Feasible Interpolation for Polynomial Calculus and Sums-Of-Squares

Tuomas Hakoniemi
Universitat Politècnica de Catalunya, Barcelona, Spain

Abstract

We prove that both Polynomial Calculus and Sums-of-Squares proof systems admit a strong form of feasible interpolation property for sets of polynomial equality constraints. Precisely, given two sets $P(x, z)$ and $Q(y, z)$ of equality constraints, a refutation Π of $P(x, z) \cup Q(y, z)$, and any assignment a to the variables z, one can find a refutation of $P(x, a)$ or a refutation of $Q(y, a)$ in time polynomial in the length of the bit-string encoding the refutation Π. For Sums-of-Squares we rely on the use of Boolean axioms, but for Polynomial Calculus we do not assume their presence.

2012 ACM Subject Classification Theory of computation → Proof complexity

Keywords and phrases Proof Complexity, Feasible Interpolation, Sums-of-Squares, Polynomial Calculus

Digital Object Identifier 10.4230/LIPIcs.ICALP.2020.63

Category Track A: Algorithms, Complexity and Games

Funding 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).

Acknowledgements I want to thank Albert Atserias for thorough comments on a preliminary versions of this work. I would also want to thank the anonymous reviewers who helped vastly to improve the presentation of this paper.

1 Introduction

In this paper we consider the proof systems Polynomial Calculus (PC) and Sums-of-Squares (SOS). PC is a proof system that is used to derive polynomial equalities from a set of polynomial equality constraints in a step-by-step fashion similar to traditional logical proof systems. A PC proof is a compact certificate that the proved polynomial is in the ideal generated by the constraints. PC was introduced by Clegg et al. [4].

Sums-of-Squares proof system on the other hand is a proof system used to derive polynomial inequalities from a set of polynomial constraints. As a proof system Sums-of-Squares was first investigated by Grigoriev and Vorobjov in [6], but it has its roots in semialgebraic geometry and combinatorial optimization. We refer the reader to [10] for a thorough presentation of these connections.

Feasible interpolation was introduced by Krajíček in [9] as a framework to prove lengths-of-proofs lower bounds for propositional proof system from lower bounds on Boolean circuits or other computational models. The feasible interpolation has been applied to prove lower bounds for example for Resolution [9] and Cutting Planes [12] from lower bounds on monotone Boolean and real circuits, respectively. On the negative side Krajíček and Pudlák showed in [8] that Extended Frege does not admit feasible interpolation with respect to Boolean circuits unless RSA is not secure against P/poly. This was later extended to Frege in [3] and to bounded depth Frege in [2] under other cryptographic assumptions.

47th International Colloquium on Automata, Languages, and Programming (ICALP 2020).
Editors: Artur Czumaj, Anuj Dawar, and Emanuela Merelli; Article No. 63; pp. 63:1–63:14
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

We will prove here feasible interpolation for both PC and SOS for equality constrains $P(x, y)$ and $Q(y, z)$ in disjoint sequences x, y and z of variables. We show that for both proof systems given a refutation Π of $P(x, z) \cup Q(y, z)$ and an assignment a to the variables z, one can in polynomial time in the bit-complexity of Π find a refutation of $P(x, a)$ or a refutation of $Q(y, a)$. Previously, a form of feasible interpolation for PC was proven for degree bounded PC-refutations by Pudlák and Sgall [13]. We know of no previous results on feasible interpolation for Sums-of-Squares proofs.

From [4] we know that PC is degree-automatable: any degree d proof can be found in time $n^{O(d)}$. The same is not true in general for SOS, since the coefficients in a small degree proof might be exceedingly large. This was first noted by O'Donnell in [11]. O'Donnell demonstrated a simple system of polynomial constraints that admit a degree 2 proofs of non-negativity, so that every degree 2 proof necessarily has coefficients of exponential bit-complexity. Later the example of [11] was strengthened by Raghavendra and Weitz in [14] by giving a system of constraints over the Boolean cube that have proofs of non-negativity of degree 2, but any proof of degree less than $O(\sqrt{n})$ must have exponential bit-complexity.

