

For the proofs below we need to consider the sets of constraints given as **indexed sets of constraints** $P = \{p_1 \geq 0, \ldots, p_\ell \geq 0\}$ and $Q = \{q_1 = 0, \ldots, q_m = 0\}$. Hence SA and SOS proofs of non-negativity of $r$ from $P$ and $Q$ take the form

$$r \equiv s_0 + \sum_{i \in [\ell]} s_i p_i + \sum_{j \in [m]} t_j q_j \mod I_n, \tag{4.1}$$

where $s_i$ is either a polynomial with non-negative coefficients for SA or a sum-of-squares for SOS for each $i \in [\ell] \cup \{0\}$ and $t_j$ is an arbitrary polynomial for each $j \in [m]$

Our main results of this chapter are as follows.

**Theorem 4.0.1.** *For every two natural numbers $n$ and $k$, every indexed sets $P$ and $Q$ of polynomial inequality and equality constraints of degree at most $k$ in $n$ pairs of twin variables, and every positive integers $s$, if there is an SOS refutation from $P$ and $Q$ with at most $s$ many explicit monomials, then there is an SOS refutation of $P$ and $Q$ of degree at most $4\sqrt{2(n+1)\log(s)} + k + 4$.*

**Theorem 4.0.2.** *For every two natural numbers $n$ and $k$, every indexed sets $P$ and $Q$ of polynomial inequality and equality constrains of degree at most $k$ in $n$ pairs of twin variables, and every positive integers $s$, if there is an SA refutation from $P$ and $Q$ with at most $s$ many explicit monomials, then there is an SA refutation of $P$ and $Q$ of degree at most $2\sqrt{2(n+1)\log(s)} + k + 2$.*

Immediate consequences of the above theorems are degree criteria for size lower bounds in Sherali-Adams and Sums-of-Squares:

**Corollary 4.0.3.** *Let $P$ and $Q$ be indexed sets of polynomials of degree at most $k$ in $n$ pairs of twin variables. If $d$ is the minimum degree of an SOS refutation of $P$ and $Q$ and $s$ is the minimum number of explicit monomials in a refutation of $P$ and $Q$, and $d \geq k + 4$, then*

$$s \geq \exp((d - k - 4)^2/(32(n+1))).$$

**Corollary 4.0.4.** *Let $P$ and $Q$ be indexed sets of polynomials of degree at most $k$ in $n$ pairs of twin variables. If $d$ is the minimum degree of an SA refutation of $P$ and $Q$ and $s$ is the minimum number of explicit monomials in an SA refutation of $P$ and $Q$, and $d \geq k+2$, then*

$$s \geq \exp((d-k-2)^2/(8(n+1))).$$

The proofs of Theorems 4.0.1 and 4.0.2 will follow the standard structure of proofs for degree-reduction lemmas for other proof systems, except for some complications in the **unrestricting lemmas.** These difficulties come from the fact that both SA and SOS proofs are static. The main tool around these difficulties is a tight Duality Theorem for degree-bounded proofs with respect to so-called **cut-off functions** as defined next.

## 4.1 Duality modulo cut-off functions

Let $P = \{p_1 \geq 0, \dots p_\ell \geq 0\}$ and $Q = \{q_1 = 0, \dots, q_m = 0\}$ be indexed sets of polynomial constraints. A **cut-off function** for $P$ and $Q$ is a function $c : [\ell + m] \to \mathbb{N}$ with $c(i) \geq \deg(p_i)$ for each $i \leq \ell$, and $c(j) \geq \deg(q_{j-\ell})$ for each $j > \ell$. An SA or SOS proof as in (4.1) has **degree mod** $c$ at most $d$ if $\deg(p) \leq d$, $\deg(s_0) \leq d$, $\deg(s_i) \leq d - c(i)$ for each $i \in [\ell]$, and $\deg(t_j) \leq d - c(j)$ for each $j \in [m]$.

We write $P, Q \vdash^{\mathrm{SA}}_{c,d} q \geq p$ and $P, Q \vdash^{\mathrm{SOS}}_{c,d} q \geq p$ if there is an SA or an SOS proof of non-negativity of $q - p$, respectively, from $P$ and $Q$ of degree mod $c$ at most $d$. An SA-pseudoexpectation for $P$ and $Q$ of degree mod $c$ at most $d$ is a linear functional $E$ from the set of all polynomials of degree at most $d$ such that $E(1) = 1$ and $E(q) \geq 0$ if $P, Q \vdash^{\mathrm{SA}}_{c,d} q \geq 0$. The SOS-pseudoexpectations for $P$ and $Q$ of degree mod $c$ at most $d$ are defined analogously. We denote by $\mathscr{E}^{\mathrm{SA}}_{c,d}(P, Q)$ and $\mathscr{E}^{\mathrm{SOS}}_{c,d}(P, Q)$ the sets of all SA and SOS pseudoexpectations of degree mod $c$ at most $d$, respectively.

Again, by Lemmas 3.2.1 and 3.3.1 and Theorem 2.4.3, we obtain the following Duality Theorems for proofs and pseudoexpectations modulo any cut-off function.

**Theorem 4.1.1.** *Let $d$ be a positive integer, let $P$ and $Q$ be indexed sets of polynomial inequality and equality constrains, let $c$ be a cut-off function for $P$ and $Q$, and let $p$ be a polynomial of degree at most $2d$. Then*

$$\sup\{r \in \mathbb{R} : P, Q \vdash^{\mathrm{SOS}}_{c,2d} p \geq r\} = \inf\{E(p) : E \in \mathscr{E}^{\mathrm{SOS}}_{c,2d}(P, Q)\}.$$

*Moreover, if the set $\mathscr{E}^{\mathrm{SOS}}_{c,2d}(P, Q)$ is non-empty, then there is a pseudoexpectation achieving the infimum.*

**Theorem 4.1.2.** *Let $d$ be a positive integer, let $P$ and $Q$ be indexed sets of polynomial inequality and equality constraints, let $c$ be a cut-off function for $P$ and $Q$, and let $p$ be a polynomial of degree at most $d$. Then*

$$\sup\{r \in \mathbb{R} : P, Q \vdash^{\mathrm{SA}}_{c,d} p \geq r\} = \inf\{E(p) : E \in \mathscr{E}^{\mathrm{SA}}_{c,d}(P, Q)\}.$$

*Moreover, if the set $\mathscr{E}^{\mathrm{SA}}_{c,d}(P, Q)$ is non-empty, then there is a pseudoexpectation achieving the infimum.*

The role of the cut-off function $c$ in our application below will be explained in due time; i.e., after its use in the unrestricting Lemmas 4.3.2 and 4.2.2 below. It is important for the lemmas that follow that the duality theorem is tight in two ways: that they have zero duality gap *and* that they respect the degree; i.e., the degree bound is the same for proofs and pseudoexpectations.

## 4.2 Unrestricting lemmas for Sums-of-Squares

For this section, fix two positive integers $n$ and $d$ for the numbers of pairs of twin variables and degree, respectively. We also fix two indexed sets $P = \{p_1 \geq 0, \ldots, p_\ell \geq 0\}$ and $Q = \{q_1 = 0, \ldots, q_m = 0\}$ of polynomial constraints in the $n$ pairs of twin variables, and a cut-off function $c$ for $P$ and $Q$.

**Lemma 4.2.1.** *Let $x$ be one of the $2n$ variables and let $m$ be a monomial of degree at most $2d-1$. Then $E(x) = 0$ implies $E(xm) = 0$ for any $E \in \mathscr{E}^{\mathrm{SOS}}_{c,2d}(P,Q)$.*

*Proof.* Let $m_1$ and $m_2$ be two monomials of degree at most $d-1$ and $d$, respectively, such that $m = m_1 m_2$. Note first that $E((xm_1)^2) = 0$, since $x - (xm_1)^2 \equiv (x - xm_1)^2 \mod I_n$ and all degrees are at most $2d$. Hence, $0 = E(x) \geq E((xm_1)^2) \geq 0$. Let then $a = E(m_2^2)$ and note that $a \geq 0$. For every positive integer $k$ we have

$$E(xm) \leq \frac{1}{2k}(E(2kxm_1m_2) + E((kxm_1 - m_2)^2)) = \frac{a}{2k},$$
$$E(xm) \geq \frac{1}{2k}(E(2kxm_1m_2) - E((kxm_1 + m_2)^2)) = -\frac{a}{2k},$$

where in both cases the equalities follow from $E((xm_1)^2) = 0$ and $E(m_2^2) = a$. Since $a \geq 0$ and the inequalities hold for every $k > 0$ it must be that $E(xm) = 0$ and the lemma is proved. □

For $q$ a polynomial in the $n$ pairs of twin variables, $i \in [n]$ an index, and $b \in \{0,1\}$ a Boolean value, we denote by $q[i/b]$ the polynomial that results from assigning $x_i$ to $b$ and $\bar{x}_i$ to $1-b$ in $q$. We extend the notation to indexed sets of such polynomials through $P[i/b]$ to mean $\{p_j[i/b] : j \in [\ell]\}$. Note that $p_j[i/b]$ is a polynomial in $n-1$ pairs of twin variables, and its degree is at most the degree of $p_j$.

**Lemma 4.2.2.** *Let $i \in [n]$, let $Q_0$ and $Q_1$ be the extensions of $Q$ with the polynomials $q_{m+1} = x_i$ and $q_{m+1} = \bar{x}_i$, respectively, and let $c'$ be the extension of $c$ that maps $\ell + m + 1$ to 1. The following hold:*

1. *The function $c'$ is a cut-off function for both $P$ and $Q_0$, and $P$ and $Q_1$;* (4.2)
2. *If $P[i/0], Q[i/0] \vdash^{\mathrm{SOS}}_{c,2d} -1 \geq 0$, then $P, Q_0 \vdash^{\mathrm{SOS}}_{c',2d} -1 \geq 0$;* (4.3)
3. *If $P[i/1], Q[i/1] \vdash^{\mathrm{SOS}}_{c,2d} -1 \geq 0$, then $P, Q_1 \vdash^{\mathrm{SOS}}_{c',2d} -1 \geq 0$.* (4.4)

*Proof.* (4.2) is obvious. By symmetry we prove only (4.3). Suppose that $P[i/0], Q[i/0] \vdash^{\text{SOS}}_{c,2d} -1 \geq 0$, say:

$$-1 = s_0 + \sum_{j\in[\ell]} s_j p_j[i/0] + \sum_{k\in[m]} t_k q_k[i/0] \mod I_n \tag{4.5}$$

For $j \in [\ell]$, write $p_j = \sum_{\alpha\in I_j} a_{j,\alpha} x^\alpha$, let $J_j = \{\alpha \in I_j : \alpha_i \geq 1\}$ and $K_j = \{\alpha \in I_j : \alpha_i = 0 \text{ and } \alpha_{n+i} \geq 1\}$ and note that

$$p_j[i/0] = p_j + \sum_{\alpha\in J_j} a_{j,\alpha}(x^\alpha/x_i^{\alpha_i})(-x_i^{\alpha_i}) + \sum_{\alpha\in K_j} a_{j,\alpha}(x^\alpha/\bar{x}_i^{\alpha_{n+i}})(1-\bar{x}_i^{\alpha_{n+i}}).$$

Therefore $p_j[i/0] \equiv p_j + r_j x_i \mod I_n$ where

$$r_j = \sum_{\alpha\in K_j} a_{j,\alpha}(x^\alpha/\bar{x}_i^{\alpha_{n+i}}) - \sum_{\alpha\in J_j} a_{j,\alpha}(x^\alpha/x_i^{\alpha_i}).$$

Note that $\deg(r_j) \leq \deg(p_j) - 1$ since $\alpha_i \geq 1$ for $\alpha \in J_j$ and $\alpha_{n+i} \geq 1$ for $\alpha \in K_j$. Now

$$s_j p_j[i/0] \equiv s_j p_j + s_j r_j x_i \mod I_n.$$

Because $c$ is a cut-off function for $P$ and $Q$ and $c'(j) = c(j)$, we have $\deg(s_j) \leq 2d - c(j) = 2d - c'(j)$. Likewise we have:

$$\deg(s_j r_j) \leq \deg(s_j) + \deg(r_j) \leq 2d - c(j) + \deg(p_j) - 1 \leq 2d - 1.$$

The second inequality follows from the fact that $\deg(r_j) \leq \deg(p_j) - 1$ for all $j \in [m]$, the third inequality follows from the fact that $c$ is a cut-off function for $P$ and $Q$. Hence, $P, Q_0 \vdash^{\text{SOS}}_{c',2d} s_j p_j[i/0]$. A similar argument with $t_j$ and $q_j$ in place of $s_j$ and $p_j$ shows that $P, Q_0 \vdash^{\text{SOS}}_{c',2d} t_j q_j[i/0]$. This gives proofs for all terms in the right-hand side of (4.5), and the proof of the lemma is complete. □

Some comments are in order about the role of the cut-off function in the above proof. First note that, at the semantic level, the constraint $p_j[i/0] \geq 0$ is equivalent to the pair of constraints $p_j \geq 0$ and $x_i = 0$. At the level of syntactic proofs, though, these two representations of the same constraint behave differently: although a lift $s_j p_j[i/0]$ of the restriction $p_j[i/0] \equiv p_j +$

$r_j x_i$ of $p_j$ may have its degree bounded by $2d$, the degree of its direct simulation through $s_j p_j + s_j r_j x_i$ could exceed $2d$. The role of the cut-off function is to restrict the lifts $s_j p_j[i/0]$ in such a way that their simulation through $s_j p_j + s_j r_j x_i$ remains a valid lift of degree at most $2d$; this is the case if, indeed, the allowed lifts $s_j p_j[i/0]$ of $p_j[i/0]$ are those satisfying $\deg(s_j) \leq 2d - c(j)$, where $c(j) \geq \deg(p_j)$. This is why $c$ is designed to depend only on the index $j$ and not on the polynomial indexed by $j$.

**Lemma 4.2.3.** *Let $i \in [n]$, let $Q_0$ and $Q_1$ be the extensions of $Q$ with the polynomials $q_{m+1} = x_i$ and $q_{m+1} = \bar{x}_i$, respectively, and let $c'$ be the extension of $c$ that maps $\ell + m + 1$ to 1. The following hold:*

- *The function $c'$ is a cut-off function for both $P$ and $Q_0$, and $P$ and $Q_1$;* (4.6)
- *If $P, Q_0 \vdash^{\mathrm{SOS}}_{c',2d} -1 \geq 0$, then $E(x_i) > 0$ for any $E \in \mathscr{E}^{\mathrm{SOS}}_{c,2d}(P, Q)$;* (4.7)
- *If $P, Q_1 \vdash^{\mathrm{SOS}}_{c',2d} -1 \geq 0$, then $E(\bar{x}_i) > 0$ for any $E \in \mathscr{E}^{\mathrm{SOS}}_{c,2d}(P, Q)$.* (4.8)

*Proof.* (4.6) is obvious. We prove (4.7); the proof of (4.8) is symmetric.

Suppose towards a contradiction that there is $E \in \mathscr{E}^{\mathrm{SOS}}_{c,2d}(P, Q)$ such that $E(x_i) = 0$. We want to show that $E$ is also in $\mathscr{E}^{\mathrm{SOS}}_{c',2d}(P, Q_0)$. This contradicts the assumption that $P, Q_0 \vdash^{\mathrm{SOS}}_{c',2d} -1 \geq 0$. Let

$$r \equiv s_0 + \sum_{j \in [\ell]} s_j p_j + \sum_{k \in [m]} t_k q_k + t_{m+1} x_i \mod I_n \tag{4.9}$$

be an SOS proof from $P$ and $Q_0$ of degree mod $c'$ at most $2d$. First note that $\deg(t_{m+1}) \leq 2d - c'(m+1) \leq 2d - 1$. Therefore, Lemma 4.2.1 applies to all the monomials of $t_{m+1}$, so that $E(t_{m+1} x_i) = 0$. The rest of (4.9) will get a non-negative value through $E$, since by assumption $E$ is in $\mathscr{E}^{\mathrm{SOS}}_{c,2d}(P, Q)$ and $c$ is $c'$ restricted to $[\ell + m]$. Thus, $E$ is in $\mathscr{E}^{\mathrm{SOS}}_{c',2d}(P, Q_0)$. □

**Lemma 4.2.4.** *Let $i \in [n]$ and assume that $d \geq 2$. The following hold:*

- *If $P[i/0], Q[i/0] \vdash^{\mathrm{SOS}}_{c,2d-2} -1 \geq 0$ and $P[i/1], Q[i/1] \vdash^{\mathrm{SOS}}_{c,2d} -1 \geq 0$, then $P, Q \vdash^{\mathrm{SOS}}_{c,2d} -1 \geq 0$;* (4.10)

- *If* $P[i/0], Q[i/0] \vdash^{\text{SOS}}_{c,2d} -1 \geq 0$ *and* $P[i/1], Q[i/1] \vdash^{\text{SOS}}_{c,2d-2} -1 \geq 0$*, then* $P, Q \vdash^{\text{SOS}}_{c,2d} -1 \geq 0$. (4.11)

*Proof.* First note that $-\bar{x}_i x_i = (x_i^2 - x_i) - x_i(x_i + \bar{x}_i - 1)$, and $d \geq 1$, so that

$$\vdash^{\text{SOS}}_{c,2d} -\bar{x}_i x_i \geq 0. \tag{4.12}$$

We prove (4.10); the proof of (4.11) is entirely analogous.

Assume $P[i/0], Q[i/0] \vdash^{\text{SOS}}_{c,2d-2} -1 \geq 0$. By Lemmas 4.2.2 and 4.2.3 and $d \geq 2$ we have $E(x_i) > 0$ for any $E \in \mathscr{E}^{\text{SOS}}_{c,2d-2}(P, Q)$. Then, by the Duality Theorem 4.1.1, there exist $\epsilon > 0$ such that $P, Q \vdash^{\text{SOS}}_{c,2d-2} x_i \geq \epsilon$. To see this, let $\gamma = \sup\{r \in \mathbb{R} : P, Q \vdash^{\text{SOS}}_{c,2d-2} x_i \geq r\} = \inf\{E(x_i) : E \in \mathscr{E}^{\text{SOS}}_{c,2d-2}(P, Q)\}$. If $\mathscr{E}^{\text{SOS}}_{c,2d-2}(P, Q)$ is empty, then $\gamma = +\infty$ and any $\epsilon > 0$ serves the purpose. If $\mathscr{E}^{\text{SOS}}_{c,2d-2}(P, Q)$ is non-empty, then the Duality Theorem says that the infimum is achieved, hence $\gamma = E(x_i) > 0$ for some $E$ in $\mathscr{E}^{\text{SOS}}_{c,2d-2}(P, Q)$, and $\epsilon = \gamma/2 > 0$ serves the purpose. Using $d \geq 2$ again, $P, Q \vdash^{\text{SOS}}_{c,2d} \bar{x}_i^2 x_i \geq \bar{x}_i^2 \epsilon$, so

$$P, Q \vdash^{\text{SOS}}_{c,2d} \bar{x}_i x_i \geq \bar{x}_i \epsilon. \tag{4.13}$$

Assume also $P[i/1], Q[i/1] \vdash^{\text{SOS}}_{c,2d} -1 \geq 0$. By Lemmas 4.2.2 and 4.2.3 we have $E(\bar{x}_i) > 0$ for any $E \in \mathscr{E}^{\text{SOS}}_{c,2d}(P, Q)$, and this time $d \geq 1$ suffices. By the same argument as before, by the Duality Theorem there exist $\delta > 0$ such that $P, Q \vdash^{\text{SOS}}_{c,2d} \bar{x}_i \geq \delta$. Now $d \geq 1$ suffices to get

$$P, Q \vdash^{\text{SOS}}_{c,2d} \bar{x}_i \epsilon \geq \delta \epsilon. \tag{4.14}$$

Adding (4.12), (4.13) and (4.14) gives $P, Q \vdash^{\text{SOS}}_{c,2d} 0 \geq \delta\epsilon$, i.e., $P, Q \vdash^{\text{SOS}}_{c,2d} -1 \geq 0$. □

## 4.3 Unrestricting lemmas for Sherali-Adams

For this section, fix again two positive integers $n$ and $d$, two indexed sets $P = \{p_1 \geq 0, \ldots, p_\ell \geq 0\}$ and $Q = \{q_1 = 0, \ldots, q_m = 0\}$ of polynomial

constraints in the $n$ pairs of twin variables, and a cut-off function$c$ for $P$ and $Q$.

The proofs for the unrestricting lemmas for SA are mostly the same as in the case of SOS. We do highlight the important differences in the proofs between the two systems when they appear. First important difference comes in the following lemma, which is an analogue of Lemma 4.2.1. For Sherali-Adams the proof of the lemma is much less involved than for Sums-of-Squares.