In view of these issues on the bit-complexity of SOS, the question arises whether doubly exponential coefficients can pose a problem for feasible interpolation. However we show that we can use the given refutation of $P(x, z) \cup Q(y, z)$ to bound the coefficients appearing in a refutation of $P(x, a)$ or a refutation of $Q(y, a)$.

Our proofs rely on a 'semantic' characterizations of refutations with bounded resources. A standard way to prove lower bounds in proof complexity is to exhibit a 'semantic' object whose existence is in contradiction with the existence of refutations with bounded resources. These include the reduction operators first used in [15] against low-degree PC-refutations, the d-designs first used in [1] against low-degree Nullstellensatz refutations and pseudoexpectations first used in [6] against low-degree Sums-of-Squares refutations. In many cases these objects actually characterize the associated classes of refutations, and thus they, from a logical point of view, give soundness and completeness theorems for resource bounded refutations. If soundness of these characterizations can be used to prove lower bounds, the completeness properties are useful in establishing upper bounds on proofs as exemplified by the proofs of Theorems 3 and 9 below.

Main results. Let $P(x, z)$ and $Q(y, z)$ be sets of polynomial equations, where x, y and z are disjoint sequences of variables. Our main results are as follows:

- For any finite field $\mathbb{F}$ there is a polynomial time algorithm that given a PC-refutation of $P(x, z) \cup Q(y, z)$, and an assignment a to the variables z, outputs a PC-refutation of $P(x, a)$ or a PC-refutation of $Q(y, a)$. (Theorem 5)
- There is a polynomial time algorithm that given an SOS-refutation of $P(x, z) \cup Q(y, z)$ over the Boolean hypercube and a Boolean assignment a to the variables z outputs an SOS-refutation of $P(x, a)$ over the Boolean hypercube or an SOS-refutation of $Q(y, a)$ over the Boolean hypercube. (Theorem 14)

Proof methods. We study the two systems in two separate parts. Each part follows the same outline. First we define a suitable class of proofs and its semantic counterpart. We define proofs over some fixed set of monomials. The idea is to shift the focus from trying to obtain size-of-proof upper bounds directly to proving the existence of proofs that use only monomials from some small set S. The corresponding semantic operators are then defined on the vector space of all polynomials which are linear combinations of elements of S.

Secondly we prove a feasible disjunction property for the system using the obtained semantic characterizations. Given a refutation of $P(x) \cup Q(y)$, where x and y are disjoint sequences of variables, we can define sets S_x and S_y whose size are polynomial in the size of the given refutation, such that either $P(x)$ has a refutation over S_x or $Q(y)$ has a refutation over S_y.

Finally we argue that the refutations whose existence is guaranteed by the feasible disjunction property can be found in time polynomial in the size of the underlying set of monomials. For PC we give a simple proof search algorithm, and for SOS we use the ellipsoid algorithm to search for a proof after meeting sufficient conditions for polynomial run-time.

2 Preliminaries

2.1 Polynomials and the Boolean Ideal

A monomial is a product of variables. A term over a field $\mathbb{F}$ is a product of a non-zero element of $\mathbb{F}$, called the coefficient of the term, and a monomial. A polynomial is a finite sum of terms, i.e. a finite linear combination of monomials. We write $\mathbb{F}[x]$ for the set of all polynomials over a field $\mathbb{F}$. In particular $\mathbb{R}[x]$ denotes the set of all monomials with real coefficients. For any set S of monomials we denote by $\mathbb{F}[S]$ the set of all linear combinations of monomials from S. For any $p \in \mathbb{R}[x]$ we denote by $\|p\|$ the largest absolute value of a coefficient that appears in p.

For SOS we consider polynomials over n pairs of twin variables $x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n$. The intended meaning is that the variables range over Boolean values $\{0, 1\}$ and that a pair of twin variables assumes opposite values. Accordingly we define the Boolean ideal I_n to be the ideal generated by the Boolean axioms $\{x_i^2 - x_i, x_i + \bar{x}_i - 1 : i \in [n]\}$. We write $p \equiv q \mod I_n$ if $p - q \in I_n$.

The Boolean axioms form a Gröbner basis for the Boolean ideal. This is readily seen using the Buchberger's criterion. The important consequence of this for our purposes is that the multivariate division algorithm with respect to the Boolean axioms leaves a unique remainder, and in particular the remainder is 0 if and only if $p \in I_n$. For more information on multivariate division and Gröbner bases, we refer the reader to [5].

2.2 Polynomial Calculus and Sums-of-Squares proofs

Let Q be a set of polynomials over an arbitrary field $\mathbb{F}$. We think of elements of Q as equality constraints $q = 0$. Let p be another polynomial. A PC-proof of p from Q is a sequence $p_1, \ldots, p_\ell$ of polynomials such that $p_\ell = p$ and for each $i \in [\ell]$ one of the following hold:

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

A PC-proof of p from Q is a certificate that p is in the ideal generated by Q. A PC-refutation of Q is a PC-proof of 1 from Q.

Let now Q be a set of real polynomials over n pairs of Boolean variables. A Sums-of-Squares proof of non-negativity of p from Q over the Boolean hypercube is a polynomial equality of the form

$$p = \sum_{i \in [k]} r_i^2 + \sum_{q \in Q} t_q q + \sum_{i \in [n]} \left(u_i \left(x_i^2 - x_i \right) + v_i \left(x_i + \bar{x}_i - 1 \right) \right), \qquad (1)$$

where r_i, t_q, u_i and v_i are arbitrary real polynomials. An SOS refutation of Q over the Boolean hypercube is a proof of non-negativity of -1. Usually we will simply write the SOS proof (1) as

$$p \equiv \sum_{i\in[k]} r_i^2 + \sum_{q\in Q} t_q q \mod I_n$$

and omit the explicit lifts of the Boolean axioms.

3 Feasible interpolation for Polynomial Calculus

3.1 PC proofs over a set of monomials

Let Q be a set of polynomials over field $\mathbb{F}$ and let S be a set of monomials containing all the monomials in Q and the empty monomial 1. Let $\hat{S} = S \cup xS$, where $xS = \{xm : m \in S \text{ and } x \text{ is a variable}\}$. A PC-proof of p from Q over S is a PC-proof of p from Q, where only monomials from the set $\hat{S}$ appear, and the inference rule p/xp is only applied when $p \in \mathbb{F}[S]$. Denote by $\mathrm{PC}_S(Q)$ the set of all p such that there exists a PC-proof of p from Q over S.

Let now $<$ be a total order on $\hat{S}$ satisfying the following two conditions:

(i) $1 \le m$ for any $m \in \hat{S}$;

(ii) if $m \in S$ and $m' \in \hat{S} \setminus S$, then $m < m'$.

The leading monomial of a polynomial $p \in \mathbb{F}[\hat{S}]$, denoted $\mathrm{LM}(p)$, is the largest monomial with respect to $<$ that appears in p with a non-zero coefficient. The leading term of a polynomial $p \in \mathbb{F}[\hat{S}]$, denoted $\mathrm{LT}(p)$ is the term, whose underlying monomial is the leading monomial of p.

We say that a term $t \in \mathbb{F}[\hat{S}]$ is S-reducible modulo Q if there is $p \in \mathrm{PC}_S(Q)$ such that $t = \mathrm{LT}(p)$. Otherwise the term is S-irreducible modulo Q. The following lemma shows that any polynomial in $\mathbb{F}[\hat{S}]$ can be uniquely factorized into a provable and an S-irreducible component.

▶ **Lemma 1.** *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*

- *$p = q + r$;*
- *$q \in \mathrm{PC}_S(Q)$;*
- *r is a sum of S-irreducible terms modulo Q.*

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

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

- $p = p_i + q_i + r_i$;
- $q_i \in \mathrm{PC}_S(Q)$;
- r_i is a sum of S-irreducible terms.
- $p_m = 0$ 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 S-reducible as witnessed by $q \in \mathrm{PC}_S(Q)$ 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 S-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 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 $q - q' \in \mathrm{PC}_S(Q)$ and so $r' - r \in \mathrm{PC}_S(Q)$, Hence $\mathrm{LT}(r' - r)$ is not S-irreducible. However, since both r and r' are sums of S-irreducible terms, it follows that $\mathrm{LT}(r' - r) = 0$ and so $r = r'$. Hence also $q = q'$. ◀

Consider now the mapping $R^Q_S \colon \mathbb{F}[\hat{S}] \to \mathbb{F}[\hat{S}]$ that maps each p to the unique sum r of S-irreducible terms modulo Q such that $p - r \in \mathrm{PC}_S(Q)$. The following lemma gathers four basic properties of the mapping.