**Lemma 4.3.1.** *Let $x$ be one of the $2n$ variables and let $m$ be a monomial of degree at most $d-1$. Then $E(x) = 0$ implies $E(xm) = 0$ for any $E \in \mathscr{E}^{\mathrm{SA}}_{c,d}(P,Q)$.*

*Proof.* Let $m = \prod_{i\in[d-1]} y_i$. The proof follows, since Sherali-Adams has a direct proof of $x - xm$ by the following telescoping sum:

$$x - x\prod_{i\in[d-1]} y_i \equiv x\bar{y}_i + xy_1\bar{y}_2 + \cdots x\prod_{i\in[d-2]} y_i\bar{y}_{d-1} \mod I_n.$$

Hence $0 = E(x) \geq E(xm)$. On the other hand $E(xm) \geq 0$, and so $E(xm) = 0$. □

The following two lemmas are analogues of Lemmas 4.2.2 and 4.2.3 for Sherali-Adams, and the proofs are practically the same.

**Lemma 4.3.2.** *Let $i \in [n]$, let $Q_0$ and $Q_1$ be the extensions of $Q$ with the polynomials $q_{m+1} = x_i$ and $q_{m+1} = \bar{x}_i$, respectively, and let $c'$ be the extension of $c$ that maps $\ell + m + 1$ to 1. The following hold:*

- *The function $c'$ is a cut-off function for both $P$ and $Q_0$, and $P$ and $Q_1$;* (4.15)
- *If $P[i/0], Q[i/0] \vdash^{\mathrm{SA}}_{c,d} -1 \geq 0$, then $P, Q_0 \vdash^{\mathrm{SA}}_{c'd} -1 \geq 0$;* (4.16)
- *If $P[i/1], Q[i/1] \vdash^{\mathrm{SA}}_{c,d} -1 \geq 0$, then $P, Q_1 \vdash^{\mathrm{SA}}_{c',d} -1 \geq 0$.* (4.17)

*Proof.* (4.15) is obvious. By symmetry we prove only (4.16). Suppose that $P[i/0], Q[i/0] \vdash^{\mathrm{SA}}_{c,d} -1 \geq 0$, say:

$$-1 = s_0 + \sum_{j\in[\ell]} s_j p_j[i/0] + \sum_{k\in[m]} t_k q_k[i/0] \mod I_n \tag{4.18}$$

For $j \in [\ell]$, write $p_j = \sum_{\alpha \in I_j} a_{j,\alpha} x^\alpha$, let $J_j = \{\alpha \in I_j : \alpha_i \geq 1\}$ and $K_j = \{\alpha \in I_j : \alpha_i = 0 \text{ and } \alpha_{n+i} \geq 1\}$ and note that

$$p_j[i/0] = p_j + \sum_{\alpha \in J_j} a_{j,\alpha}(x^\alpha / x_i^{\alpha_i})(-x_i^{\alpha_i}) + \sum_{\alpha \in K_j} a_{j,\alpha}(x^\alpha / \bar{x}_i^{\alpha_{n+i}})(1 - \bar{x}_i^{\alpha_{n+i}}).$$

Therefore $p_j[i/0] \equiv p_j + r_j x_i \mod I_n$ where

$$r_j = \sum_{\alpha \in K_j} a_{j,\alpha}(x^\alpha / \bar{x}_i^{\alpha_{n+i}}) - \sum_{\alpha \in J_j} a_{j,\alpha}(x^\alpha / x_i^{\alpha_i}).$$

Note that $\deg(r_j) \leq \deg(p_j) - 1$ since $\alpha_i \geq 1$ for $\alpha \in J_j$ and $\alpha_{n+i} \geq 1$ for $\alpha \in K_j$. Now

$$s_j p_j[i/0] \equiv s_j p_j + s_j r_j x_i \mod I_n.$$

Because $c$ is a cut-off function for $P$ and $Q$ and $c'(j) = c(j)$, we have $\deg(s_j) \leq d - c(j) = d - c'(j)$. Likewise we have:

$$\deg(s_j r_j) \leq \deg(s_j) + \deg(r_j) \leq d - c'(j) + \deg(p_j) - 1 \leq d - 1.$$

The second inequality follows from the fact that $\deg(r_j) \leq \deg(p_j) - 1$ for all $j \in [m]$, the third inequality follows from the fact that $c$ is a cut-off function for $P$ and $Q$. Hence, $P, Q_0 \vdash^{\mathrm{SA}}_{c',d} s_j p_j[i/0]$. A similar argument with $t_j$ and $q_j$ in place of $s_j$ and $p_j$ shows that $P, Q_0 \vdash^{\mathrm{SA}}_{c',d} t_j q_j[i/0]$. This gives proofs for all terms in the right-hand side of (4.18), and the proof of the lemma is complete. □

**Lemma 4.3.3.** *Let $i \in [n]$, let $Q_0$ and $Q_1$ be the extensions of $Q$ with the polynomials $q_{m+1} = x_i$ and $q_{m+1} = \bar{x}_i$, respectively, and let $c'$ be the extension of $c$ that maps $\ell + m + 1$ to 1. The following hold:*

- *The function $c'$ is a cut-off function for both $P$ and $Q_0$, and $P$ and $Q_1$;* (4.19)
- *If $P, Q_0 \vdash^{\mathrm{SA}}_{c',d} -1 \geq 0$, then $E(x_i) > 0$ for any $E \in \mathscr{E}^{\mathrm{SA}}_{c,d}(P, Q)$;* (4.20)
- *If $P, Q_1 \vdash^{\mathrm{SA}}_{c',d} -1 \geq 0$, then $E(\bar{x}_i) > 0$ for any $E \in \mathscr{E}^{\mathrm{SA}}_{c,d}(P, Q)$.* (4.21)

*Proof.* (4.19) is obvious. We prove (4.20); the proof of (4.21) is symmetric. Suppose towards a contradiction that there is $E \in \mathscr{E}^{\mathrm{SA}}_{c,d}(P, Q)$ such that

$E(x_i) = 0$. We want to show that $E$ is also in $\mathscr{E}^{\mathrm{SA}}_{c',d}(P, Q_0)$. This contradicts the assumption that $P, Q_0 \vdash^{\mathrm{SA}}_{c',d} -1 \geq 0$. Let

$$r \equiv s_0 + \sum_{j\in[\ell]} s_j p_j + \sum_{k\in[m]} t_k q_k + t_{m+1} x_i \mod I_n \tag{4.22}$$

be an SA proof from $P$ and $Q_0$ of degree mod $c'$ at most $d$. First note that $\deg(t_{m+1}) \leq d - c'(m+1) \leq 2d - 1$. Therefore, Lemma 4.3.1 applies to all the monomials of $t_{m+1}$, so that $E(t_{m+1}x_i) = 0$. The rest of (4.22) will get a non-negative value through $E$, since by assumption $E$ is in $\mathscr{E}^{\mathrm{SA}}_{c,d}(P, Q)$ and $c$ is $c'$ restricted to $[\ell + m]$. Thus, $E$ is in $\mathscr{E}^{\mathrm{SA}}_{c'd}(P, Q_0)$. □

Finally we obtain the following analogue of Lemma 4.2.4.

**Lemma 4.3.4.** *Let $i \in [n]$ and assume that $d \geq 2$. The following hold:*

- *If $P[i/0], Q[i/0] \vdash^{\mathrm{SA}}_{c,d-1} -1 \geq 0$ and $P[i/1], Q[i/1] \vdash^{\mathrm{SA}}_{c,d} -1 \geq 0$, then $P, Q \vdash^{\mathrm{SA}}_{c,d} -1 \geq 0$;* (4.23)
- *If $P[i/0], Q[i/0] \vdash^{\mathrm{SA}}_{c,d} -1 \geq 0$ and $P[i/1], Q[i/1] \vdash^{\mathrm{SA}}_{c,d-1} -1 \geq 0$, then $P, Q \vdash^{\mathrm{SA}}_{c,d} -1 \geq 0$.* (4.24)

*Proof.* First note that $-\bar{x}_i x_i = (x_i^2 - x_i) - x_i(x_i + \bar{x}_i - 1)$, and $d \geq 2$, so that

$$\vdash^{\mathrm{SA}}_{c,d} -\bar{x}_i x_i \geq 0. \tag{4.25}$$

We prove (4.23); the proof of (4.24) is entirely analogous.

Assume $P[i/0], Q[i/0] \vdash^{\mathrm{SA}}_{c,d-1} -1 \geq 0$. By Lemmas 4.3.2 and 4.3.3 and $d \geq 2$ we have $E(x_i) > 0$ for any $E \in \mathscr{E}^{\mathrm{SA}}_{c,d-1}(P, Q)$. Then, by the Duality Theorem 4.1.2, there exist $\epsilon > 0$ such that $P, Q \vdash^{\mathrm{SA}}_{c,d-1} x_i \geq \epsilon$. To see this, let $\gamma = \sup\{r \in \mathbb{R} : P, Q \vdash^{\mathrm{SA}}_{c,d-1} x_i \geq r\} = \inf\{E(x_i) : E \in \mathscr{E}^{\mathrm{SA}}_{c,d-1}(P, Q)\}$. If $\mathscr{E}^{\mathrm{SA}}_{c,d-1}(P, Q)$ is empty, then $\gamma = +\infty$ and any $\epsilon > 0$ serves the purpose. If $\mathscr{E}^{\mathrm{SA}}_{c,d-1}(P, Q)$ is non-empty, then the Duality Theorem says that the infimum is achieved, hence $\gamma = E(x_i) > 0$ for some $E$ in $\mathscr{E}^{\mathrm{SA}}_{c,d-1}(P, Q)$, and $\epsilon = \gamma/2 > 0$ serves the purpose. Using $d \geq 2$ again, we obtain that

$$P, Q \vdash^{\mathrm{SA}}_{c,d} \bar{x}_i x_i \geq \bar{x}_i \epsilon. \tag{4.26}$$

Assume also $P[i/1], Q[i/1] \vdash^{\mathrm{SA}}_{c,d} -1 \geq 0$. By Lemmas 4.3.2 and 4.3.3 we have $E(\bar{x}_i) > 0$ for any $E \in \mathscr{E}^{\mathrm{SA}}_{c,d}(P,Q)$, and this time $d \geq 1$ suffices. By the same argument as before, by the Duality Theorem there exist $\delta > 0$ such that $P, Q \vdash^{\mathrm{SA}}_{c,d} \bar{x}_i \geq \delta$. Now $d \geq 1$ suffices to get

$$P, Q \vdash^{\mathrm{SA}}_{c,d} \bar{x}_i \epsilon \geq \delta\epsilon. \tag{4.27}$$

Adding (4.25), (4.26) and (4.27) gives $P, Q \vdash^{\mathrm{SA}}_{c,d} 0 \geq \delta\epsilon$, i.e., $P, Q \vdash^{\mathrm{SA}}_{c,d} -1 \geq 0$. □

## 4.4 Size-degree trade-off for Sums-of-Squares

We need one more technical concept: an SOS proof as in (4.1) is **multilinear** if $s_0$ and $s_j$ are sums of squares of multilinear polynomials for each $j \in [\ell]$, and $t_k$ is a multilinear polynomial for each $k \in [m]$.

**Lemma 4.4.1.** *For every positive integer $s$ and any indexed sets $P$ and $Q$ of polynomial inequality and equality constraints, if there is an SOS refutation from $P$ and $Q$ with at most $s$ many distinct significant monomials, then there is a multilinear SOS refutation from $P$ and $Q$ with at most $s$ many distinct significant monomials.*

*Proof.* Let $P = \{p_1 \geq 0, \ldots, p_\ell \geq 0\}$ and $Q = \{q_1 = 0, \ldots, q_m = 0\}$ and suppose that there is a refutation from $P$ and $Q$ as in (4.1), with $s_0 = \sum_{i=1}^{k_0} r_{i,0}^2$ and $s_j = \sum_{i=1}^{k_j} r_{i,j}^2$ for $j \in [\ell]$, where the number of distinct monomials among the $r_{i,0}$, $r_{i,j}$ and $t_k$ is at most $s$. For each polynomial $r$ let $\bar{r}$ be its direct multilinearization; i.e., each power $x^l$ with $l \geq 2$ that appears in $r$ is replaced by $x$. It is obvious that $r \equiv \bar{r} \mod I_n$ and also $r^2 \equiv \bar{r}^2 \mod I_n$, where $n$ is the number of pairs of twin variables in $P$ and $Q$. Moreover, the number of distinct monomials among $\bar{r}_{i,0}$, $\bar{r}_{i,j}$ and $\bar{t}_k$ does not exceed $s$. Thus, setting $s'_0 = \sum_{i=1}^{k_0} \bar{r}_{i,0}^2$, $s'_j = \sum_{i=1}^{k_J} \bar{r}_{i,J}^2$ and $t'_k = \bar{t}_k$ we get

$$-1 \equiv s'_0 + \sum_{j\in[\ell]} s'_j p_j + \sum_{k\in[m]} t'_k q_k \mod I_n. \tag{4.28}$$

It follows that $P$ $Q$ has a multilinear refutation with at most $s$ distinct significant monomials. □

Theorem 4.0.1 will be a consequence of the following lemma for a suitable choice of $d$ and $c$:

**Lemma 4.4.2.** *For every natural number $n$, any indexed sets $P$ and $Q$ of polynomial inequality and equality constraints in $n$ pairs of twin variables, every cut-off function $c$ for $P$ and $Q$, every real $s \geq 1$ and every positive integer $d$, if there is a multilinear SOS refutation from $P$ and $Q$ with at most $s$ many distinct significant monomials of degree at least $d$, then there is an SOS refutation from $P$ and $Q$ of degree mod $c$ at most $2d' + 2d''$, where $d' = d + \lfloor 2(n+1)\log(s)/d \rfloor$ and $d'' = \max\{1, \lceil (\max c)/2 \rceil\}$.*

*Proof.* The proof is an induction on $n$. Let $P$ and $Q$ be indexed sets of polynomials in $n$ pairs of twin variables, let $c$ be a cut-off function for $P$ and $Q$, let $s \geq 1$ be a real, let $d$ be a positive integer, and let $\Pi$ be a multilinear refutation of $P$ and $Q$ with at most $s$ many distinct significant monomials of degree at least $d$.

For $n = 0$ the statement is true because $2d'' \geq 2\lceil (\max c)/2 \rceil \geq \max c$. Assume now that $n \geq 1$. Let $t \leq s$ be the exact number of distinct significant monomials of degree at least $d$ in $\Pi$. The total number of variable occurrences in such monomials is at least $dt$. Therefore, there exists one among the $2n$ variables that appears in at least $dt/2n$ of the significant monomials of degree at least $d$. Let $i \in [n]$ be the index of such a variable, basic or twin. If it is basic, let $a = 0$. If it is twin, let $a = 1$. Our goal is to show that

$$P[i/a], Q[i/a] \vdash^c_{2d'+2d''-2} -1 \geq 0 \text{ and } P[i/1-a], Q[i/1-a] \vdash^c_{2d'+2d''} -1 \geq 0, \tag{4.29}$$

for $d'$ and $d''$ as stated in the lemma. If we achieve so, then $d' + d'' \geq 2$ because $d' \geq d \geq 1$ and $d'' \geq 1$, so Lemma 4.2.4 applies on (4.29) to give $P, Q \vdash^c_{2d'+2d''} -1 \geq 0$, which is what we are after.

Consider $P[i/a]$ and $Q[i/a]$ first. These are sets of polynomials on $n-1$ pairs of twin variables, and $\Pi[i/a]$ is a multilinear refutation of $P[i/a]$ and

$Q[i/a]$ that has at most $s' := t(1 - d/2n)$ distinct significant monomials of degree at least $d$. Moreover $c$ is a cut-off function for the sets. We distinguish the cases $s' < 1$ and $s' \geq 1$. If $s' < 1$, then all significant monomials in $\Pi[i/a]$ have degree at most $d - 1$. Since $2d'' \geq \max c$, this refutation has degree mod $c$ at most $2(d-1)+2d'' \leq 2d'+2d''-2$. This gives the first part of (4.29). If $s' \geq 1$, then first note that $d < 2n$. Moreover, the induction hypothesis applied to $P[i/a]$,$Q[i/a]$ and $s'$, and the same $c$ and $d$, gives that there is a refutation of $P[i/a]$ and $Q[i/a]$ of degree mod $c$ at most $2d_a + 2d''$, where

$$d_a = d + \lfloor 2n \log(t(1 - d/2n))/d \rfloor \leq d + \lfloor 2(n+1) \log(s)/d \rfloor - 1. \quad (4.30)$$

Here we used the inequality $\log(1 + x) \leq x$ which holds true for every real $x > -1$, and the fact that $d < 2n$. This gives the first part of (4.29) since $d_a \leq d' - 1$.

Consider $P[i/1 - a]$ and $Q[i/1 - a]$ next. In this case, the best we can say is that $c$ is still a cut-off function for the sets, and that $\Pi[i/1 - a]$ is a multilinear refutation of the sets that still has at most $s$ many distinct significant monomials of degree at least $d$. But $P[i/1 - a]$ and $Q[i/1 - a]$ have at most $n - 1$ pairs of twin variables, so the induction hypothesis applies. Applied to the same $c$, $s$ and $d$, it gives that there is a refutation of $P[i/1 - a]$ and $Q[i/1 - a]$ of degree mod $c$ at most $2d_{1-a} + 2d''$, where

$$d_{1-a} = d + \lfloor 2n \log(s)/d \rfloor \leq d + \lfloor 2(n+1) \log(s)/d \rfloor. \quad (4.31)$$

This gives the second part of (4.29) since $d_{1-a} \leq d'$. The proof is complete. □

We are ready now to prove Theorem 4.0.1. We will actually prove the following slightly stronger statement.

**Theorem 4.4.3.** *For every two natural numbers $n$ and $k$, every indexed sets $P$ and $Q$ of polynomials of degree at most $k$ with $n$ pairs of twin variables, and every positive integers $s$, if there is an SOS refutation from $P$ and $Q$ with at most $s$ many **distinct significant monomials**, then there is an SOS refutation of $P$ and $Q$ of degree at most $4\sqrt{2(n+1)\log(s)} + k + 4$.*

*Proof.* Assume that there is a refutation of $P$ and $Q$ with at most $s$ many distinct significant monomials. Applying Lemma 4.4.1 we get a multilinear refutation with at most $s$ many distinct significant monomials, and hence with at most $s$ many distinct significant monomials of degree at least $d_0$, for any $d_0$ of our choice. We choose

$$d_0 := \lfloor \sqrt{2(n+1)\log(s)} \rfloor + 1. \tag{4.32}$$

By assumption $s \geq 1$ and we chose $d_0$ in such a way that $d_0 \geq 1$. Thus, Lemma 4.4.2 applies to any cut-off function $c$ for $Q$, in particular for the cut-off function that is $k$ everywhere. This gives a refutation of degree mod $c$ at most $2d' + k + 2$ with

$$d' \leq d_0 + 2(n+1)\log(s)/d_0 \leq 2\sqrt{2(n+1)\log(s)} + 1. \tag{4.33}$$

Since a proof of degree mod $c$ at most $2d' + k + 2$ is also a proof of standard degree at most $2d' + k + 2$, the proof is complete. □

### 4.4.1 Size-degree trade-offs for Positivstellensatz proofs

Positivstellensatz proof system is an extension of Sums-of-Squares, defined originally in [40]. A Positivstellensatz proof of non-negativity of $r$ from $P$ and $Q$ is a polynomial equality of the form

$$r = \sum_{i\in[k]} r_i^2 + \sum_{R\subseteq P} \sum_{i\in[k_R]} r_{i,R}^2 \prod_{p\in R} p + \sum_{q\in Q} t_q q \\ + \sum_{i\in[n]} \big(u_i(x_i^2 - x_i) + v_i(x_i + \bar{x}_i - 1)\big). \tag{4.34}$$

Note that when $|P| \leq 1$, the Positivstellensatz proof 4.34 is an SOS proof. However, with the power of multiplying inequality constraints together, one can possibly obtain proofs smaller than in SOS.

We say that the PS proof 4.34 has **product-width** at most $w$ if for any $R$ with $|R| > w$, $r_{i,R} = 0$ for any $i \in [k_R]$. Now any PS proof from $P$ and $Q$ of product-width at most $w$ can be considered as an SOS proof

from the sets $P^w$ and $Q$, where $P^w = \{\prod_{p\in R} p : R \subseteq P, |R| \leq w\}$. Now the set of constraints $P^w$ has degree at most $kw$, and hence an immediate consequence of the size-degree trade-off for SOS is the following size-degree trade-off for Positivstellensatz proofs with bounded product-width.

**Theorem 4.4.4.** *For every two natural numbers $n$ and $k$, every indexed sets $P$ and $Q$ of polynomial inequality and equality constrains of degree at most $k$ in $n$ pairs of twin variables, and every two positive integers $s$ and $w$, if there is a PS refutation from $Q$ of product-width at most $w$ and monomial size at most $s$, then there is a PS refutation from $Q$ of product-width at most $w$ and degree at most $4\sqrt{2(n+1)\log(s)} + kw + 4$.*

In the paper [6] we painstakingly proved this form of the result from first premises. The proof above simplifies the proof slightly. It is still open whether a similar size-degree trade-off holds for Positivstellensatz proofs with unbounded product-width.

## 4.5 Size-degree trade-off for Sherali-Adams

We say that an SA proof as in (4.1) is **multilinear** if $s_0$ and $s_j$ are positive linear combinations of multilinear monomials for each $j \in [\ell]$, and $t_k$ is a multilinear polynomial for each $k \in [m]$.

**Lemma 4.5.1.** *For every positive integer $s$ and any indexed sets $P$ and $Q$ of polynomial inequality and equality constraints, if there is an SA refutation from $P$ and $Q$ with at most $s$ many distinct significant monomials, then there is a multilinear SA refutation from $P$ and $Q$ with at most $s$ many distinct significant monomials.*

*Proof.* Let $P = \{p_1 \geq 0, \ldots, p_\ell \geq 0\}$ and $Q = \{q_1 = 0, \ldots, q_m = 0\}$ and suppose that there is a refutation from $P$ and $Q$ as in (4.1), where the number of distinct significant monomials is at most $s$. For each polynomial $r$ let $\bar{r}$ be its direct multilinearization; i.e., each power $x^l$ with $l \geq 2$ that appears in $r$ is replaced by $x$. It is obvious that $r \equiv \bar{r} \mod I_n$, where $n$ is

the number of pairs of twin variables in $P$ and $Q$. Moreover, the number of distinct significant monomials among $\bar{s}_0$, $\bar{s}_j$ and $\bar{t}_k$ does not exceed $s$. Now

$$-1 \equiv \bar{s}_0 + \sum_{j\in[\ell]} \bar{s}_j p_j + \sum_{k\in[m]} \bar{t}_k q_k \mod I_n, \tag{4.35}$$

and so $P$ and $Q$ has a multilinear refutation with at most $s$ distinct significant monomials. □

Theorem 4.0.2 will again be a consequence of the following lemma for a suitable choice of $d$ and $c$:

**Lemma 4.5.2.** *For every natural number $n$, any indexed sets $P$ and $Q$ of polynomial inequality and equality constrains in $n$ pairs of twin variables, every cut-off function $c$ for $P$ and $Q$, every real $s \geq 1$ and every positive integers $d$, if there is a multilinear SA refutation of $P$ and $Q$ with at most $s$ many distinct signicant monomials of degree at least $d$, then there is an SA refutation from $P$ and $Q$ of degree mod $c$ at most $d' + d''$, where $d' = d + \lfloor 2(n+1)\log(s)/d \rfloor$ and $d'' = \max\{1, \max c\}$.*

*Proof.* The proof is an induction on $n$. Let $P$ and $Q$ be indexed sets of polynomials in $n$ pairs of twin variables, let $c$ be a cut-off function for $P$ and $Q$, let $s \geq 1$ be a real, let $d$ be a positive integer, and let $\Pi$ be a multilinear refutation of $P$ and $Q$ with at most $s$ many distinct significant monomials of degree at least $d$.

For $n = 0$ the statement is true because $d'' \geq \max c$. Assume now that $n \geq 1$. Let $t \leq s$ be the exact number of distinct significant monomials of degree at least $d$ in $\Pi$. The total number of variable occurrences in such monomials is at least $dt$. Therefore, there exists one among the $2n$ variables that appears in at least $dt/2n$ of the distinct significant monomials of degree at least $d$. Let $i \in [n]$ be the index of such a variable, basic or twin. If it is basic, let $a = 0$. If it is twin, let $a = 1$. Our goal is to show that

$$P[i/a], Q[i/a] \vdash^{\mathrm{SA}}_{c,d'+d''-1} -1 \geq 0 \text{ and } P[i/1-a], Q[i/1-a] \vdash^{\mathrm{SA}}_{c,d'+d''} -1 \geq 0, \tag{4.36}$$

for $d'$ and $d''$ as stated in the lemma. If we achieve so, then $d' + d'' \geq 2$ because $d' \geq d \geq 1$ and $d'' \geq 1$, so Lemma 4.3.4 applies on (4.36) to give $P, Q \vdash^{\mathrm{SA}}_{c,d'+d''} -1 \geq 0$, which is what we are after.

Consider $P[i/a]$ and $Q[i/a]$ first. These are sets of polynomials on $n-1$ pairs of twin variables, and $\Pi[i/a]$ is a multilinear refutation of $P[i/a]$ and $Q[i/a]$ that has at most $s' := t(1 - d/2n)$ distinct significant monomials of degree at least $d$. Moreover $c$ is a cut-off function for the sets. We distinguish the cases $s' < 1$ and $s' \geq 1$. If $s' < 1$, then all significant monomials in $\Pi[i/a]$ have degree at most $d-1$. Since $d'' \geq \max c$, this refutation has degree mod $c$ at most $(d-1) + d'' \leq d' + d'' - 1$. This gives the first part of (4.36). If $s' \geq 1$, then first note that $d < 2n$. Moreover, the induction hypothesis applied to $P[i/a]$,$Q[i/a]$ and $s'$, and the same $c$ and $d$, gives that there is an SA refutation of $P[i/a]$ and $Q[i/a]$ of degree mod $c$ at most $d_a + d''$, where

$$d_a = d + \lfloor 2n \log(t(1 - d/2n))/d \rfloor \leq d + \lfloor 2(n+1) \log(s)/d \rfloor - 1. \quad (4.37)$$

Here we used the inequality $\log(1+x) \leq x$ which holds true for every real $x > -1$, and the fact that $d < 2n$. This gives the first part of (4.36) since $d_a \leq d' - 1$.

Consider $P[i/1-a]$ and $Q[i/1-a]$ next. In this case, the best we can say is that $c$ is still a cut-off function for the sets, and that $\Pi[i/1-a]$ is a multilinear refutation of the sets that still has at most $s$ many distinct significant monomials of degree at least $d$. But $P[i/1-a]$ and $Q[i/1-a]$ have at most $n-1$ pairs of twin variables, so the induction hypothesis applies. Applied to the same $c$, $s$ and $d$, it gives that there is an SA refutation of $P[i/1-a]$ and $Q[i/1-a]$ of degree mod $c$ at most $d_{1-a} + d''$, where

$$d_{1-a} = d + \lfloor 2n \log(s)/d \rfloor \leq d + \lfloor 2(n+1) \log(s)/d \rfloor. \quad (4.38)$$

This gives the second part of (4.36) since $d_{1-a} \leq d'$. The proof is complete. □

Again instead of proving Theorem 4.0.2, we prove the following slightly stronger statement from which Theorem 4.0.2 follows directly.

**Theorem 4.5.3.** *For any two natural numbers $n$ and $k$, any indexed sets $P$ and $Q$ of polynomial in $n$ of degree at most $k$ in $n$ pairs of twin variables, and every positive integer $s$, if there is an SA refutation of $P$ and $Q$ with at most $s$ many* ***distinct significant monomials****, then there is an SA refutation of $P$ and $Q$ of degree at most $2\sqrt{2(n+1)\log(s)} + k + 2$*

*Proof.* Assume that there is a refutation of $P$ and $Q$ with at most $s$ many distinct significant monomials. Applying Lemma 4.4.1 we get a multilinear refutation with at most $s$ many distinct significant monomials, and hence with at most $s$ many distinct significant monomials of degree at least $d_0$, for any $d_0$ of our choice. We choose

$$d_0 := \lfloor \sqrt{2(n+1)\log(s)} \rfloor + 1. \tag{4.39}$$

By assumption $s \geq 1$ and we chose $d_0$ in such a way that $d_0 \geq 1$. Thus, Lemma 4.5.2 applies to any cut-off function $c$ for $P$ and $Q$, in particular for the cut-off function that is $k$ everywhere. This gives a refutation of degree mod $c$ at most $d' + k + 1$ with

$$d' \leq d_0 + 2(n+1)\log(s)/d_0 \leq 2\sqrt{2(n+1)\log(s)} + 1. \tag{4.40}$$

Since a proof of degree mod $c$ at most $d' + k + 1$ is also a proof of standard degree at most $d' + k + 1$, the proof is complete. □

## 4.6 Applications

The obvious targets for applications of Theorems 4.0.2 and 4.0.1 are the examples from the literature that are known to require linear degree to refute. For some of them, such as the Knapsack, the SOS size lower bound that follows was already known [38]. For some others, the applications of the Theorems yields a new result. This section concentrates on SOS as the stronger of the two systems.

### 4.6.1 Tseitin, Knapsack, and Random CSPs

The first set of examples that come to mind are the Tseitin formulas: If $G_n = (V, E)$ is an $n$-vertex graph from a family $\{G_n : n \in \mathbb{N}\}$ of constant degree regular expander graphs, then the formula $\mathrm{TS}_n$ has one Boolean variable $x_e$ for each $e \in E$ and one parity constraint $\sum_{e:u\in e} x_e = 1 \mod 2$ for each $u \in V$. Whenever the degree $d$ of the graphs is even, this is unsatisfiable when $n$ is odd. In the encoding of the constraints given by the system of polynomial equations $Q = \{\prod_{e:u\in e}(1 - 2x_e) = -1 : u \in V\}$, the Tseitin formulas $\mathrm{TS}_n$ were shown to require degree $\Omega(n)$ to refute in SOS in Corollary 1 from [37]. Since the number of variables of $\mathrm{TS}_n$ is $dn/2$, the constraints in $Q$ are equations of degree $d$, and $d$ is a constant, Theorem **??** gives:

**Corollary 4.6.1.** *There exists $\epsilon \in \mathbb{R}_{>0}$ such that for every sufficiently large $n \in \mathbb{N}$, every SOS refutation of $\mathrm{TS}_n$ has monomial size at least $2^{\epsilon n}$.*

Among the semialgebraic proof systems in the literature, exponential size lower bounds for Tseitin formulas were known before for a proof system called static $\mathrm{LS}_+$ in [38, 47]. Up to at most doubling the degree, this can be seen as the subsystem of SOS in which every square $s_j$ is of the very special form

$$s_j = \Big(\Big(\sum_{i\in[n]} a_i x_i + b\Big) \prod_{i\in I} x_i \prod_{j\in J}(1 - x_j)\Big)^2.$$

A second set of examples are the Knapsack equations $2x_1 + \cdots + 2x_n = k$, which are unsatisfiable for odd integers $k$. We denote them $\mathrm{KS}_{n,k}$. These are known to require degree $\Omega(\min\{k, 2n - k\})$ to refute in SOS [36]. Since the number of variables is $n$ and the degree is one, Theorem 4.0.1 gives an exponential size $2^{\Omega(n)}$ lower bound when $k = n$. For this example, an exponential size lower bound for SOS was also proved in Theorem 9.1 from [38] when $k = \Theta(n)$, so this result is not new. We state the precise relationship that the degree-reduction theorem gives in terms of $n$ and $k$, which yields superpolynomial lower bounds for $k = \omega(\sqrt{n \log n})$.

**Corollary 4.6.2.** *There exist $\epsilon \in \mathbb{R}_{>0}$ such that for every sufficiently large $n \in \mathbb{N}$ and $k \in [n]$, every SOS refutation of $\mathrm{KS}_{n,k}$ has monomial size at least $2^{\epsilon k^2/n}$.*

The third set of examples come from sparse random instances of constraint satisfaction problems. As far as we know, monomial size lower bounds for these examples do not follow from earlier published work without using our result, so we give the details.

When $C$ is a clause with $k$ literals, say $x_{i_1} \vee \cdots \vee x_{i_\ell} \vee \bar{x}_{i_{\ell+1}} \vee \cdots \vee \bar{x}_{i_k}$, we write $p_C$ for the unique multilinear polynomial on the variables $x_{i_1}, \ldots, x_{i_k}$ of $C$ that evaluates to the same truth-value as $C$ over Boolean assignments; concretely $p_C = 1 - \prod_{j=1}^{\ell}(1 - x_{i_j}) \prod_{j=\ell+1}^{k} x_{i_j}$. More generally, if $C$ denotes a constraint on $k$ Boolean variables, we write $p_C$ for the unique multilinear polynomial on the variables of $C$ that represents $C$ over Boolean assignments; i.e., such that $p_C(x) = 1$ if $x$ satisfies $C$, and $p_C(x) = 0$ if $x$ falsifies $C$, for any $x \in \{0,1\}^n$.

**Theorem 4.6.3** (see Theorem 12 in [84])**.** *For every $\delta \in \mathbb{R}_{>0}$ there exist $c, \epsilon \in \mathbb{R}_{>0}$ such that, asymptotically almost surely as $n$ goes to infinity, if $m = \lceil cn \rceil$ and $C_1, \ldots, C_m$ are random 3-XOR (resp. 3-SAT) constraints on $x_1, \ldots, x_n$ that are chosen uniformly and independently at random, then there is a degree $\epsilon n$ SOS pseudoexpectation for the system of polynomial equations $p_{C_1} = 1, \ldots p_{C_m} = 1$, and at the same time every truth assignment for $x_1, \ldots, x_n$ satisfies at most a $1/2 + \delta$ fraction (resp. $7/8 + \delta$) of the constraints $C_1, \ldots, C_m$.*

It should be noted that it is not immediately obvious, from just reading the definitions, that the statement of Theorem 12 in [84] gives the pseudoexpectation as stated in Theorem 4.6.3. However, the proof of Theorem 12 in [84] is by now sufficiently well understood to know that Theorem 4.6.3 holds true as stated. One way of seeing this is by noting that the proof of Theorem 12 in [84] and the proof of the lower bound for the Tseitin formulas in Corollary 1 of [37] are essentially the same. In particular Theorem 12 in

[84] holds true also for proving the existence of SOS pseudo-expectations as stated in Theorem 4.6.3.

As an immediate consequence we get:

**Corollary 4.6.4.** *There exist $c, \epsilon \in \mathbb{R}_{>0}$ such that, asymptotically almost surely as $n$ goes to infinity, if $m = \lceil cn \rceil$ and $C_1, \ldots, C_m$ are random 3-XOR (resp. 3-SAT) constraints on $x_1, \ldots, x_n$ that are chosen uniformly and independently at random, then every SOS refutation of $p_{C_1} = 1, \ldots, p_{C_m} = 1$ has monomial size at least $2^{\epsilon n}$.*

It is often stated that Theorem 4.6.3 gives optimal integrality gaps for the approximability of MAX-3-XOR and MAX-3-SAT by linear degree SOS. Corollary 4.6.4 is its analogue for subexponential size SOS. There is however a subtlety in that the validity of the integrality gap statement could depend on the encoding of the objective function. The next section is devoted to clarify this.

### 4.6.2 MAX-CSPs

An instance $\mathscr{I}$ of the Boolean MAX-CSP problem is a sequence $C_1, \ldots, C_m$ of constraints on $n$ Boolean variables. We are asked to maximize the fraction of satisfied constraints. If $p_j$ denotes the unique multilinear polynomial on the variables of $C_j$ that represents $C_j$, then the *optimal value* for an instance $\mathscr{I}$ can be formulated as follows::

$$\mathrm{opt}(\mathscr{I}) := \max_{x \in \{0,1\}^n} \quad \tfrac{1}{m} \textstyle\sum_{j=1}^{m} p_j(x). \tag{4.41}$$

We could ask for the least upper bound on (4.41) that can be certified by an SOS proof of some given complexity $c$, i.e., monomial size at most $s$, degree at most $2d$, etc. There are at least three formulations of this question. Using the notation $\vdash_c$ to denote SOS provability with complexity $c$, the

three formulations are:

$$\begin{aligned}
&\mathrm{sos}''_c(\mathscr{I}) := \\
&\qquad \inf\{\gamma \in \mathbb{R} : \vdash_c \tfrac{1}{m}\textstyle\sum_{j=1}^m p_j(x) \leq \gamma\}, && (4.42)\\
&\mathrm{sos}'_c(\mathscr{I}) := \\
&\qquad \inf\{\gamma \in \mathbb{R} : \{p_j(x) = y_j : j \in [m]\} \vdash_c \tfrac{1}{m}\textstyle\sum_{j=1}^m y_j \leq \gamma\}, && (4.43)\\
&\mathrm{sos}_c(\mathscr{I}) := \\
&\qquad \inf\{\gamma \in \mathbb{R} : \{p_j(x) = y_j : j \in [m]\} \cup \{\tfrac{1}{m}\textstyle\sum_{j=1}^m y_j \geq \gamma\} \vdash_c -1 \geq 0\}. && (4.44)
\end{aligned}$$

The first formulation asks directly for the least upper bound on the objective function of (4.41) that can be certified in complexity $c$. The second formulation is similar but stronger since it allows $m$ additional Boolean variables $y_1, \ldots, y_m$, and their twins. The third is the strongest of the three as it asks for the least value that can be proved impossible. In addition, unlike the other two, the set of hypotheses in (4.44) mixes equations and inequality constraints. It should be obvious that (for natural complexity measures) we have $\mathrm{sos}_c(\mathscr{I}) \leq \mathrm{sos}'_c(\mathscr{I}) \leq \mathrm{sos}''_c(\mathscr{I})$ so lower bounds on $\mathrm{sos}_c$ imply lower bounds for the other two.

Theorem 4.6.3 gives, by itself, optimal integrality gaps for MAX-3-XOR and MAX-3-SAT for linear degree SOS in the $\mathrm{sos}''_c$ formulation, when $c$ denotes SOS-degree. However, the degree lower bound that follows from this formulation does not let us apply our main theorem; the statement is not about refutations, it is about proving an inequality, so Theorem 4.0.1 does not apply. In the following we argue that Theorem 4.6.3 also gives optimal integrality gaps in the $\mathrm{sos}'_c$ and $\mathrm{sos}_c$ formulations of the problems. Since the $\mathrm{sos}_c$ formulation *is* about refutations, our main theorem will apply.

We write $\alpha_c(\mathscr{I})$ for the supremum of the $\alpha \in [0,1]$ for which

$$\alpha \cdot \mathrm{sos}_c(\mathscr{I}) \leq \mathrm{opt}(\mathscr{I}) \leq \mathrm{sos}_c(\mathscr{I}) \tag{4.45}$$

holds. If $\mathscr{C}$ is a class of instances, then we write $\alpha^*_c(\mathscr{C}) := \inf\{\alpha_c(\mathscr{I}) : \mathscr{I} \in \mathscr{C}\}$; the *$\mathrm{sos}_c$-approximation factor* for $\mathscr{C}$. It is our goal to show that

Theorem 4.6.3 implies that, for SOS proofs of sublinear degree, the $\mathrm{sos}_c$-approximation factor of MAX-3-XOR is at most $1/2$, and that of MAX-3-SAT is at most $7/8$. These are optimal. This will follow from Theorem 4.6.3 and the following general fact about pseudo-expectations that (pseudo-)satisfy all the constraints:

**Lemma 4.6.5.** *Let $\mathscr{I}$ be a MAX-CSP instance with $n$ Boolean variables and $m$ constraints of arity at most $k$, represented by multilinear polynomials $p_1, \ldots, p_m$, and let $Q = \{p_j(x) = 1 : j \in [m]\}$, $Q' = \{p_j(x) = y_j : j \in [m]\}$ and $P' = \{\frac{1}{m}\sum_{j=1}^m y_j \geq 1\}$. If there is a degree-$2dk$ SOS pseudo-expectation $E$ for $Q$, then there is a degree-$2d$ SOS pseudo-expectation $E'$ for $P'$ and $Q'$.*

*Proof.* Let $\sigma$ be the substitution that sends $y_j$ to $p_j(x)$ and $\bar{y}_j$ to $1 - p_j(x)$ for $j = 1, \ldots, m$. For each polynomial $p$ on the $x$ and $y$ variables, define $E'(p) := E(p[\sigma])$, where $p[\sigma]$ denotes the result applying the substitution to $p$. The proof that this works relies on the fact that if $p$ and $q$ are polynomial in the $x$ and $y$ variables, then $(pq)[\sigma] = p[\sigma]q[\sigma]$, and $\deg((pq)[\sigma]) \leq \deg(p[\sigma]q[\sigma]) \leq 2k(\deg(p) + \deg(q))$. In particular, squares maps to squares by the substitution. It is obvious that each equation $p_j(x) = y_j$ lifts: $E'(t(p_j(x) - y_j)) = E(t[\sigma](p_j(x) - p_j(x))) = E(0) = 0$. It is equaly obvious that the inequality $\frac{1}{m}\sum_{j=1}^m y_j - 1 \geq 0$ lifts: $E'(s(\frac{1}{m}\sum_{j=1}^m y_j - 1)) = \frac{1}{m}\sum_{j=1}^m E(s[\sigma](p_j(x) - 1)) \geq 0$. This completes the proof of the lemma. □

Combining this with Theorem 4.6.3 and Theorem 4.0.1 we get:

**Corollary 4.6.6.** *For every $\delta \in \mathbb{R}_{>0}$, there exist $r, \epsilon \in \mathbb{R}_{>0}$ such that if $c$ denotes SOS monomial size at most $2^{\epsilon n}$, where $n$ is the number of variables, then $\alpha_c^*(\textit{MAX-3-XOR}) \leq 1/2 + \delta$ (resp. $\alpha_c^*(\textit{MAX-3-SAT}) \leq 7/8 + \delta$), and the gap is witnessed by an instance $\mathscr{I}$ with $m = \lceil rn \rceil$ many uniformly and independently chosen random constraints, for which $\mathrm{sos}_c(\mathscr{I}) = 1$ and $\mathrm{opt}(\mathscr{I}) \leq 1/2 + \delta$ (resp. $\mathrm{opt}(\mathscr{I}) \leq 7/8 + \delta$), asymptotically almost surely as $n$ goes to infinity.*

# Chapter 5

# Feasible interpolation for Polynomial Calculus, Sums-of-Squares and Sherali-Adams

In this chapter we prove a form of feasible interpolation for Polynomial Calculus, Sums-of-Squares and Sherali-Adams. We prove that for any of the three systems there is a polynomial-time algorithm that given

- two set $Q_1(x, z)$ and $Q_2(y, z)$ in disjoint sequences $x$, $y$ and $z$ of variables;
- a refutation of $Q_1(x, z) \cup Q_2(y, z)$;
- and an assignment $a$ to the $z$-variables

outputs a refutation of $Q_1(x, a)$ or a refutation of $Q_2(y, a)$. Hence not only is an interpolant of $Q_1(x, z) \cup Q_2(y, z)$ computable in time polynomial in the size of the given refutation of $Q_1(x, z) \cup Q_2(y, z)$, but moreover we can actually find a refutation to match.