▶ **Lemma 2.** *The following hold.*

(i) *If there is no refutation of Q over S, then $R^Q_S(1) = 1$;*
(ii) *R^Q_S is a linear function;*
(iii) *$R^Q_S(R^Q_S(p)) = R^Q_S(p)$ for any polynomial $p \in \mathbb{F}[\hat{S}]$;*
(iv) *$R^Q_S(xm) = R^Q_S(xR^Q_S(m))$ for any $m \in S$ and any variable x.*

Proof. (i) If there is no refutation of Q over S, then, by part (i) of the definition of $<$, the constant polynomial 1 is S-irreducible modulo Q. On the other hand $0 \in \mathrm{PC}_S(Q)$ and so, by the uniqueness of the factorization, $R^Q_S(1) = 1$.

(ii) Firstly, we have that $p - R^Q_S(p), q - R^Q_S(q) \in \mathrm{PC}_S(Q)$, and so $p + q - (R^Q_S(p) + R^Q_S(q)) \in \mathrm{PC}_S(Q)$. 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 factorization, $R^Q_S(p+q) = R^Q_S(p) + R^Q_S(q)$. Similarly $ap - aR^Q_S(p) \in \mathrm{PC}_S(Q)$ and so $R^Q_S(ap) = aR^Q_S(p)$.

(iii) We have that $p - R^Q_S(p), R^Q_S(p) - R^Q_S(R^Q_S(p)) \in \mathrm{PC}_S(Q)$ and so also $p - R^Q_S(R^Q_S(p)) \in \mathrm{PC}_S(Q)$, where $R^Q_S(R^Q_S(p))$ is a sum of S-irreducible terms modulo Q. Hence, again by the uniqueness of the factorization, $R^Q_S(p) = R^Q_S(R^Q_S(p))$.

(iv) Again, we have that $m - R^Q_S(m) \in \mathrm{PC}_S(Q)$. Now, by Lemma 1, each term t in $R^Q_S(m)$ satisfies $t \leq m$. Hence, by part (ii) of the definition of $<$, each t in $R^Q_S(m)$ is in S, and so $R^Q_S(m) \in \mathbb{F}[S]$. Hence also $xm - xR^Q_S(m) \in \mathrm{PC}_S(Q)$. It follows that $R^Q_S(xm) = R^Q_S(xR^Q_S(m))$. ◀

3.2 Feasible disjunction for PC

In this section we prove a feasible disjunction property for Polynomial Calculus using the machinery developed in the previous section. Below $P(x)$ and $Q(y)$ are set of polynomials in disjoint sequences x and y of variables.

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 3.** *Let Π be a PC-refutation of $P(x) \cup Q(y)$, and let S be the set of all monomials appearing in the refutation Π. Then there is a PC-refutation of $P(x)$ over S_x or a PC-refutation of $Q(y)$ over S_y.*

Proof. Suppose towards a contradiction that the conclusion does not hold, and consider the reduction operators $R^{P(x)}_{S_x}$ and $R^{Q(y)}_{S_y}$. 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

$$R(m_x m_y) = R^{P(x)}_{S_x}(m_x) R^{Q(y)}_{S_y}(m_y)$$

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

We claim now that R has the following properties:

(i) $R(1) = 1$;
(ii) $R(p(x,a)) = 0$ for any $p(x,a) \in P(x,a)$;
(iii) $R(q(y,a)) = 0$ for any $q(y,a) \in Q(y,a)$;
(iv) $R(x_i m) = R(x_i R(m))$ if $m \in S$;
(v) $R(y_i m) = R(y_i R(m))$ if $m \in S$.

The item (i) holds, since by Lemma 2(i), $R_{S_x}^{P(x)}(1) = R_{S_y}^{Q(y)}(1) = 1$. It is clear that both (ii) and (iii) hold.