This is actually a typical situation in proofs of feasible interpolation. Many known proofs of feasible interpolation explicitly construct a refutation

of either $Q_1(x,a)$ or $Q_2(y,a)$ from a given refutation of $Q_1(x,z) \cup Q_2(y,z)$ (see e.g. [76, 72]). Our proof is however novel in the methods used. We do not construct either of the refutations explicitly from the given refutation of $Q_1(x,z) \cup Q_2(y,z)$. Rather we first show that a small refutation of either $Q_1(x,a)$ or $Q_2(y,a)$ exists. This existential property is called **the feasible disjunction property** of the proof systems after [73]. Only after proving the feasible disjunction property we show that we can actually efficiently find the small refutation, whose existence is guaranteed by the feasible disjunction property.

We prove the feasible disjunction property using the semantic tools for proofs over sets of monomials developed in Chapter 3. For these proofs it is more natural and cleaner to consider refutations of the union of two sets $Q_1(x)$ and $Q_2(y)$ of polynomial constraints in disjoint sequences of variables. The setting with a given refutation of $Q_1(x,z) \cup Q_2(y,z)$ reduces to the former after assigning the values of $z$-variables. In short, we show that if there is a refutation of $Q_1(x) \cup Q_2(y)$ that uses only monomials from some set $S$, then either $Q_1(x)$ has a refutation over $S_x$ or $Q_2(y)$ has a refutation over $S_y$, where $S_x$ is the projection of $S$ to the $x$-variables. For Sums-of-Squares and Sherali-Adams the actual result takes slightly more cumbersome form.

The basic idea behind the proofs of feasible disjunction property is very simple. Assuming towards a contradiction that there is no refutation of $Q_1(x)$ over $S_x$ nor a refutation of $Q_2(y)$ over $S_y$, we obtain semantic objects, either reduction operators or pseudoexpectations, witnessing these assumptions. As these semantic objects are defined on disjoint sequences of variables, we can combine them to form a semantic object that contradicts the existence of a refutation of $Q_1(x,z) \cup Q_2(y,z)$ that uses only monomials from the set $S$. The proofs are thus resource-bounded versions of the obvious semantic proof of Halldén Completeness of classical propositional logic [44], which states that if $\varphi \vee \psi$ is a theorem and $\varphi$ and $\psi$ don't share any propositional variables, then $\varphi$ is a theorem or $\psi$ is a theorem.

In this chapter we also show that there are efficient proof search algorithms for proofs over sets of monomials. The algorithm for Polynomial

Calculus is a modification of the one for degree-bounded PC proofs from [22]. The algorithm has a polynomial-time run-time for any fixed finite fields, but for infinite fields intermediate coefficient bloat can become a hinderance for the run-time.

For Sherali-Adams and Sums-of-Squares the proof search for proofs over a set of monomials is a linear or semidefinite program of size polynomial in the size of the set of monomials and the encoding of the constraints. This immediately gives a polynomial-time proof search algorithm for Sherali-Adams with ellipsoid algorithm, but for Sums-of-Squares we need to bound the initial ellipsoid by considering proof search problem with a bound on the size of the coefficients appearing in the SOS proof.

Together with the feasible disjunction property these proof search algorithms yield the proofs of the feasible interpolation theorems. As we give an efficient algorithm for Polynomial Calculus only over fixed finite fields, we can prove the feasible interpolation property only for fixed finite fields. Similarly we prove the feasible interpolation theorem for Sums-of-Squares only for sets of equality constraints, since we need to consider explicitly bounded SOS refutations and we only have the corresponding semantic objects in this case for sets of equality constraints.

Finally in Section 5.4 we prove that Sums-of-Squares cannot admit monotone feasible interpolation with respect to polynomial-sized monotone Boolean circuits by showing that the Clique-Coloring formulas have small refutations in Sums-of-Squares. The monotone feasible interpolation theorem for Sums-of-Squares would thus be in contradiction with known lower bounds for monotone circuits [80, 3].

## 5.1 Feasible interpolation for Polynomial Calculus

First we prove the feasible interpolation property for Polynomial Calculus over any finite field. The feasible disjunction property does not rely on the finiteness of the field, but stays true over any field. However we obtain the

feasible interpolation property only over finite fields, since we can guarantee the polynomial run-time in the proof search algorithm of Section 5.1.2 only over finite fields. We do not assume the presence of Boolean axioms in this section.

### 5.1.1 Feasible disjunction for Polynomial Calculus

For a set of monomials $S$, and a sequence $x$ of variables, we denote by $S_x$ the projection of $S$ onto the variables $x$, i.e. $m \in S_x$, if only variables from $x$ appear in $m$, there is some $m'$, where no variables from $x$ appear and $mm' \in S$.

**Theorem 5.1.1.** *Let $\mathbb{F}$ be a field, let $Q_1(x)$ and $Q_2(y)$ be two sets of equality constraints in disjoint sequences $x$ and $y$ of variables, let $\Pi$ be a PC/$\mathbb{F}$ refutation of $Q_1(x) \cup Q_2(y)$, and let $S$ be the set of all monomials appearing in the refutation $\Pi$. Then there is a PC/$\mathbb{F}$ refutation of $P(x)$ over $S_x$ or a PC/$\mathbb{F}$ refutation of $Q(y)$ over $S_y$.*

*Proof.* Suppose towards a contradiction that the conclusion does not hold. Then, by Theorem 3.1.6, there are reduction operators $R_x$ and $R_y$ for $Q_1(x)$ and $Q_2(y)$ over $S_x$ and $S_y$, respectively.

Let $S' := \{m_x m_y : m_x \in S_x \text{ and } m_y \in S_y\}$, and define a linear function $R\colon \mathbb{F}[S'] \to \mathbb{F}[S']$ with

$$R(m_x m_y) = R_x(m_x) R_y(m_y)$$

for any $m_x m_y \in S'$ and extend linearly.

We claim now that $R$ has the following properties:

- $R(1) = 1$; (5.1)
- $R(q_1) = 0$ for any $q_1 \in Q_1(x)$; (5.2)
- $R(q_2) = 0$ for any $q_2 \in Q_2(y)$; (5.3)
- $R(x_i m) = R(x_i R(m))$ if $m \in S$; (5.4)
- $R(y_i m) = R(y_i R(m))$ if $m \in S$. (5.5)

(5.1) holds, since $R_x(1) = R_y(1) = 1$. It is clear that both (5.2) and (5.3) hold.

Finally (5.4) holds by (3.12) and (3.13), since

$$\begin{aligned} R(x_i m) &= R_x(x_i m_x) R_y(m_y) \\ &= R_x(x_i R_x(m_x)) R_y(R_y(m_y)) \\ &= R(x_i R_x(m_x) R_y(m_y)) \\ &= R(x_i R(m)) \end{aligned}$$

The case (5.5) is proved similarly.

Now the existence of such $R$ is in contradiction with the assumption that in $\Pi$ there appears only monomials from $S$. Firstly $R$ is defined for all the polynomial appearing in $\Pi$. Secondly, by (5.2) and (5.3), $R$ maps each axiom in $P(x) \cup Q(y)$ to zero, and, by linearity and (5.4) and (5.5), respects the inference rules in the sense that $R$ maps the consequent of a rule to zero whenever it maps the premises to zero. Hence, by induction on the structure of the refutation, $R(1) = 0$, against (5.1). □

### 5.1.2 Proof search for Polynomial Calculus

In this section we give a proof search algorithm for Polynomial Calculus proofs over a set $S$ of monomials. We show that for any fixed finite field $\mathbb{F}$ the algorithm can find a PC/$\mathbb{F}$ proof of $p = 0$ from $Q$ over a set $S$ of monomials in time polynomial in $|S|$, $|Q|$ and $n$ if one exists. In particular one can find a degree $d$ PC/$\mathbb{F}$ proof of $p = 0$ from $Q$ in time polynomial in $n^d$ and $|Q|$ if one exists.

For any field $\mathbb{F}$, we construct a basis $B$ for the vector space $\mathrm{PC}_S^{\mathbb{F}}(Q)$ of all polynomials $p \in \mathbb{F}[\widehat{S}]$ that admit a proof from $Q$ over $S$. This construction is carried out by the algorithm 1 which is a modification of an algorithm from [22]. For the algorithm fix any total ordering $<$ on $\widehat{S}$ that satisfies the following property:

- $m < m'$ for any $m \in S$ and $m' \in \widehat{S} \setminus S$. (5.6)

Define the leading monomial $\mathrm{LM}(p)$ and leading term $\mathrm{LT}(p)$ of a polynomial $p$ with respect to the ordering $<$. The leading monomial of $p$ is the highest monomial with respect to $<$ with a non-zero coefficient in $p$, and the leading term is the non-zero term in $p$, whose underlying monomial is the leading monomial of $p$.

**Algorithm 1:** Proof search over $S$

```
Initially A = Q and B = ∅;
while A ≠ ∅ do
    Pick p ∈ A and remove it from A;
    while LM(p) ∈ LM(B) do
        Let q ∈ B be such that LM(q) = LM(p);
        Let p ← p − aq, where a is such that LT(p) = aLT(q);
    end
    If p ≠ 0, add p to B;
    If p ∈ 𝔽[S], add xp to A for every variable x;
end
Output B;
```

The output $B$ of the algorithm 1 is a linearly independent set of polynomials, since all elements of $B$ have distinct leading monomials. As all elements of $B$ have distinct leading monomials there is never more than $n|S|$ elements added to $A$ and thus the algorithm halts after polynomially many rounds in $|S|$, $|Q|$ and $n$. Hence for any fixed finite field the algorithm will halt in time polynomial in $|S|$, $|Q|$ and $n$. In the following we prove that $B$ is actually a basis for $\mathrm{PC}_S^{\mathbb{F}}(Q)$.

**Lemma 5.1.2.** *At the end of the algorithm 1,* $\mathrm{span}(B) = \mathrm{PC}_S^{\mathbb{F}}(Q)$.

*Proof.* Clearly each $q \in B$ has a proof from $Q$ over $S$, and so $\mathrm{span}(B) \subseteq \mathrm{PC}_S^{\mathbb{F}}(Q)$.

Now suppose $p \in \mathrm{PC}_S^{\mathbb{F}}(Q)$ and let $p_1, \ldots, p_\ell$ be a PC proof of $p = 0$ from $Q$ over $S$. We show by induction on the structure of the proof that

$p_i \in \mathrm{span}(B)$ for any $i \in [\ell]$. To see that any element of $Q$ is in $B$, note that $\mathrm{span}(A \cup B)$ can only increase at each stage of the algorithm. Hence, as the algorithm halts with $A = \emptyset$, at the end each element of $Q$ is in $\mathrm{span}(B)$. If $p_i = ap_j + bp_k$ for some $j, k < i$, and $p_j, p_k \in \mathrm{span}(B)$, then clearly $p_i \in \mathrm{span}(B)$.

Finally, suppose that $p_i = xp_j$ for some $j < i$ and some variable $x$. Now we have $p_j \in \mathbb{F}[S]$, and by induction assumption, $p_j \in \mathrm{span}(B)$. Write $p_j = \sum a_k q_k$ for some $a_k \in \mathbb{F}$ and $q_k \in B$. We claim that $q_k$ is in $\mathbb{F}[S]$ for each $k$ with non-zero $a_k$. To see this, let $m$ be the maximal monomial that appears in any $q_k$ with a non-zero coefficient. Now $m$ appears in only one of the $q_k$'s, since they all have distinct leading monomials, and so the monomial $m$ has a non-zero coefficient in $p_j$. Hence $m$ is in $S$, and so, by (5.6), $q_k$ is in $\mathbb{F}[S]$ for every $k$. Now for any $k$, the polynomial $q_k$ was added to $B$ and $xq_k$ was added to $A$ at some stage of the algorithm. At that stage $xq_k$ is in $\mathrm{span}(A \cup B)$. However, since the span only increases during the execution of the algorithm, $xq_k$ is in $\mathrm{span}(B)$ at the end of the algorithm. Hence $xp_j$ is in $\mathrm{span}(B)$ at the end of the algorithm. □

Now to check whether there is a PC/$\mathbb{F}$ proof of $p = 0$ from $Q$ over $S$ one simply needs to reduce the polynomial $p$ with respect to the basis $B$. This is easy to do, since all the elements of $B$ have distinct leading monomials. In order to construct the proof, one needs proofs for the basis elements. The construction of these proofs is easily incorporable into the algorithm above, but was omitted for readability.

**Remark 5.1.3.** We claim the polynomial-time proof search only for fixed finite fields, since although the algorithm 1 always halts in polynomially many steps in $|S|$, $|Q|$ and $n$, there is no way to combat potential coefficient bloat in infinite fields, and in the worst case the magnitude of the largest coefficient in $A \cup B$ might be squared after each round of the algorithm.

In Chapter 6 we give an example over rationals where such blow-up is necessary showing that over rationals the worst case time-complexity of algorithm 1 is necessarily exponential.

### 5.1.3 Feasible interpolation for Polynomial Calculus

As a consequence of Theorem 5.1.1 and Section 5.1.2 we obtain the feasible interpolation property for PC over any finite field.

**Theorem 5.1.4.** *For any finite field $\mathbb{F}$, there is a polynomial time algorithm that given*

- *two sets $Q_1(x,z)$ and $Q_2(y,z)$ of equality constraints in disjoint sequences $x, y$ and $z$ of variables;*
- *a PC/$\mathbb{F}$ refutation of $Q_1(x,z) \cup Q_2(y,z)$;*
- *an assignment $a$ to the variables $z$*

*outputs a PC/$\mathbb{F}$-refutation of $Q_1(x,a)$ or a PC/$\mathbb{F}$-refutation of $Q_2(y,a)$.*

## 5.2 Feasible interpolation for Sums-of-Squares

Secondly we prove feasible interpolation property for Sums-of-Squares. We prove the feasible interpolation property for SOS only for sets of equality constraints. This is due to our need to consider explicitly bounded proofs in order to give a polynomial time search algorithm for SOS proofs. Hence we need to prove the feasible disjunction property in a form that also takes into account the magnitude of the coefficients appearing in the refutations. This we can do using $\varepsilon$-pseudoexpectations, but with the cost of losing the inequality constraints along the way.

### 5.2.1 Feasible disjunction for Sums-of-Squares

**Theorem 5.2.1.** *Let $Q_1(x)$ and $Q_2(y)$ be two sets of equality constraints in disjoint sequences $x$ and $y$ of variables, let $\Pi$ be an $R$-bounded SOS refutation of $Q_1(x) \cup Q_2(y)$, let $S$ be the set of all explicit monomials appearing in the refutation $\Pi$, and let $R' = 2R(|Q_1(x) \cup Q_2(y)| + n)|S|$. Then there*

*is a $R'$-bounded refutation of $Q_1(x)$ over $S_x$ or a $R'$-bounded refutation of $Q_2(y)$ over $S_y$.*

*Proof.* Suppose towards a contradiction that the conclusion does not hold. Then, by Lemma 3.2.12, there are $1/R'$-pseudoexpectations for $Q_1(x)$ and $Q_2(y)$ over $S_x$ and $S_y$, respectively. Now define a linear functional $E\colon \mathbb{R}[S^2] \to \mathbb{R}$ with

$$E(m) = E_x(m_x)E_y(m_y),$$

for $m \in S^2$ and extend linearly. Here $m_x$ and $m_y$ are the projections of the monomial $m$ to variables $x$ and $y$, respectively. We claim that $E$ has the following properties.

- $E(1) = 1$; (5.7)
- $E(p^2) \geq 0$ for any $p \in \mathbb{R}[S]$; (5.8)
- $E(m(x_i^2 - x_i)) = 0$ for any $m \in S$ and any variable $x_i$; (5.9)
- $E(m(y_i^2 - y_i)) = 0$ for any $m \in S$ and any variable $y_i$; (5.10)
- $|E(m(x_i + \bar{x}_i - 1))| \leq 1/R'$ for any $m \in S$ and any variable $x_i$; (5.11)
- $|E(m(y_i + \bar{y}_i - 1))| \leq 1/R'$ for any $m \in S$ and any variable $y_i$; (5.12)
- $|E(mq)| \leq 1/R'$ for any $m \in S$ and any $q \in Q_i$ for $i = 1, 2$; (5.13)

Firstly (5.7) holds, since $E_x(1) = E_y(1) = 1$.

For (5.8), write $p = \sum_{m\in S} a_m m$. Now the matrix $(E_y(m_y m'_y))_{m,m'\in S}$ is positive semidefinite and so there are vectors $u$ such that for all $m, m' \in S$ we have $E_y(m_y m'_y) = \sum_u u_m u_{m'}$. Now we have

$$\begin{aligned} E\big(p^2\big) &= \sum_{m,m'} a_m a_{m'} E_x(m_x m'_x) E_y\big(m_y m'_y\big) \\ &= \sum_{m,m'} \sum_u a_m u_m a_{m'} u_{m'} E_x(m_x m'_x) \\ &= E_x\left(\left(\sum_m \sum_u a_m u_m m_x\right)^2\right) \geq 0 \end{aligned}$$

To see that (5.9) holds, let $m \in S$. Now

$$E(m(x_i^2 - x_i)) = E_x(m_x(x_i^2 - x_i))E_y(m_y) = 0,$$

since $E_x(m_x(x_i^2 - x_i)) = 0$. The case (5.10) follows similarly.

For (5.11), let $m \in S$. Now

$$|E(m(x_i + \bar{x}_i - 1))| = |E_x(m_x(x_i + \bar{x}_i - 1))||E_y(m_y)| \leq 1/R',$$

where the last inequality holds since $E_x$ is an $1/R'$-pseudoexpectation for $Q_1(x)$ over $S_x$ and since $|E_y(m_y)| \leq 1$ for all $m \in S$. Cases (5.12) and (5.8) follow by a similar argument.

Now the existence of such $E$ is in contradiction with the assumption that there is a refutation of $Q_1(x) \cup Q_2(y)$ with all the explicit monomials among $S$: applying the $E$ on both sides of the refutation we reach a contradiction of the form $-1 > -1$ as in Lemma 3.2.11. □

### 5.2.2 Proof search for SOS proofs

In this section we show how to efficiently find SOS proofs over a set of monomials by formulating the search for an SOS proof as a semidefinite program, and using the ellipsoid algorithm to check the feasibility of the said program.

Let us first recall the ellipsoid method and its implications to the feasibility problem of semidefinite programming. The ellipsoid method is a general purpose optimization method for convex optimization problems introduced in [86]. Its rise to fame came when Khachiyan used the method to give the first polynomial time algorithm for linear programming [50, 51]. We refer the reader to the monograph [42] for a very thorough treatment of the Ellipsoid algorithm.

For our purposes, the ellipsoid method can be used to solve the following computational problem. Given a set $Q$ of linear and semidefinite constraints, and positive rationals $r$ and $R$, with the promise that if the feasible region of $Q$ is non-empty, then it contains a ball of radius $r$, i.e. the feasible region is **full-dimensional**, which itself is contained in a larger ball

of radius $R$ centered at the origin, the **initial ellipsoid**, then the ellipsoid method either finds a feasible point of $Q$, or tells that the feasible region is empty, in time polynomial in $\langle Q \rangle$, $\log(1/r)$ and $\log(R)$, where $\langle Q \rangle$ denotes the number of bits needed to encode all the constraints. This follows from the central-cut ellipsoid method of [42] and the fact that there is a **strong separation oracle** for PSD matrices as observed already in [41]: given a symmetric rational matrix $A$, one can in time polynomial in $\langle A \rangle$, either verify that $A$ is a PSD matrix, or find a vector $v$ such that $v^T A v < 0$.

As noted earlier, to achieve a polynomial time proof search algorithm for SOS proofs over a set of monomials, we need to impose a restriction on the magnitude of the coefficients in an SOS proof. This is to bound the radius of initial ellipsoid so that our starting point for the proof search is not too far from the origin. For semidefinite programs in general, there are examples whose feasible region is too far from the origin [79], and thus the initial ellipsoid cannot be chosen small enough to guarantee polynomial run-time. For SOS this was first noted by O'Donnell in [66] in non-Boolean context and then expanded on by [78] for Boolean SOS. Chapter 6 of this thesis further explores this issue.

The following lemma and its corollary show that a bound on the coefficients of the polynomials $t_q$ and $u_i$ translates into a bound on the coefficients appearing in the polynomials $r_i$ and in the lifts of the $x^2 - x$ axioms. The proof of the lemma is a minor modification of a special case of the main theorem of [78].

**Lemma 5.2.2.** *Let $p \in \mathbb{R}[S]$ and suppose that there are $r_i \in \mathbb{R}[S]$ such that*

$$p \equiv \sum r_i^2 \mod J_n.$$

*Then there is a PSD matric $C$ such that*

$$p \equiv \langle C, \mathbf{v}_S \mathbf{v}_S^T \rangle \mod J_n,$$

*and all the entries in $C$ are bounded from above in absolute value by polynomial in $2^{\text{poly}(|S|)}$ and $\|p\|_\infty$.*

*Proof.* Let $\mathbf{v}_S$ be a vector of all the monomials in $S$, and let $D$ be a PSD matrix such that

$$p \equiv \langle D, \mathbf{v}_S \mathbf{v}_S^T \rangle \mod J_n$$

Denote the matrix $\mathbf{v}_S \mathbf{v}_S^T$ averaged over all the $0,1$-assignments on the $2n$ variables (not necessarily respecting the twin variables, i.e. twins can have the same value) by $M_S$, i.e. $M_S = \mathbb{E}_{\alpha \in \{0,1\}^{2n}}[\mathbf{v}_S(\alpha)\mathbf{v}_S^T(\alpha)]$. Now, by Lemma 6 of [78], the smallest non-zero eigenvalue $\delta$ of $M_S$ is at least $1/2^{\text{poly}(|S|)}$.

Let now $\Pi = \sum uu^T$ be the projector onto the zero eigenspace of $M_S$. Since $\mathbb{E}_{\alpha \in \{0,1\}^{2n}}[u^T \mathbf{v}_S(\alpha)\mathbf{v}_S^T(\alpha)u] = u^T M_S u = 0$ for each $u$ in the zero eigenspace of $M_S$, the inner product $u^T \mathbf{v}_S(\alpha)$ is zero for every assignment $\alpha$. Thus $u^T \mathbf{v}_S \equiv 0 \mod J_n$, and so

$$\begin{aligned} \langle D, \mathbf{v}_S \mathbf{v}_S^T \rangle &\equiv \langle D, (\Pi + \Pi^\perp)\mathbf{v}_S \mathbf{v}_S^T (\Pi + \Pi^\perp) \rangle \mod J_n \\ &\equiv \langle D, \Pi^\perp \mathbf{v}_S \mathbf{v}_S^T \Pi^\perp \rangle \mod J_n \\ &\equiv \langle \Pi^\perp D \Pi^\perp, \mathbf{v}_S \mathbf{v}_S^T \rangle \mod J_n \end{aligned}$$

Let $C = \Pi^\perp D \Pi^\perp$, so that

$$p \equiv \langle C, \mathbf{v}_S \mathbf{v}_S^T \rangle \mod J_n.$$

Now, by taking averages on both sides, we obtain that

$$\mathbb{E}_{\alpha \in \{0,1\}^{2n}}[r(\alpha)] \geq \langle C, M_S \rangle$$

The left hand side is at most polynomial in $R$ and $|S|$. On the other hand the right hand side is at least $\delta \text{Tr}(C)$, since every non-zero eigenvalue of $M_S$ is at least $\delta$ and the zero eigenspace of $C$ is included in the zero-eigenspace of $M_S$. Since the Frobenius norm of $C$ is bounded by $\text{Tr}(C)$ we have that each entry of $C$ is at most polynomial in $2^{\text{poly}(|S|)}$ and $R$. □

**Corollary 5.2.3.** *Let $Q$ be a set of equality constraints, let $S$ be a set of monomials containing all the monomials in $Q$, all the variables and the empty monomial 1, and let $p \in \mathbb{R}[S^2]$. If there is an $R$-bounded proof of non-negativity of $p$ from $Q$ over $S$, then there is a PSD matrix $C$ and polynomials $t_q$ for every $q \in Q$ and $u_i$ for every $i \in [n]$ such that*

$$p \equiv \langle C, \mathbf{v}_S \mathbf{v}_S^T \rangle + \sum_{q \in Q} t_q q + \sum_{i \in [n]} u_i (x_i + \bar{x}_i - 1), \tag{5.14}$$

*and all the entries in $C$ are bounded from above in absolute value by polynomial in $2^{\mathrm{poly}(|S|)}$, $R$ and $\|p\|_\infty$; and $\|t_q\|_\infty, \|u_i\|_\infty \leq R$ for any $q \in Q$ and $i \in [n]$.*

*Proof.* If

$$p \equiv \sum_{i\in[k]} r_i^2 + \sum_{q\in Q} t_q q + \sum_{i\in[n]} u_i(x_i + \bar{x}_i - 1) \mod J_n$$

, then

$$p - \sum_{q\in Q} t_q q - \sum_{i\in[n]} u_i(x_i + \bar{x}_i - 1) \equiv \sum_{i\in[k]} r_i^2 \mod J_n,$$

and the previous lemma provides us with a suitable matrix $C$. □

The existence of the proof 5.14 can now be expressed as feasibility of a set of linear and semidefinite constraints. Moreover the bounds on the entries of $C$ allow us to narrow down the search space for an $R$-bounded proof so that we can efficiently check the feasibility, and thus find an SOS proof, using ellipsoid algorithm. We discuss the details next.

For a set $Q$ of equality constraints; a polynomial $p$; a set $S$ of (multilinear) monomials containing all the monomials in $Q$, $p$, all the variables and the empty monomial 1; and a positive real $R$ we define the semidefinite program $\mathrm{SDP}(Q, p, S; R)$ as follows.

**Variables:** Introduce a variable $x_{m,m'}$ for any $m, m' \in S$. These correspond to the entries in the matrix $C$ in (5.14). For any $q \in Q$ and any $m \in S$ introduce a variable $x_{m,q}$. These correspond to the coefficients in the polynomial $t_q$ of (5.14). Finally, for any $i \in [n]$ and any $m \in S$ introduce the variables $x_{m,i}$. These correspond to the coefficients in the lifts of the Boolean axiom $x_i + \bar{x}_i - 1$. Let $X$ be the $|S| \times |S|$-matrix of variables, such that $X_{m,m'} = x_{m,m'}$. The number of variables is polynomial in $|S|$ and $|Q|$.

**Constraints:** For any $q \in Q$, let $\bar{q}$ denote the coefficient vectors of $q$, i.e. $\bar{q}^T \mathbf{v}_S = q$ for any $q \in Q$. Let $\dot{S}$ denote the set of all multilinearizations of

elements of $S^2$, and write $p = \sum_{m \in \dot{S}} a_m m$. For any $m \in \dot{S}$ we introduce the linear equality constraint $C_m = a_m$, where

$$C_m := \sum_{\substack{m_1,m_2 \in S \\ m_1 m_2 \equiv m \mod J_n}} x_{m_1,m_2} + \sum_{\substack{m_1,m_2 \in S \\ m_1 m_2 \equiv m \mod J_n}} \sum_{q \in Q} x_{m_1,q} \bar{q} m_2$$

$$+ \sum_{i \in [n]} \left( \sum_{\substack{m_1 \in S \\ x_i m_1 \equiv m \mod J_n}} x_{m_1,i} + \sum_{\substack{m_2 \in S \\ \bar{x}_i m_2 \equiv m \mod J_n}} x_{m_2,i} - \sum_{\substack{m_3 \in S \\ m_3 \equiv m \mod J_n}} x_{m_3,i} \right).$$

In short the constraint states that the entries of the matrix $C$ and the coefficients for the lifts should be chosen so that each monomial $m$ ends up with the correct coefficient for $p$. Secondly we impose the constraints $-R \leq x_{m,q} \leq R$ for any $q \in Q$ and $m \in S$ and $-R \leq x_{m,i} \leq R$ for any $i \in [n]$ and $m \in S$. We furthermore impose the PSD-constraint $X \succeq 0$. The size of the encoding of all the constraints is polynomial in $|S|$, $\langle Q \rangle$ and $\langle p \rangle$ and $\log R$.

Now it is straightforward to verify that any feasible solution for the above constraints gives an $R$-bounded SOS proof of non-negativity of $p$ from $Q$ over $S$, and vice versa.

Corollary 5.2.3 gives us an upper bound for radius of the initial ellipsoid. However, with all the linear equality constraints, the feasible region of the program $\mathrm{SDP}(Q, p, S; R)$ is never full-dimensional. However by fuzzying the constraints slightly we gain full-dimensionality without affecting our end goal too much. The trick is well-known, we sketch the argument below. A similar argument can be found in e.g. [66].

For $\varepsilon > 0$, an $\varepsilon$-relaxation of the above constraints is the same set of constraints with the constraints $C_m = a_m$ replaced by $|C_m - a_m| \leq \varepsilon$, and the constraints $-R \leq x_{m,q} \leq R$ and $-R \leq x_{m,i} \leq R$ replaced by $-R - \varepsilon \leq x_{m,q} \leq R + \varepsilon$ and $-R - \varepsilon \leq x_{m,i} \leq R + \varepsilon$. Now if there is a feasible solution for the original set of constraints, the set of solutions of the $\varepsilon$-relaxation has volume at least $1/2^{\mathrm{poly}(\log(1/\varepsilon), |S|)}$. We choose $\varepsilon$ of order $1/2^{\mathrm{poly}(|S|)}$. This gives the smaller radius $r$ in the ellipsoid algorithm of order $1/2^{\mathrm{poly}(|S|)}$.

Now one can find a feasible solution to the $\varepsilon$-relaxation of the program $\mathrm{SDP}(Q, p, S; R)$ in time polynomial in $|S|$, $\langle Q \rangle$, $\langle p \rangle$ and $\log R$ using the ellipsoid algorithm.

Any solution for the $\varepsilon$-relaxation translates into an $R + \varepsilon$-bounded SOS proof of non-negativity of a polynomial $p+q$ from $Q$ over $S$, where $\|q\|_\infty \leq \varepsilon'$ for some small $\varepsilon'$ of size polynomial in $1/2^{\mathrm{poly}(|S|)}$ and $|Q|$. Now for each term $a_m m$ that appears in $q$, define $q_m$ as follows: if $a_m > 0$ let $q_m = a_m(1-m)^2$, and if $a_m < 0$ let $q_m = -a_m(m)^2$. Now adding all $q_m$ to $p + q$ gives Sums-of-Squares proof of $p - \varepsilon''$ for some $\varepsilon''$ of size polynomial in $1/2^{\mathrm{poly}(|S|)}$ and $|Q|$.

In conclusion, given a set of equality constraints $Q$; a polynomial $p$; a set $S$ of monomials containing all the monomials in $Q$ and $p$, all the variables and the empty monomial 1; and a non-negative real $R$, one can find an $R + \varepsilon$-bounded SOS proof of non-negativity of $p + \varepsilon$ from $Q$ over $S$, for some $\varepsilon$ of size polynomial in $1/2^{\mathrm{poly}(|S|)}$ and $|Q|$, in time polynomial in $|S|$, $\langle Q \rangle$, $\langle p \rangle$ and $\log R$.

### 5.2.3 Feasible interpolation for Sums-of-Squares

Again we obtain the feasible interpolation property for SOS as a corollary to Theorem 5.2.1 and Section 5.2.2.

**Theorem 5.2.4.** *There is a polynomial time algorithm that given*

- *two sets $Q_1(x, z)$ and $Q_2(y, z)$ of equality constraints in disjoint sequences $x, y$ and $z$ of variables;*
- *an SOS refutation of $Q_1(x, z) \cup Q_2(y, z)$;*
- *an assignment $a$ to the variables $z$*

*outputs an SOS-refutation of $Q_1(x, a)$ or an SOS-refutation of $Q_2(y, a)$.*

## 5.3 Feasible interpolation for Sherali-Adams

Finally we prove the feasible interpolation property for Sherali-Adams. Unlike with SOS, for SA we can prove the feasible interpolation property for both equality and inequality constraints as there is no need to consider the analogues of $\varepsilon$-pseudoexpectations. However, as the SA proofs and pseudoexpectations over sets of monomials are not as nicely behaved as their counterparts for SOS, the statement of the feasible disjunction property for SA takes slightly more cumbersome form.

### 5.3.1 Feasible disjunction for Sherali-Adams

Recall the definition of a closed set of monomials from (3.47) and (3.48). We define the **closure** of a set $S$ of monomials, denoted $\bar{S}$, in $n$ pairs of twin variables $x_i, \bar{x}_i, i \in [n]$ as the least set of monomials satisfying the following conditions:

- $S \subseteq \bar{S}$;
- $1 \in \bar{S}$;
- $x_i, \bar{x}_i \in \bar{S}$ for any $i \in [n]$;
- if $x_i m \in \bar{S}$ and all indices appearing in $m$ are at least $i$, then $\bar{x}_i m \in \bar{S}$ and $m \in \bar{S}$;
- if $\bar{x}_i m \in \bar{S}$ and all indices appearing in $m$ are at least $i$, then $x_i m \in \bar{S}$ and $m \in \bar{S}$.

Now it is clear that $\bar{S}$ satisfies the conditions (3.47) and (3.48). It is equally clear that one can compute $\bar{S}$ from $S$ in time polynomial in $n$ and $|S|$.

With the definition of closure of a set of monomials at hand we can state and prove the feasible disjunction property for Sherali-Adams.

**Theorem 5.3.1.** *Let $P_1(x)$ and $P_2(y)$ be two sets of inequality constraints and $Q_1(x)$ and $Q_2(y)$ be two set of equality constraints in disjoint sequences*

*$x$ and $y$ of variables. Let $\Pi$ be an SA refutation of $P_1(x) \cup P_2(y)$ and $Q_1(x) \cup Q_2(y)$, and let $S$ be the set of explicit monomials appearing in $\Pi$. Then there is an SA refutation of $P_1(x)$ and $Q_1(x)$ over $\overline{S_x^2}$ or an SA refutation of $P_2(y)$ and $Q_2(y)$ over $\overline{S_y^2}$.*

*Proof.* Suppose towards a contradiction that neither conclusion holds. Then, by Theorem 3.3.7, there are SA pseudoexpectations $E_x$ for $P_1(x)$ and $Q_1(x)$ over $\overline{S_x^2}$ and $E_y$ for $P_2(y)$ and $Q_2(y)$ over $\overline{S_y^2}$.

Now define a linear functional $E\colon \mathbb{R}[S^2] \to \mathbb{R}$ by

$$E(m) = E_x(m_x)E_y(m_y)$$

for $m \in S^2$ and extend linearly, where $m_x$ and $m_y$ are the projections of $m$ to the variables $x$ and $y$, respectively.

We claim that $E$ has the following properties:

- $E(1) = 1$; (5.15)
- $E(m) \geq 0$ for any $m \in S$; (5.16)
- $E(m(x_i^2 - x_i)) = 0$ for any $m \in S$; (5.17)
- $E(m(y_i^2 - y_i)) =$ for any $m \in S$; (5.18)
- $E(m(x_i + \bar{x}_i - 1)) = 0$ for any $m \in S$; (5.19)
- $E(m(y_i + \bar{y}_i - 1)) = 0$ for any $m \in S$; (5.20)
- $E(mp) \geq 0$ for any $p \in P_j$ for $j = 1, 2$ and $m \in S$ (5.21)
- $E(mq) = 0$ for any $q \in Q_j$ for $j = 1, 2$ and $m \in S$. (5.22)

(5.15) holds since, by definition, $E_x(1) = E_y(1) = 1$. (5.16) holds since $E(m) = E_x(m_x)E_y(m_y)$ and both $E_x(m_x)$ and $E_y(m_y)$ are non-negative. To see that (5.17) holds, first note that, for any $m \in S$, $E_x(m_x(x_i^2 - x_i))$ is defined and equals 0. Now $E(m(x_i^2 - x_i)) = E_x(m_x(x_i^2 - x_i))E_y(m_y) = 0$. The cases (5.18) - (5.20) are proved similarly. For (5.21) suppose without a loss of generality that $p \in P_1$. First note that for any $m \in S$ both $E_x(m_x p)$ and $E_y(m_y)$ are defined and are non-negative. Hence $E(mp) = E_x(m_x p)E_y(m_y) \geq 0$. The case (5.22) is argued similarly.

Now the existence of such $E$ is in contradiction with the assumption that there is a refutation of $P_1(x) \cup P_2(y)$ and $Q_1(x) \cup Q_2(y)$ with all the explicit monomials among $S$: applying the $E$ on both sides of the refutation yields a contradiction of the form $-1 \geq 0$. □

#### 5.3.1.1 Proof search for Sherali-Adams proofs

In this section we show how to efficiently find SA proofs of non-negativity over a set of monomials by formulating the search for SA proofs as a linear program whose feasible solutions are in one-to-one correspondence with SA proofs of non-negativity. Then again we can use ellipsoid algorithm to search for a feasible solution, and thus for an SA proof. Unlike with semidefinite programming, ellipsoid algorithm can always solve the feasibility of a set of linear constraints, in polynomial time in the size of the encoding of the constraints. This is because a linear program has a feasible solution of relatively small bit-complexity if it has any at all. Similarly there are ways to circumvent the requirement for full-dimensionality with linear programming. We refer the reader to [49] for a readable and thorough account on the ellipsoid algorithm for linear programming. Thus the problem with too large coefficients we encountered with SOS does not come up with SA.

For sets $P$ and $Q$ of inequality and equality constraints, respectively, a polynomial $r$ and set $S$ of multilinear monomials containing all the monomials in $P$, $Q$ and $r$, all the variables and the empty monomial 1 we define a linear program $\mathrm{LP}(P, Q, r, S)$ as follows.

**Variables:** Introduce a variable $x_m$ for any $m \in S$. These correspond to the coefficients of the polynomial $s$ in the proof (2.7). Similarly for any $p \in P$ and for any $q \in Q$, introduce variables $x_{m,p}$ and $x_{m,q}$ for any $m \in S$. These correspond to the coefficients in the lifts of the non-logical axioms. Finally, for any $i \in [n]$ introduce the variables $x_i$ for any $m \in S$. These correspond to the coefficients in the lifts of the Boolean axioms.

**Constraints:** For any $p \in P$ and any $q \in Q$, let $\bar{p}$ and $\bar{q}$ denote the coefficient vectors of $p$ and $q$. Let $\dot{S}$ denote the set of all multilinearizations of monomials from $S^2$, and write $r = \sum_{m \in \dot{S}} a_m m$. For any $m \in S$ we introduce the linear constraint

$$a_m = x_m + \sum_{\substack{m_1, m_2 \in S \\ m_1 m_2 \equiv m \mod J_n}} \left( \sum_{p \in P} x_{m',p} \bar{p}_{m''} + \sum_{q \in Q} x_{m',q} \bar{q}_{m''} \right) + \sum_{i \in [n]} \left( \sum_{\substack{m_1 \in S \\ x_i m_1 \equiv m \mod J_n}} x_{m_1,i} + \sum_{\substack{m_2 \in S \\ \bar{x}_i m_2 \equiv m \mod J_n}} x_{m_2,i} - x_{m,i} \right) \quad (5.23)$$

In short the constraint tells that coefficients for the lifts should be chosen so that each monomial $m$ ends up with the correct coefficient.

We impose the constraint $x_m \geq 0$ for any $m \in S$, and the constraint $x_{m,p} \geq 0$ for any $m \in S$ and $p \in P$.

Now it is straightforward to verify that any feasible solution for the above constraints gives an SA proof of non-negativity of $r$ from $P$ and $Q$ over $S$, and vice versa. The size of the linear program is polynomial in $|S|$, $\langle P \rangle$, $\langle Q \rangle$ and $\langle r \rangle$. Thus the ellipsoid algorithm or any other polynomial-time algorithm for linear programming can be used to find a feasible solution for the constraints in time polynomial in $|S|$, $\langle P \rangle$, $\langle Q \rangle$ and $\langle r \rangle$.

### 5.3.2 Feasible interpolation for Sherali-Adams

Finally as a consequence of Theorem 5.3.1 and Section 5.3.1.1, we obtain feasible interpolation for Sherali-Adams.

**Theorem 5.3.2.** *There is a polynomial time algorithm that given*

- *two sets $P_1(x,z)$ and $P_2(y,z)$ of inequality constraints and two set $Q_1(x,z)$ and $Q_2(y,z)$ of equality constraints in disjoint sequences $x, y$ and $z$ of variables;*
- *an SA refutation $\Pi$ of $P_1(x,z) \cup P_2(y,z)$ and $Q_1(x,z) \cup Q_2(y,z)$;*

- *an assignment $a$ to the $z$ variables*

*outputs an SA refutation of $P_1(x,a)$ and $Q_1(x,a)$ or an SA refutation of $P_2(y,a)$ and $Q_2(y,a)$.*

## 5.4 No monotone feasible interpolation for Sums-of-Squares

Finally in this section we show that SOS does not admit monotone feasible interpolation, i.e. feasible interpolation with respect to poly-sized monotone Boolean circuits in the case that the interpolating function is monotone. We prove that SOS has poly-sized proofs of the clique-coloring formulas, and so monotone feasible interpolation property would be in contradiction with the monotone circuit lower bounds for the clique function [80, 3].

Let us first recall the clique-coloring formulas. Let $k > \ell$. We define two CNFs $\mathrm{Clique}_{n,k}(x,z)$ and $\mathrm{Color}_{n,\ell}(y,z)$ stating that there is a clique of size $k$ and a coloring with $\ell$ colors, respectively, on a graph on $[n]$ encoded by the variables $z$.

Introduce variables $x_{ui}$ for any $u \in [k]$ and $i \in [n]$ stating that node $i$ is the $u$th element of the clique encoded by the $x$ variables, variables $y_{ia}$ stating that node $i$ gets the color $a$, and variables $z_{ij}$ for any $\{i,j\} \subseteq [n]$ for distinct $i$ and $j$ stating that there is an edge between nodes $i$ and $j$.

The formula $\mathrm{Clique}_{n,k}(x,z)$ consists of the following clauses:

- $\bigvee_{i\in[n]} x_{ui}$ for any $u \in [k]$; (5.24)
- $\bar{x}_{ui} \vee \bar{x}_{uj}$ for any $u \in [k]$ and any distinct $i,j \in [n]$; (5.25)
- $\bar{x}_{ui} \vee \bar{x}_{vi}$ for any distinct $u,v \in [k]$ and any $i \in [n]$; (5.26)
- $\bar{x}_{ui} \vee \bar{x}_{vj} \vee z_{ij}$ for any distinct $u,v \in [k]$ and any distinct $i,j \in [n]$. (5.27)

Clauses (5.24) and (5.25) together say that exactly one of the nodes in $[n]$ is the $u$th element of the clique encoded by the variables $x$. Clause (5.26) says

that no node is both the $u$th and $v$th element of the clique for distinct $u$ and $v$. Finally (5.27) states that all nodes in the clique are pairwise connected by an edge.

The formula $\text{Color}_{n,\ell}(y, z)$ consists of the following clauses:

- $\bigvee_{a\in[\ell]} y_{ia}$ for any $i \in [n]$; (5.28)
- $\bar{y}_{ia} \vee \bar{y}_{ib}$ for any $i \in [n]$ and distinct $a, b \in [\ell]$; (5.29)
- $\bar{y}_{ia} \vee \bar{y}_{ja} \vee \bar{z}_{ij}$ for any distinct $i, j \in [n]$ and any $a \in [\ell]$. (5.30)

Clauses (5.28) and (5.29) together say that every node gets exactly one of the $\ell$ colors, and clause (5.30) states that no two nodes with the same color are connected by an edge.

In the following we construct SOS refutations for $\text{Clique}_{n,k} \wedge \text{Color}_{n,\ell}$. Our construction follows closely that of [39], where small refutations of $\text{Clique}_{n,k} \wedge \text{Color}_{n,\ell}$ were constructed for degree 4 Lovasz-Schrijver proofs.

We translate all the clauses into polynomial inequality constraints in a straightforward manner: for a clause $\ell_1 \vee \ldots \vee \ell_k$ we define the polynomial constrain $\sum_{i\in[k]} \ell_i \geq 1$. We call this the additive encoding of CNFs into polynomial constraints.

We begin by proving a simple but very useful lemma.

**Lemma 5.4.1.** *Let $m_1, \ldots, m_n$ be monomials of degree at most $k$. Then there is a degree $3k$ SOS proof of non-negativity of $1 - \sum_{i\in[n]} m_i$ from the constraints $m_i + m_j \leq 1$ for any distinct $i, j \in [n]$.*

*Proof.* We have that

$$1 - \sum_{i\in[n]} m_i \equiv \left(1 - \sum_{i\in[n]} m_i\right)^2 + \sum_{\substack{i,j\in[n]\\ i<j}} \left(m_i^2 + m_j^2\right)(1 - m_i + m_j) \mod I_n$$

□

**Lemma 5.4.2.** *There is a constant degree SOS refutation of the additive encoding of $\text{Clique}_{n,k} \wedge \text{Color}_{n,\ell}$ for $k > \ell$. Moreover the refutation is of bit-complexity $\text{poly}(n)$, i.e. the refutation does not contain exceedingly large coefficients.*

*Proof.* We introduce a shorthand to make the proof a little more readable. Let $p_{ua}$ stand for the polynomial

$$\sum_{i\in[n]} x_{ui}y_{ia}.$$

The idea is that the polynomial $p_{ua}$ aims to capture the statement that the $u$th vertex of the clique is of color $a$.

Now our aim is to prove that both

$$\sum_{a\in[\ell]} p_{ua} \geq 1 \text{ for all } u \in [k] \tag{5.31}$$

and

$$\sum_{u\in[\ell]} p_{ua} \leq 1 \text{ for all } a \in [\ell] \tag{5.32}$$

have constant degree SOS proofs of non-negativity from $\text{Clique}_{n,k} \wedge \text{Color}_{n,\ell}$. With these we reach a contradiction as

$$\ell - k = \sum_{u\in[\ell]} \left( \sum_{a\in[\ell]} p_{ua} - 1 \right) + \sum_{a\in[k]} \left( 1 - \sum_{u\in[\ell]} p_{ua} \right)$$

It is straightforward to derive (5.31). Namely, we have that

$$\sum_{a\in[\ell]} p_{ua} - 1 \equiv \sum_{i\in[n]} x_{ui}^2 \left( \sum_{a\in[\ell]} y_{ia} - 1 \right) + \left( \sum_{i\in[n]} x_{ui} - 1 \right) \mod I_n$$

Secondly to derive (5.32), we show that for any two distinct monomials $m_1$ and $m_2$ from the sum $\sum_{u\in[\ell]} p_{ua}$, there is a constant degree SOS proof of non-negativity of $1 - m_1 - m_2$ from $\text{Clique}_{n,k} \wedge \text{Color}_{n,\ell}$. Then the claim follows by Lemma 5.4.1.

If $m_1 = x_{ui}y_{ia}$ and $m_2 = x_{uj}y_{ja}$ for distinct $i$ and $j$, then

$$1 - x_{ui}y_{ia} - x_{uj}y_{ja} \equiv (x_{ui} - x_{ui}y_{ia})^2 + (x_{uj} - x_{uj}y_{ja})^2 + (1 - x_{ui} - x_{uj}) \mod I_n$$

If on the other hand $m_1 = x_{ui}y_{ia}$ and $m_2 = x_{vi}y_{ia}$ for distinct $u$ and $v$, then

$$1 - x_{ui}y_{ia} - x_{vi}y_{ia} \equiv \bar{y}_{ia}^2 + y_{ia}^2(1 - x_{ui} - x_{vi}) \mod I_n$$

Finally for the most interesting case, when $m_1 = x_{ui}y_{ia}$ and $m_2 = x_{vj}y_{ja}$ for distinct $i$ and $j$, and distinct $u$ and $v$, we have that

$$\begin{aligned} 1 - x_{ui}y_{ia} - x_{vj}y_{ja} \equiv (1 - x_{ui}y_{ia} - x_{vj}y_{ja} + x_{ui}y_{ia}x_{vj}y_{ja})^2 \\ + (x_{ui}y_{ia}x_{vj}y_{ja})^2(\bar{x}_{ui} + \bar{x}_{vj} + z_{ij} - 1) \\ + (x_{ui}y_{ia}x_{vj}y_{ja})^2(\bar{y}_{ia} + \bar{y}_{ja} + \bar{z}_{ij} - 1) \mod I_n \end{aligned}$$

□

Unfortunately it seems that the above proof does not translate to give poly-sized Sherali-Adams refutations of $\text{Clique}_{n,k} \wedge \text{Color}_{n,\ell}$. The problem comes down to Lemma 5.4.1: Sherali-Adams can easily prove Lemma 5.4.1 in case all monomials $m_i$ are actually just variables. However with monomials of degree more than 1, the Sherali-Adams proof of $1 - \sum_{i\in[n]} m_i$ from the constraints $m_i + m_j \leq 1$ seems to blow up exponentially in size.

# Chapter 6

# Bit-complexity vs. Monomial-size in Polynomial Calculus and Sums-of-Squares

In this chapter we consider the relationship between monomial-size and bit-complexity in Polynomial Calculus Resolution over rationals and Sums-of-Squares. We show that there is an unsatisfiable set $Q$ of polynomial equality constraints in $O(n^2)$ Boolean variables that has both PCR/$\mathbb{Q}$ and SOS refutations of degree 2 and with polynomially many monomials in $n$, but which requires exponential bit-complexity to refute in both systems.

O'Donnell considered the bit-complexity of Sums-of-Squares proofs in [66] in connection with degree automatability of Sums-of-Squares proofs. O'Donnell showed that there is a set of polynomial constraints $Q_1$ (in non-Boolean variables) and a polynomial $p$ such that $p$ has a degree 2 proofs of non-negativity from $Q_1$, but any degree 2 proof requires coefficients of doubly exponential magnitude. This shows that a degree $d$ Sums-of-Squares proof cannot always be found, if one exists, in time $n^{O(d)}$. O'Donnell's example however has small proofs of degree 4.

A more severe example was given by Raghavendra and Weitz in [78]. They gave an example of a set $Q_2$ of polynomial constraints in $O(n^2)$ Boolean variables and a polynomial $q$ that has degree 2 proofs of non-negativity from

$Q_2$, but any proof of degree $O(n)$ requires coefficients of magnitude doubly exponential in $n$. Their example is built on O'Donnell's by replacing every non-Boolean variable by an instance of Knapsack. The proof uses Grigoriev's degree lower bound for Knapsack in Sums-of-Squares [36] and the degree $O(n)$ pseudoexpectations for Knapsack provided by the degree lower bound, and completeness of degree bounded pseudoexpectations operators.

For Polynomial Calculus it has also often been stated that a degree $d$ Polynomial Calculus proofs can be found in time $n^{O(d)}$ if they exist. This is certainly true over finite fields as already observed in Section 5.1.2. However for Polynomial Calculus over reals or rationals there is no way to control the potential coefficient bloat in the proof search algorithm of Section 5.1.2.

The example of Raghavendra and Weitz leaves however open the possibility that there are proofs of non-negativity of $q$ from $Q_2$ of polynomial bit-complexity. Our result implies that this is not the case. Our set of constraints is built, in turn, from that of [78] by adjoining an additional constraints to their set of constraints. We consider here an unsatisfiable set of constraints especially, since this allows us to translate the result also to Polynomial Calculus.

For Sums-of-Squares we prove a trade-off result between the number of monomials and the size of coefficients appearing in the refutations of our set of constraints $Q$. We prove that any Sums-of-Squares refutation of $Q$ that uses less than exponentially many monomials in $n$ must contain a coefficient of doubly exponential magnitude in $n$. Our proof is similar to the proof of Raghavendra and Weitz, but we use a lower bound on the number of distinct significant monomials in any refutation of Knapsack given by Grigoriev's degree lower bound [36] and Theorem 4.4.3, and pseudoexpectations over sets of monomials given by the lower bound and Theorem 3.2.8.

For Polynomial Calculus Resolution over rationals we prove a three-way trade-off showing that any PCR/$\mathbb{Q}$ refutation of $Q$ with coefficients smaller than doubly exponential in $n$, and with less than exponentially many monomials in $n$, must be of height exponential in $n$. This proof uses the p-simulation of PCR/$\mathbb{Q}$ by SOS as proved in Section 3.4, which gives bounds on the SOS simulation in terms of the size of coefficients and

the height of the given PCR/$\mathbb{Q}$ refutation. Originally the fact that SOS p-simulates PCR/$\mathbb{Q}$ was proved in [15].

## 6.1 The constraints

In this section we introduce the set of constraints that we use to prove our claims about lower bounds on bit-complexity.

Recall first the knapsack constraint KNAPSACK$(n, k)$:

$$x_1 + \ldots + x_n = k.$$

If $k$ is not an integer, the constraint is unsatisfiable over the Boolean values. However, for any $\varepsilon$ strictly between 0 and 1, KNAPSACK$(2n, n+\varepsilon)$ requires degree at least $2n$ to refute in SOS [36].

Now, by Theorem 4.4.3, to refute KNAPSACK$(2n, n + \varepsilon)$ in SOS one needs at least $s_n$ distinct significant monomials, where

$$s_n = \exp\left(\frac{(2n-5)^2}{32(2n+1)}\right).$$

A lower bound of the same order for the monomial-size was also obtained earlier in [39] using more ad hoc methods.

For our purposes it is important that our lower bound is for the number of distinct significant monomials. It follows that for any $\varepsilon$ strictly between 0 and 1 and for any set $S$ of monomials containing all the variables and the empty monomial 1 of size less than $s_n$, there is no SOS refutation of KNAPSACK$(2n, n + \varepsilon)$ over $S$, and thus, by Theorem 3.2.8 there is a pseudoexpectation for KNAPSACK$(2n, n + \varepsilon)$ over $S$. This property will be key in the proof of Theorem 6.3.1.

Now we turn to the set of constraints we consider here. The set is slightly modified from [78], we add the constraint (6.1) in order to obtain an unsatisfiable set of constraints.

For each $i \in [n]$, introduce $2n$ variables $x_{ij}$, $j \in [2n]$. Denote by $\mathrm{ks}_i$ the polynomial $\sum_{j\in[2n]} x_{ij} - n$. Note that the constraint $\mathrm{ks}_i = \varepsilon$ is just the constraint KNAPSACK$(2n, n + \varepsilon)$ in the variables $x_{ij}, j \in [2n]$. Denote by $Q_n$ the following set of constraints

- $\mathrm{ks}_1 = 1/2$; (6.1)
- $\mathrm{ks}_i^2 = \mathrm{ks}_{i+1}$ for each $i \in [n-1]$; (6.2)
- $\mathrm{ks}_n^2 = 0$. (6.3)

Now, as noted above already, the constraint (6.1) is by itself unsatisfiable over the Boolean cube. However, both PCR/$\mathbb{Q}$ and SOS require linear degree to refute (6.1) by itself. The role of (6.2) and (6.3) is two-fold: on one hand they decrease the degree needed to refute the constraints, but the repeated squaring inherent in the constraints also forces the coefficients to blow-up.

## 6.2 The upper bounds

In this section we show that both PCR/$\mathbb{Q}$ and SOS have refutations of $Q_n$ of degree 2 and of monomial-size polynomial in $n$. Each of these refutations however uses coefficients of exponential bit-complexity in $n$ and thus the refutations themselves have bit-complexities that are exponential in $n$. In the next section we show that exponential bit-complexities are necessary for both PCR/$\mathbb{Q}$ and SOS.

**Lemma 6.2.1.** *There is a PCR/$\mathbb{Q}$ refutation of $Q_n$ of degree 2 and of monomial-size* poly$(n)$.

*Proof.* We prove by induction that for any $i \in [n]$ there is a PCR/$\mathbb{Q}$ proof of $\mathrm{ks}_i^2 = 1/2^{2^i}$ from $Q_n$ of degree 2 and monomial-size poly$(n)$. For $i = 1$, we obtain this as follows. First derive $\mathrm{ks}_1^2 = \mathrm{ks}_1/2$ from $\mathrm{ks}_1 = 1/2$. This can be done in $n+1$ steps, in degree 2 and with polynomially many monomials. Secondly derive $\mathrm{ks}_1/2 = 1/4$ from $\mathrm{ks}_1 = 1/2$. This can be done in one step. Finally combine the two derivations to obtain a derivation of $\mathrm{ks}_1^2 = 1/4$.

Suppose then that we have a proof of $\mathrm{ks}_i^2 = 1/2^{2^i}$ from $Q_n$. We derive $\mathrm{ks}_{i+1}^2 = 1/2^{2^{i+1}}$ as follows. First derive $\mathrm{ks}_{i+1} = 1/2^{2^i}$ from $\mathrm{ks}_i^2 = 1/2^{2^i}$ and $\mathrm{ks}_i^2 = \mathrm{ks}_{i+1}$. Secondly derive both $\mathrm{ks}_{i+1}^2 = \mathrm{ks}_{i+1}/2^{2^i}$ and $\mathrm{ks}_{i+1}/2^{2^i} = 1/2^{2^{i+1}}$ from $\mathrm{ks}_{i+1} = 1/2^{2^i}$, and combine these to obtain a proof of $\mathrm{ks}_{i+1}^2 = 1/2^{2^{i+1}}$.

In the end we have a proof of $\mathrm{ks}_n^2 = 1/2^{2^n}$ from $Q_n$ of degree 2 and of monomial-size $\mathrm{poly}(n)$. By combining this with the axiom $\mathrm{ks}_n^2 = 0$ we reach a contradiction. Note that this last step involves a multiplication by a coefficient of doubly exponential magnitude. □

**Lemma 6.2.2.** *There is an SOS refutation of $Q_n$ of degree 2 and of monomial-size $\mathrm{poly}(n)$.*

*Proof.* The following is an SOS refutation of $Q_n$:

$$-1 = \sum_{i\in[n]} \left(\frac{1 - 2n^{2^{i-1}}\mathrm{ks}_i}{\sqrt{n}}\right)^2 + 4\left(\mathrm{ks}_1 - \frac{1}{2}\right) - \sum_{i\in[n-1]} 4n^{2^i-1}\left(\mathrm{ks}_i^2 - \mathrm{ks}_{i+1}\right) - 4n^{2^n-1}\mathrm{ks}_n^2$$

□

## 6.3 Lower bound for Sums-of-Squares

In this section we prove our main claim about bit-complexity of SOS refutations. The proof of the claim is very similar to the one in [78] with the use of $S$-pseudoexpectations instead of degree bounded pseudoexpectations being the central novel idea in the proof.

For a monomial $m$ in variables $x_{ij}, i \in [n], j \in [2n]$, for each $i \in [n]$ denote by $m_i$ the monomial in variables $x_{ij}, j \in [2n]$ such that $m = m_1 \cdots m_n$. For any $I \subseteq [n]$ let $m_I = \prod_{i\in I} m_i$. We call $m_i$ and $m_I$ the projections of $m$ to index $i$ and set $I$, respectively. For a set $S$ of monomials in variables $x_{ij}, i \in [n], j \in [2n]$, denote by $S_i$ and $S_I$ the sets of projections of all elements of $S$ to index $i$ and set $I$, respectively.

**Theorem 6.3.1.** *There is a constant $c > 0$ such that for large enough $n$, any SOS refutation of $Q_n$ has at least $2^{cn}$ distinct explicit monomials or contains a coefficient of magnitude at least $2^{2^n}/2^{cn}$.*

*Proof.* Let $c$ be such that $s_n \geq 2^{2cn}$ for large enough $n$. Let $n$ be large enough, let $\Pi$ be an SOS refutation of $Q_n$ with less than $2^{cn}$ distinct explicit

monomials and let $S$ be the set of explicit monomials appearing in the refutation $\Pi$. Now $S_i^2$ has size less than $s_n$ for any $i \in [n]$. Now by Section 6.1 and by Theorem 3.2.8, for any $i \in [n]$ there is a pseudoexpectation $E_i$ for $\{\mathrm{ks}_i = 1/2^{2^{i-1}}\}$ over $S_i^2$.

Now define a linear functional $E\colon \mathbb{R}[S^2] \to \mathbb{R}$ as follows: for each $m \in S^2$ let

$$E(m) := E_1(m_1) \cdots E_n(m_n),$$

and extend linearly to the whole of $\mathbb{R}[S^2]$.

We prove that $E$ has the following properties:

- $E(1) = 1$; (6.4)
- $E(p^2) \geq 0$ for any $p \in \mathbb{R}[S]$; (6.5)
- $E(m(x_{ij}^2 - x_{ij})) = 0$ for any $i \in [n]$, $j \in [2n]$ and $m \in S$; (6.6)
- $E(m(\bar{x}_{ij}^2 - \bar{x}_{ij})) = 0$ for any $i \in [n]$, $j \in [2n]$ and $m \in S$; (6.7)
- $E(m(x_{ij} + \bar{x}_{ij} - 1)) = 0$ for any $i \in [n]$, $j \in [2n]$ and $m \in S$; (6.8)
- $E(m(\mathrm{ks}_1 - 1/2)) = 0$ for any $m \in S$; (6.9)
- $E(m(\mathrm{ks}_i^2 - \mathrm{ks}_{i+1})) = 0$ for any $i \in [n-1]$ and $m \in S$; (6.10)
- $|E(p\mathrm{ks}_n^2)| \leq |S|\|p\|_\infty / 2^{2^n}$ for any polynomial $p \in \mathbb{R}[S]$. (6.11)

Now applying $E$ to the given refutation $\Pi$, we have that $-1 \geq E(p\mathrm{ks}_n^2)$, where $p$ is the lift of $\mathrm{ks}_n^2 = 0$ in $\Pi$, and thus

$$1 \leq |E(p\mathrm{ks}_n^2)| \leq |S|\|p\|_\infty / 2^{2^n}.$$

By rearranging the inequality we obtain that

$$\|p\|_\infty \geq 2^{2^n}/|S| \geq 2^{2^n}/2^{cn}.$$

Finally we prove that $E$ has the desired properties. (6.4) follows since $E_i(1) = 1$ for any $i \in [n]$.

To see that (6.5) holds, define for each $i \in [n]$, a linear function $T_i$ with $T_i(m) = E_i(m_i) \prod_{i' \neq i} m_{i'}$. Now clearly $E(m) = T_1(T_2(\ldots T_n(m)\ldots))$. We show that for any $i \in [n]$ and any $p \in \mathbb{R}[S_{[i]}]$, $T_i(p^2)$ is a sum of squares

of polynomials in $\mathbb{R}[S_{[i-1]}]$, where $S_{[i]}$ is the projection of $S$ to the initial segment $[i]$. To simplify notation, we prove the case when $i = 2$. The general case is not conceptually any harder. So write $p$ as

$$\sum_{\alpha}\sum_{\beta} a_{\alpha\beta}x_1^{\alpha}x_2^{\beta},$$

where $x_1$ and $x_2$ are sequences of the variables in $S_1$ and $S_2$, respectively. Now

$$T_2(p^2) = \sum_{\alpha,\alpha'}\sum_{\beta,\beta'} a_{\alpha\beta}a_{\alpha'\beta'}x_1^{\alpha}x_1^{\alpha'}E_2(x_2^{\beta}x_2^{\beta'}).$$

Now the matrix $(E_2(x_2^{\beta}x_2^{\beta'}))_{\beta,\beta'}$ is positive semidefinite, and so there are some vectors $u$ such that $E_2(x_2^{\beta}x_2^{\beta'}) = \sum_u u_\beta u_{\beta'}$. Now

$$\begin{aligned} T_2(p^2) &= \sum_{\alpha,\alpha'}\sum_{\beta,\beta'} a_{\alpha\beta}a_{\alpha'\beta'}x_1^{\alpha}x_1^{\alpha'}\sum_u u_\beta u_{\beta'} \\ &\sum_{\alpha,\alpha'}(\sum_{\beta}\sum_{u} a_{\alpha\beta}u_\beta)(\sum_{\beta'}\sum_{u} a_{\alpha'\beta'}u_{\beta'})x_1^{\alpha}x_1^{\alpha'} \\ &= (\sum_{\alpha}\sum_{\beta}\sum_{u} a_{\alpha\beta}u_\beta x^{\alpha})^2 \end{aligned}$$

For (6.6), we have that $E(m(x_{ij}^2 - x_{ij})) = E_i(m_i(x_{ij}^2 - x_{ij}))\prod_{i'\neq i} E_{i'}(m_{i'}) = 0$, since $E_i(m_i(x_{ij}^2 - x_{ij})) = 0$. The items (6.7) and (6.8) are proved similarly.

For (6.9), we have that

$$E(m(\mathrm{ks}_1 - 1/2)) = E_1(m_1(\mathrm{ks}_1 - 1/2))\prod_{i'\neq 1} E_{i'}(m_{i'}) = 0,$$

since $E_1(m_1(\mathrm{ks}_1 - 1/2)) = 0$ as $E_1$ is a pseudoexpectation for $\{\mathrm{ks}_1 = 1/2\}$ over $S_1^2$.

For (6.10) we evaluate the terms $E(m\mathrm{ks}_i^2)$ and $E(m\mathrm{ks}_{i+1})$ separately and show that they are equal. Firstly we have that

$$\begin{aligned} E(m\mathrm{ks}_i^2) &= E_i(m_i\mathrm{ks}_i^2)\prod_{i'\neq i} E_{i'}(m_{i'}) \\ &= E_i(m_i\mathrm{ks}_i/2^{2^{i-1}})\prod_{i'\neq i} E_{i'}(m_{i'}) \\ &= E_i(m_i/\left(2^{2^{i-1}}\right)^2)\prod_{i'\neq i} E_{i'}(m_{i'}) \\ &= E(m)/2^{2^i}. \end{aligned}$$

Here the second equality follows from the facts that $E_i$ is a pseudoexpectation for $\{\mathrm{ks}_i = 1/2^{2^{i-1}}\}$ over $S_i^2$ and all the monomials from the polynomial $m_i\mathrm{ks}_i$ are among $S_i^2$. The third equality follows similarly, since the monomials $m_i$ is among $S_i^2$.

Secondly we have that

$$\begin{aligned} E(m\mathrm{ks}_{i+1}) &= E_{i+1}(m_{i+1}\mathrm{ks}_{i+1}) \prod_{i' \neq i+1} E_{i'}(m_{i'}) \\ &= E_{i+1}(m_{i+1})/2^{2^i} \prod_{i' \neq i+1} E_{i'}(m_{i'}) \\ &= E(m)/2^{2^i}, \end{aligned}$$

where the second equality follows since $E_{i+1}$ is a pseudoexpectation for $\{\mathrm{ks}_{i+1} = 1/2^{2^i}\}$ over $S_{i+1}^2$, and $m_{i+1}$ is in $S_{i+1}^2$.

Finally for (6.11) first note that for any $m \in S$ we have that

$$\begin{aligned} E(m\mathrm{ks}_n^2) &= E_n(m_n\mathrm{ks}_n^2) \prod_{i<n} E_i(m_i) \\ &= E_n(m_n\mathrm{ks}_n)/2^{2^{n-1}} \prod_{i<n} E_i(m_i) \\ &= E_n(m_n)/\left(2^{2^{n-1}}\right)^2 \prod_{i<n} E_i(m_i) \\ &= E(m)/2^{2^n}. \end{aligned}$$

Here the second equality follows again from the facts that $E_n$ is a pseudoexpectation for $\{\mathrm{ks}_n = 1/2^{2^{n-1}}\}$ over $S_n^2$ and all the monomials from the polynomial $m_n\mathrm{ks}_n$ are among $S_n^2$. The third equality follows similarly, since the monomials $m_n$ is among $S_n^2$.

Now write $p = \sum_{m \in S} a_m m$. We have that

$$\begin{aligned} |E(p\mathrm{ks}_n^2)| &= |E(p)/2^{2^n}| \\ &\leq \sum_{m \in S} |a_m E(m)|/2^{2^n} \\ &\leq |S|\|p\|_\infty/2^{2^n}, \end{aligned}$$

where the last inequality follows from the fact that $0 \leq E(m) \leq 1$. This in turn follows from previous items as for any $m \in S$ we have that $m \equiv m^2 \mod I_n$ and $1 - m \equiv (1-m)^2 \mod I_n$. □

As a corollary to the above theorem, we obtain the following lower bound for the bit-complexity of SOS refutations.

**Corollary 6.3.2.** *Any SOS refutation of $Q_n$ has bit-complexity $2^{\Omega(n)}$.*

## 6.4 Lower bound for Polynomial Calculus

Finally in this section we prove an analogue of Theorem 6.3.1 for Polynomial Calculus Resolution over rationals. Already from the Corollary 6.3.2 alone we obtain lower bounds on the bit-complexity of PCR/$\mathbb{Q}$ refutations of $Q_n$ using the simulation of [15]. It is however instructive to prove an analogue of Theorem 6.3.1 also for PCR/$\mathbb{Q}$.

For SOS we were able to pinpoint exactly where the large coefficient resides in an SOS refutation that uses too few monomials: it must reside in the lift of the constraint $\mathrm{ks}_n^2 = 0$. However for PCR/$\mathbb{Q}$ we will not be able to be this precise. Moreover we need to bring height of the refutation also into the picture. We show that any PCR/$\mathbb{Q}$ refutation that uses only few monomials and coefficients of small magnitude must be very tall.

To prove the theorem for Polynomial Calculus we use the simulation of Lemma 3.4.2. The important thing here is that the lemma gives explicit bounds on coefficients in the SOS simulation in terms of the height of a given PCR/$\mathbb{Q}$ refutation. This is how we bring the height of a PCR/$\mathbb{Q}$ refutation also into the picture.

For any set $S$ of monomials, let $\tilde{S}$ denote some minimal set of monomials so that there for any $m \in S^2$ there are $u_i, v_i \in \tilde{S}$ such that

$$\bar{m} - m = \sum_{i \in [n]} \big( u_i(x_i^2 - x_i) + v_i(\bar{x}_i^2 - \bar{x}_i) \big),$$

where $\bar{m}$ denotes the multilinearization of $m$. In other words $\tilde{S}$ contains just enough monomials in order to certify the equivalence of each $m \in S^2$ to its multilinearization. It is clear that for any $S$ there is $\tilde{S}$ of size polynomial in the size of $S$ and the maximum degree of a monomial in $S$.

**Theorem 6.4.1.** *There are constants $c > 0$ and $d > 0$ such that for large enough $n$, every $2^{2^{n/2}}$-bounded PCR/$\mathbb{Q}$ refutation of $Q_n$ that uses at most $2^{dn}$ different monomials has height at least*

$$2^{n/2-2} - \frac{cn}{2^{n/2+2}} - \frac{5}{4}.$$

*Proof.* Let $c$ be as in Theorem 6.3.1, and let $d$ be such that for any set $S$ of monomials of size at most $2^{dn}$ with maximum degree at most $10n$, the size of $S \cup \tilde{S}$ is less than $2^{cn}$ for large enough $n$. Let $n$ be large enough and let $\Pi$ be a $2^{2^{n/2}}$-bounded PCR/$\mathbb{Q}$ refutation of $Q_n$ of height $h$ that uses at most $2^{dn}$ different monomials. Without a loss of generality we may assume that the degree of $\Pi$ is at most $10n$. Let $S$ be the set of all monomials in the refutation. Now by Lemma 3.4.2, there is an $2^{2^{n/2}(4h+5)}$-bounded SOS refutation of $Q_n$ over $S$.

We may assume that the explicit monomials of the SOS refutation are among $S \cup \tilde{S}$. Now the size of $S \cup \tilde{S}$ is less that $2^{cn}$. Thus, by the proof of Theorem 6.3.1, the lift of the constraint $\mathrm{ks}_n^2 = 0$ contains a coefficient of magnitude at least $2^{2^n}/2^{cn}$.

Putting everything together we obtain that

$$2^{2^{n/2}(4h+5)} \geq 2^{2^n}/2^{cn}.$$

After solving for $h$ we obtain the wanted lower bound for the height. □

We obtain a lower bound on bit-complexity for Polynomial Calculus as a corollary to the above theorem.

**Corollary 6.4.2.** *Any PCR/$\mathbb{Q}$ refutation of $Q_n$ has bit-complexity $2^{\Omega(n)}$.*

# Chapter 7

# Conclusion and future work

We conclude by considering some open questions related to the work presented in this thesis.

### Size-degree trade-offs for Sums-of-Squares and Sherali-Adams

Most important question here is whether the $O(\sqrt{n \log(s)}+k)$ upper bound in the degree-reduction lemma is tight? For Resolution and Polynomial Calculus, whose size-width/degree trade-offs adopt the same form, the bound is known to be tight. In both cases different version of the ordering principle witnesses the necessity of the square root of the number of variables in the upper bound [17, 34]. Similarly for Sherali-Adams the ordering principle gives a tight example of the trade-off [25]. Interestingly, also the pigeonhole principle $\mathrm{PHP}_n^{n+1}$ is a tight example for the trade-off for Sherali-Adams [25, 7].

It was recently shown by Potechin that the total ordering principle, which has $N = n(n-1)$ variables, can be refuted in SOS in degree $O(\sqrt{n})$, whence in degree $O(\sqrt[4]{N})$ [71]. Since the relationship between $N$ and $\sqrt{n}$ is a 4th root, this means that the total ordering principle cannot be used for witnessing the necessity of the square root of the number of variables in our theorem. The degree upper of $\sqrt[4]{N}$ for the total ordering principle is also known to be essentially tight [71].

A note is in order about the encoding Potechin uses. Rather than en-

coding the wide clauses in the total ordering principle as linear inequality constraints, Potechin uses auxiliary non-Boolean variables $z_i$ for any $i \in [n]$ and encodes the wide clause with

- $\sum_{j \neq i} x_{ji} = 1 + z_i^2$. (7.1)

Hence the upper bound does not immediately apply to the situation considered here with only Boolean variables. In the appendix of [71], Potechin sketches out a solution by replacing the single auxiliary variables $z_i$ by a bunch of Boolean auxiliary variables.

We want to point out here that both the upper bound and the lower bound of [71] apply also for the encoding with Boolean inequality constraints instead of (7.1). For the lower bound this follows, since one can easily simulate an SOS refutation that uses the encoding with inequality constraints using the encoding (7.1). For the upper bound, a close look at Potechin's proof reveals that only a minor rewording of the proof gives the upper bound also for encoding with the wide clauses encoded as inequality constraints.

The remaining question is thus whether one can find an example that shows that the upper bound given by the degree-reduction lemma is tight for SOS, or whether one can improve the bound given by the lemma. The proof of the upper bound in [71] uses the totality of the order in an essential way, and thus leaves open the possibility that by relaxing the principle to a partial ordering principle we could still obtain a tight example from the ordering principle for the size-degree trade-off of SOS.

A second important open question concerns both SOS and SA, and the interplay of the two complexity measures considered, degree and monomial size. In the proof of the size-degree trade-off we show how to transform a refutation with a small number of monomials into a refutation of small degree. This transformation however blows up the number of monomials exponentially. The question is thus whether this blow-up is necessary, or whether one can minimize both measures simultaneously. For Resolution and Polynomial Calculus, the necessity of (a superpolynomial) blow-up has been demonstrated in [89] and [58], respectively. In short, both papers

show that there is a CNF that has both polynomially sized refutations of relatively high degree, and refutations of small degree, but for which any refutation of minimal degree must have superpolynomially many monomials.

### Feasible interpolation for Polynomial Calculus, Sums-of-Squares and Sherali-Adams

We have seen that Sums-of-Squares cannot admit monotone feasible interpolation with respect to polynomial-sized monotone Boolean circuits. Pudlák and Sgall prove in [75] that degree bounded Polynomial Calculus admits monotone feasible interpolation with respect to monotone polynomial programs. Also recently Fleming et al proved in [32] that Sherali-Adams admits a monotone feasible interpolation with respect to monotone linear programming circuits. It is however open whether one can prove monotone feasible interpolation for Polynomial Calculus or Sherali-Adams with respect to monotone Boolean circuits.

We obtain feasible interpolation for Polynomial Calculus only over finite fields, since we have the poly-time search algorithm for PC proofs over a set of monomials only over finite fields (See Remark 5.1.3). However, as Polynomial Calculus is deductive proof system, it is most likely that one can give a syntactic proof, similar to the one for Resolution [56], of the feasible interpolation property for PC. Such syntactic proof might give new insights into the issue of bit-complexity, and better handle on the size of the coefficients.

Finally we want to emphasize that although we proved the feasible interpolation for Sums-of-Squares and Sherali-Adams only over the $\{0,1\}$-values, the argument works equally well for Boolean values over the $\pm 1$ basis.

### Bit-complexity of PCR/$\mathbb{Q}$ and SOS refutations

From the point of view of proof complexity the most important open question related to Chapter 6 is whether the phenomenon presented in the chapter can occur when the set of constraints comes from a translation of a CNF,

or whether the monomial size and bit-complexity are polynomially equivalent when PCR/$\mathbb{R}$ or SOS is considered as a refutation system for CNFs. The constraints in Chapter 6 do not arise from any CNF.

# Bibliography


[1] Michael Alekhnovich, Eli Ben-Sasson, Alexander A. Razborov, and Avi Wigderson. Space complexity in propositional calculus. *SIAM J. Comput.*, 31(4):1184–1211, 2002. doi:10.1137/S0097539700366735.

[2] Michael Alekhnovich and Alexander A. Razborov. Lower bounds for polynomial calculus: Non-binomial case. In *42nd Annual Symposium on Foundations of Computer Science, FOCS 2001, 14-17 October 2001, Las Vegas, Nevada, USA*, pages 190–199. IEEE Computer Society, 2001. doi:10.1109/SFCS.2001.959893.

[3] Noga Alon and Ravi B. Boppana. The monotone circuit complexity of boolean functions. *Comb.*, 7(1):1–22, 1987. doi:10.1007/BF02579196.

[4] Elizabeth A. Arnold. Modular algorithms for computing Gröbner bases. *J. Symb. Comput.*, 35(4):403–419, 2003. doi:10.1016/S0747-7171(02)00140-2.

[5] Albert Atserias and Víctor Dalmau. A combinatorial characterization of resolution width. *J. Comput. Syst. Sci.*, 74(3):323–334, 2008. doi:10.1016/j.jcss.2007.06.025.

[6] Albert Atserias and Tuomas Hakoniemi. Size-Degree Trade-Offs for Sums-of-Squares and Positivstellensatz Proofs. In Amir Shpilka, editor, *34th Computational Complexity Conference (CCC 2019)*, volume 137 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 24:1–24:20, Dagstuhl, Germany, 2019. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. doi:10.4230/LIPIcs.CCC.2019.24.

[7] Albert Atserias and Massimo Lauria. Circular (yet sound) proofs. In Mikolás Janota and Inês Lynce, editors, *Theory and Applications of Satisfiability Testing - SAT 2019 - 22nd International Conference, SAT 2019, Lisbon, Portugal, July 9-12, 2019, Proceedings*, volume 11628 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 2019. doi:10.1007/978-3-030-24258-9_1.

[8] Albert Atserias, Massimo Lauria, and Jakob Nordström. Narrow proofs may be maximally long. *ACM Trans. Comput. Log.*, 17(3):19:1–19:30, 2016. Preliminary version in CCC 2014. doi:10.1145/2898435.

[9] Boaz Barak, Fernando G. S. L. Brandão, Aram Wettroth Harrow, Jonathan A. Kelner, David Steurer, and Yuan Zhou. Hypercontractivity, sum-of-squares proofs, and their applications. In *Proceedings of the 44th Symposium on Theory of Computing Conference, STOC 2012, New York, NY, USA, May 19 - 22, 2012*, pages 307–326, 2012. doi:10.1145/2213977.2214006.

[10] Boaz Barak and David Steurer. Sum-of-squares proofs and the quest toward optimal algorithms. In *Proceedings of International Congress of Mathematicians (ICM)*, 2014. URL: http://eccc.hpi-web.de/report/2014/059/.

[11] Paul Beame, Russell Impagliazzo, Jan Krajíček, Toniann Pitassi, and Pavel Pudlák. Lower bounds on hilbert's nullstellensatz and propositional proofs. *Proceedings of the London Mathematical Society*, s3-73(1):1–26, 1996. doi:10.1112/plms/s3-73.1.1.

[12] Paul Beame and Toniann Pitassi. Simplified and improved resolution lower bounds. In *37th Annual Symposium on Foundations of Computer Science, FOCS '96, Burlington, Vermont, USA, 14-16 October, 1996*, pages 274–282, 1996. doi:10.1109/SFCS.1996.548486.

[13] Eli Ben-Sasson and Russell Impagliazzo. Random cnf's are hard for the polynomial calculus. *Comput. Complex.*, 19(4):501–519, 2010. doi:10.1007/s00037-010-0293-1.

[14] Eli Ben-Sasson and Avi Wigderson. Short proofs are narrow - resolution made simple. *J. ACM*, 48(2):149–169, 2001. Preliminary version in STOC 1999. doi:10.1145/375827.375835.

[15] Christoph Berkholz. The Relation between Polynomial Calculus, Sherali-Adams, and Sum-of-Squares Proofs. In Rolf Niedermeier and Brigitte Vallée, editors, *35th Symposium on Theoretical Aspects of Computer Science (STACS 2018)*, volume 96 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 11:1–11:14, Dagstuhl, Germany, 2018. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. doi:10.4230/LIPIcs.STACS.2018.11.

[16] Maria Luisa Bonet, Carlos Domingo, Ricard Gavaldà, Alexis Maciel, and Toniann Pitassi. Non-automatizability of bounded-depth frege proofs. In *Proceedings of the 14th Annual IEEE Conference on Computational Complexity, Atlanta, Georgia, USA, May 4-6, 1999*, pages 15–23. IEEE Computer Society, 1999. doi:10.1109/CCC.1999.766258.

[17] Maria Luisa Bonet and Nicola Galesi. Optimality of size-width tradeoffs for resolution. *Computational Complexity*, 10(4):261–276, 2001. doi:10.1007/s000370100000.

[18] Maria Luisa Bonet, Toniann Pitassi, and Ran Raz. No feasible interpolation for tc0-frege proofs. In *38th Annual Symposium on Foundations of Computer Science, FOCS '97, Miami Beach, Florida, USA, October 19-22, 1997*, pages 254–263. IEEE Computer Society, 1997. doi:10.1109/SFCS.1997.646114.

[19] Samuel R. Buss. Lower bounds on nullstellensatz proofs via designs. In Paul Beam and Samuel R. Buss, editors, *Proof Complexity and Feasible Arithmetics, Proceedings of a DIMACS Workshop, New Brunswick, New Jersey, USA, April 21-24, 1996*, volume 39 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 59–71. DIMACS/AMS, 1996. doi:10.1090/dimacs/039/04.

[20] Samuel R. Buss, Dima Grigoriev, Russell Impagliazzo, and Toniann Pitassi. Linear gaps between degrees for the polynomial calculus modulo distinct primes. *J. Comput. Syst. Sci.*, 62(2):267–289, 2001. doi:10.1006/jcss.2000.1726.

[21] Eden Chlamtac and Madhur Tulsiani. Convex relaxations and integrality gaps. In Miguel F. Anjos and Jean B. Lasserre, editors, *Handbook on Semidefinite, Conic and Polynomial Optimization*, pages 139–169. Springer US, Boston, MA, 2012. doi:10.1007/978-1-4614-0769-0_6.

[22] Matthew Clegg, Jeff Edmonds, and Russell Impagliazzo. Using the groebner basis algorithm to find proofs of unsatisfiability. In Gary L. Miller, editor, *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996*, pages 174–183. ACM, 1996. doi:10.1145/237814.237860.

[23] Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. *Journal of Symbolic Logic*, 44(1):36–50, 1979. doi:10.2307/2273702.

[24] David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms*. Undergraduate Texts in Mathematics. Springer, fourth edition, 2015. doi:10.1007/978-3-319-16721-3.

[25] Stefan Dantchev, Barnaby Martin, and Mark Rhodes. Tight rank lower bounds for the sherali–adams proof system. *Theoretical Computer Science*, 410(21):2054 – 2063, 2009. doi:https://doi.org/10.1016/j.tcs.2009.01.002.

[26] Stefan S. Dantchev. Rank complexity gap for lovász-schrijver and sherali-adams proof systems. In *Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing*, STOC '07, page 311–317, New York, NY, USA, 2007. Association for Computing Machinery. doi:10.1145/1250790.1250837.

[27] Sanjeeb Dash. Exponential lower bounds on the lengths of some classes of branch-and-cut proofs. *Math. Oper. Res.*, 30(3):678–700, 2005. doi:10.1287/moor.1050.0151.

[28] Mateus de Oliveira Oliveira and Pavel Pudlák. Representations of monotone boolean functions by linear programs. *ACM Trans. Comput. Theory*, 11(4):22:1–22:31, 2019. doi:10.1145/3337787.

[29] G. L. Ebert. Some comments on the modular approach to gröbner-bases. *SIGSAM Bull.*, 17(2):28–32, may 1983. doi:10.1145/1089330.1089336.

[30] Yuval Filmus. Another look at degree lower bounds for polynomial calculus. *Theoretical Computer Science*, 796:286–293, 2019.

[31] Samuel Fiorini, Serge Massar, Sebastian Pokutta, Hans Raj Tiwary, and Ronald de Wolf. Linear vs. semidefinite extended formulations: exponential separation and strong lower bounds. In *Proceedings of the 44th Symposium on Theory of Computing Conference, STOC 2012, New York, NY, USA, May 19 - 22, 2012*, pages 95–106, 2012. doi:10.1145/2213977.2213988.

[32] Noah Fleming, Mika Göös, Stefan Grosser, and Robert Robere. On Semi-Algebraic Proofs and Algorithms. In Mark Braverman, editor, *13th Innovations in Theoretical Computer Science Conference (ITCS 2022)*, volume 215 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 69:1–69:25, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.ITCS.2022.69.

[33] Noah Fleming, Denis Pankratov, Toniann Pitassi, and Robert Robere. Random Θ(log n)-cnfs are hard for cutting planes. In Chris Umans, editor, *58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017, Berkeley, CA, USA, October 15-17, 2017*, pages 109–120. IEEE Computer Society, 2017. doi:10.1109/FOCS.2017.19.

[34] Nicola Galesi and Massimo Lauria. Optimality of size-degree tradeoffs for polynomial calculus. *ACM Trans. Comput. Log.*, 12(1):4:1–4:22, 2010. doi:10.1145/1838552.1838556.

[35] Dima Grigoriev. Tseitin's tautologies and lower bounds for nullstellensatz proofs. In *39th Annual Symposium on Foundations of Computer Science, FOCS '98, November 8-11, 1998, Palo Alto, California, USA*, pages 648–652. IEEE Computer Society, 1998. doi:10.1109/SFCS.1998.743515.

[36] Dima Grigoriev. Complexity of positivstellensatz proofs for the knapsack. *Computational Complexity*, 10(2):139–154, 2001. doi:10.1007/s00037-001-8192-0.

[37] Dima Grigoriev. Linear lower bound on degrees of positivstellensatz calculus proofs for the parity. *Theor. Comput. Sci.*, 259(1-2):613–622, 2001. doi:10.1016/S0304-3975(00)00157-2.

[38] Dima Grigoriev, Edward A. Hirsch, and Dmitrii V. Pasechnik. Complexity of semi-algebraic proofs. In *STACS 2002, 19th Annual Symposium on Theoretical Aspects of Computer Science, Antibes - Juan les Pins, France, March 14-16, 2002, Proceedings*, pages 419–430, 2002. doi:10.1007/3-540-45841-7_34.

[39] Dima Grigoriev, Edward A. Hirsch, and Dmitrii V. Pasechnik. Complexity of semi-algebraic proofs. In Helmut Alt and Afonso Ferreira, editors, *STACS 2002, 19th Annual Symposium on Theoretical Aspects of Computer Science, Antibes - Juan les Pins, France, March 14-16, 2002, Proceedings*, volume 2285 of *Lecture Notes in Computer Science*, pages 419–430. Springer, 2002. doi:10.1007/3-540-45841-7_34.

[40] Dima Grigoriev and Nicolai Vorobjov. Complexity of null-and positivstellensatz proofs. *Annals of Pure and Applied Logic*, 113(1-3):153–160, 2001. doi:10.1016/S0168-0072(01)00055-0.

[41] Martin Grötschel, László Lovász, and Alexander Schrijver. The ellipsoid method and its consequences in combinatorial optimization. *Combinatorica*, 1(2):169 – 197, June 1981. doi:10.1007/BF02579273.

[42] Martin Grötschel, László Lovász, and Alexander Schrijver. *Geometric Algorithms and Combinatorial Optimization*, volume 2 of *Algorithms and Combinatorics*. Springer-Verlag Berlin Heidelberg, 1993. doi:10.1007/978-3-642-78240-4.

[43] Armin Haken. The intractability of resolution. *Theoretical Computer Science*, 39:297–308, 1985. Third Conference on Foundations of Software Technology and Theoretical Computer Science. doi:10.1016/0304-3975(85)90144-6.

[44] Sören Halldén. On the semantic non-completeness of certain lewis calculi. *The Journal of Symbolic Logic*, 16(2):127–129, 1951. URL: http://www.jstor.org/stable/2266686.

[45] Pavel Hrubes and Pavel Pudlák. Random formulas, monotone circuits, and interpolation. In Chris Umans, editor, *58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017, Berkeley, CA, USA, October 15-17, 2017*, pages 121–131. IEEE Computer Society, 2017. doi:10.1109/FOCS.2017.20.

[46] Russell Impagliazzo, Pavel Pudlák, and Jirí Sgall. Lower bounds for the polynomial calculus and the gröbner basis algorithm. *Computational Complexity*, 8(2):127–144, 1999. doi:10.1007/s000370050024.

[47] D. M. Itsykson and A. A. Kojevnikov. Lower bounds on static lovász-schrijver calculus proofs for tseitin tautologies. *Journal of Mathematical Sciences*, 145(3):4942–4952, Sep 2007. Preliminary version in ICALP '06. doi:10.1007/s10958-007-0329-5.

[48] Cédric Josz and Didier Henrion. Strong duality in lasserre's hierarchy for polynomial optimization. *Optimization Letters*, 10(1):3–10, 2016. doi:10.1007/s11590-015-0868-5.

[49] Howard Karloff. *Linear Programming*. Modern Birkhäuser Classics. Birkhäuser Basel, address, 1991. doi:10.1007/978-0-8176-4844-2.

[50] L. G. Khachiyan. A polynomial algorithm in linear programming. *Dokl. Akad. Nauk SSSR*, 244(5):1093 – 1096, 1979.

[51] L.G. Khachiyan. Polynomial algorithms in linear programming. *USSR Computational Mathematics and Mathematical Physics*, 20(1):53 – 72, 1980. doi:10.1016/0041-5553(80)90061-0.

[52] Jan Krajícek. *Bounded arithmetic, propositional logic, and complexity theory*, volume 60 of *Encyclopedia of mathematics and its applications*. Cambridge University Press, 1995.

[53] Jan Krajícek. On frege and extended frege proof systems. In Peter Clote and Jeffrey B. Remmel, editors, *Feasible Mathematics II*, Progress in Computer Science and Applied Logic, pages 284–319. Birkhäuser Boston, 1995.

[54] Jan Krajícek and Pavel Pudlák. Some consequences of cryptographical conjectures for $s^1_2$ and EF. *Inf. Comput.*, 140(1):82–94, 1998. doi:10.1006/inco.1997.2674.

[55] Jan Krajíček. Lower bounds to the size of constant-depth propositional proofs. *Journal of Symbolic Logic*, 59(1):73–86, 1994. doi:10.2307/2275250.

[56] Jan Krajíček. Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic. *The Journal of Symbolic Logic*, 62(2):457–486, 1997. URL: http://www.jstor.org/stable/2275541.

[57] J. L. Krivine. Anneaux préordonnés. *Journal d'Analyse Mathématique*, 12(1):307–326, Dec 1964. doi:10.1007/BF02807438.

[58] Guillaume Lagarde, Jakob Nordström, Dmitry Sokolov, and Joseph Swernofsky. Trade-Offs Between Size and Degree in Polynomial Calculus. In Thomas Vidick, editor, *11th Innovations in Theoretical*

*Computer Science Conference (ITCS 2020)*, volume 151 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 72:1–72:16, Dagstuhl, Germany, 2020. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. doi:10.4230/LIPIcs.ITCS.2020.72.

[59] Jean B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM Journal on Optimization*, 11(3):796–817, 2001. doi:10.1137/S1052623400366802.

[60] Monique Laurent. Sums of squares, moment matrices and optimization over polynomials. In Mihai Putinar and Seth Sullivant, editors, *Emerging Applications of Algebraic Geometry*, pages 157–270. Springer New York, New York, NY, 2009. doi:10.1007/978-0-387-09686-5_7.

[61] Massimo Lauria and Jakob Nordström. Tight size-degree bounds for sums-of-squares proofs. *Computational Complexity*, 26(4):911–948, 2017. Preliminary version in CCC 2015. doi:10.1007/s00037-017-0152-4.

[62] James R. Lee, Prasad Raghavendra, and David Steurer. Lower bounds on the size of semidefinite programming relaxations. In *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing, STOC 2015, Portland, OR, USA, June 14-17, 2015*, pages 567–576, 2015. doi:10.1145/2746539.2746599.

[63] James R. Lee, Prasad Raghavendra, David Steurer, and Ning Tan. On the power of symmetric LP and SDP relaxations. In *IEEE 29th Conference on Computational Complexity, CCC 2014, Vancouver, BC, Canada, June 11-13, 2014*, pages 13–21, 2014. doi:10.1109/CCC.2014.10.

[64] László Lovász and Alexander Schrijver. Cones of matrices and set-functions and 0-1 optimization. *SIAM Journal on Optimization*, 1(2):166–190, 1991. doi:10.1137/0801013.

[65] Mladen Miksa and Jakob Nordström. A generalized method for proving polynomial calculus degree lower bounds. In David Zuckerman, editor,

*30th Conference on Computational Complexity, CCC 2015, June 17-19, 2015, Portland, Oregon, USA*, volume 33 of *LIPIcs*, pages 467–487. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2015. doi:10.4230/LIPIcs.CCC.2015.467.

[66] Ryan O'Donnell. SOS Is Not Obviously Automatizable, Even Approximately. In Christos H. Papadimitriou, editor, *8th Innovations in Theoretical Computer Science Conference (ITCS 2017)*, volume 67 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 59:1–59:10, Dagstuhl, Germany, 2017. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. doi:10.4230/LIPIcs.ITCS.2017.59.

[67] Ryan O'Donnell and Yuan Zhou. Approximability and proof complexity. In *Proceedings of the Twenty-Fourth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2013, New Orleans, Louisiana, USA, January 6-8, 2013*, pages 1537–1556, 2013. doi:10.1137/1.9781611973105.111.

[68] Pablo A. Parrilo. *Structured Semidefinite Programs and Semialgebraic Geometry Methods in Robustness and Optimization*. PhD thesis, California Institute of Technology, 2000.

[69] Vern I. Paulsen and Mark Tomforde. Vector spaces with an order unit. *Indiana University Mathematics Journal*, 58(3):1319–1359, 2009. URL: http://www.jstor.org/stable/24903253.

[70] Toniann Pitassi and Nathan Segerlind. Exponential lower bounds and integrality gaps for tree-like lovász-schrijver procedures. *SIAM J. Comput.*, 41(1):128–159, 2012. Preliminary version in SODA 2009. doi:10.1137/100816833.

[71] Aaron Potechin. Sum of Squares Bounds for the Ordering Principle. In Shubhangi Saraf, editor, *35th Computational Complexity Conference (CCC 2020)*, volume 169 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 38:1–38:37, Dagstuhl, Ger-

many, 2020. Schloss Dagstuhl–Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.CCC.2020.38.

[72] Pavel Pudlák. On the complexity of the propositional calculus. In S. Barry Cooper and John K. Truss, editors, *Sets and Proofs*, London Mathematical Society Lecture Note Series, pages 197 – 218. Cambridge University Press, 1999. doi:10.1017/CBO9781107325944.010.

[73] Pavel Pudlák. On reducibility and symmetry of disjoint NP pairs. *Theor. Comput. Sci.*, 295:323–339, 2003. doi:10.1016/S0304-3975(02)00411-5.

[74] Pavel Pudlák and Samuel R. Buss. How to lie without being (easily) convicted and the length of proofs in propositional calculus. In Leszek Pacholski and Jerzy Tiuryn, editors, *Computer Science Logic, 8th International Workshop, CSL '94, Kazimierz, Poland, September 25-30, 1994, Selected Papers*, volume 933 of *Lecture Notes in Computer Science*, pages 151–162. Springer, 1994. doi:10.1007/BFb0022253.

[75] Pavel Pudlák and Jirí Sgall. Algebraic models of computation and interpolation for algebraic proof systems. In Paul Beame and Samuel R. Buss, editors, *Proof Complexity and Feasible Arithmetics, Proceedings of a DIMACS Workshop, New Brunswick, New Jersey, USA, April 21-24, 1996*, volume 39 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 279–295. DIMACS/AMS, 1996. doi:10.1090/dimacs/039/15.

[76] Pavel Pudlák. Lower bounds for resolution and cutting plane proofs and monotone computations. *Journal of Symbolic Logic*, 62(3):981–998, 1997. doi:10.2307/2275583.

[77] Mihai Putinar. Positive polynomials on compact semi-algebraic sets. *Indiana University Mathematics Journal*, 42(3):969–984, 1993. URL: http://www.jstor.org/stable/24897130.

[78] Prasad Raghavendra and Benjamin Weitz. On the Bit Complexity of Sum-of-Squares Proofs. In Ioannis Chatzigiannakis, Piotr Indyk,

Fabian Kuhn, and Anca Muscholl, editors, *44th International Colloquium on Automata, Languages, and Programming (ICALP 2017)*, volume 80 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 80:1–80:13, Dagstuhl, Germany, 2017. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. doi:10.4230/LIPIcs.ICALP.2017.80.

[79] Motakuri V. Ramana. An exact duality theory for semidefinite programming and its complexity implications. *Mathematical Programming*, 77(1):129 – 162, April 1997. doi:10.1007/BF02614433.

[80] Alexander A. Razborov. Lower bounds on the monotone complexity of some boolean functions. *Dokl. Akad. Nauk SSSR*, 281(4):798–801, 1985.

[81] Alexander A. Razborov. Lower bounds for the polynomial calculus. *Comput. Complex.*, 7(4):291–324, 1998. doi:10.1007/s000370050013.

[82] Tateaki Sasaki and Taku Takeshima. A modular method for gröbner-basis construction over q and solving system of algebraic equations. *Journal of Information Processing*, 12:371–379, 1990.

[83] Claus Scheiderer. Positivity and sums of squares: A guide to recent results. In Mihai Putinar and Seth Sullivant, editors, *Emerging Applications of Algebraic Geometry*, pages 271–324. Springer New York, New York, NY, 2009. doi:10.1007/978-0-387-09686-5_8.

[84] Grant Schoenebeck. Linear level lasserre lower bounds for certain k-csps. In *49th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2008, October 25-28, 2008, Philadelphia, PA, USA*, pages 593–602, 2008. doi:10.1109/FOCS.2008.74.

[85] Hanif D. Sherali and Warren P. Adams. A hierarchy of relaxations between the continuous and convex hull representations for zero-one programming problems. *SIAM Journal on Discrete Mathematics*, 3(3):411–430, 1990. doi:10.1137/0403036.

[86] N.Z. Shor. Cut-off method with space extension in convex programming problems. *Cybernetics*, 13(1):94–96, 1977. doi:10.1007/BF01071394.

[87] Dmitry Sokolov. (Semi)algebraic proofs over ±1 variables. In Konstantin Makarychev, Yury Makarychev, Madhur Tulsiani, Gautam Kamath, and Julia Chuzhoy, editors, *Proccedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing, STOC 2020, Chicago, IL, USA, June 22-26, 2020*, pages 78–90. ACM, 2020. doi:10.1145/3357713.3384288.

[88] Gilbert Stengle. A nullstellensatz and a positivstellensatz in semialgebraic geometry. *Mathematische Annalen*, 207(2):87–97, Jun 1974. doi:10.1007/BF01362149.

[89] Neil Thapen. A tradeoff between length and width in resolution. *Theory of Computing*, 12(5):1–14, 2016. doi:10.4086/toc.2016.v012a005.

[90] G. S. Tseitin. On the complexity of derivation in propositional calculus. In *Studies in constructive mathematics and mathematical logic. Part II*, volume 8 of *Zap. Nauchn. Sem. LOMI*, pages 234 – 259. "Nauka", Leningrad. Otdel., 1968.

[91] Benjamin Weitz. *Polynomial Proof Systems, Effective Derivations, and their Applications in the Sum-of-Squares Hierarchy*. PhD thesis, EECS Department, University of California, Berkeley, May 2017. URL: http://www2.eecs.berkeley.edu/Pubs/TechRpts/2017/EECS-2017-38.html.

[92] Franz Winkler. A p-adic approach to the computation ofgröbner bases. *Journal of Symbolic Computation*, 6(2):287–304, 1988. doi:10.1016/S0747-7171(88)80049-X.