Finally (iv) holds, by Lemma 2, since

$$\begin{aligned} R(x_i m) &= R_{S_x}(x_i m_x) R_{S_y}(m_y) \\ &= R_{S_x}(x_i R_{S_x}(m_x)) R_{S_y}(R_{S_y}(m_y)) \\ &= R(x_i R_{S_x}(m_x) R_{S_y}(m_y)) \\ &= R(x_i R(m)) \end{aligned}$$

The case (v) is proved similarly.

Now the existence of such R is in contradiction with the assumption that in Π there appears only monomials from S. Firstly R is defined for all the polynomial appearing in Π. Secondly, by (ii) and (iii), R maps each axiom in $P(x) \cup Q(y)$ to zero, and, by linearity and (iv) and (v), 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 (i). ◀

3.3 Proof search over S

In this section we show how to find proofs over a given set S of monomials in time polynomial in $|S|$. We make this claim only for proofs over a finite field $\mathbb{F}$. In order to avoid pathological counterexamples we tacitly assume that the size of S is at least the number of distinct variables in S.

We begin by constructing a basis B for $\mathrm{PC}_S(Q)$. The construction is given by the following algorithm, which is a modification of an algorithm from [4].

Algorithm 1 Proof search over S.

```
Initially $A = Q$ and $B = \emptyset$;
while $A \neq \emptyset$ do
    Pick $p \in A$ and remove it from $A$;
    while $\mathrm{LM}(p) \in \mathrm{LM}(B)$ do
        Let $q \in B$ be such that $\mathrm{LM}(q) = \mathrm{LM}(p)$;
        Let $p \leftarrow p - aq$, where $a$ is such that $\mathrm{LT}(p) = a\mathrm{LT}(q)$;
    end
    If $p \neq 0$, add $p$ to $B$;
    If $p \in \mathbb{F}[S]$, add $xp$ to $A$ for every variable $x$;
end
Output $B$;
```

Now B 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 $|S|^3$ elements in A and thus the algorithm halts after polynomially many steps in $|S|$. Hence for any finite field the above algorithm will halt in time polynomial in $|S|$. In the following we prove that B is actually a basis for $\mathrm{PC}_S(Q)$.

▶ **Lemma 4.** *At the end of the above algorithm* $\mathrm{span}(B) = \mathrm{PC}_S(Q)$.

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

Now suppose $p \in \mathrm{PC}_S(Q)$ and let $p_1, \dots, p_\ell$ be a PCR proof of p 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 each axiom 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 axiom 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 $p_j \in \mathbb{F}[S]$, 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 $q_k \in \mathbb{F}[S]$ 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 $m \in S$, and so $q_k \in \mathbb{F}[S]$ for every k. Now for any k, q_k was added to B and xq_k was added to A at some stage of the algorithm. Now, at that stage $xq_k \in \mathrm{span}(A \cup B)$. However, since the span only increases during the execution of the algorithm, $xq_k \in \mathrm{span}(B)$ at the end of the algorithm. Hence $xp_j \in \mathrm{span}(B)$ at the end of the algorithm. ◀

Now to check whether there is a PC proof of p 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.

3.4 Feasible interpolation

Finally as a consequence of Theorem 3 and Section 3.3 we obtain the feasible interpolation property for PC over any finite field. Below $P(x, z)$ and $Q(y, z)$ are two sets of polynomials, where x, y and z are disjoint sequences of variables.

▶ **Theorem 5.** *For any finite field $\mathbb{F}$, there is a polynomial time algorithm that given a PC-refutation of $P(x, z) \cup Q(y, z)$, and an assignment a to the variables z, outputs a PC-refutation of $P(x, a)$ or a PC-refutation of $Q(y, a)$.*

4 Feasible interpolation for Sums-of-Squares

4.1 Bounded SOS proofs over a set of monomials

Let Q be a set of polynomials and let S be a set of monomials that includes all the monomials appearing in Q and the empty monomial 1.

Denote by S^2 the set of all monomials m such that $m = m_1 m_2$, where $m_1, m_2 \in S$. An SOS proof of non-negativity of some $p \in \mathbb{R}[S^2]$ from Q over S is a polynomial equality of the form

$$p \equiv \sum_{i \in [k]} r_i^2 + \sum_{q \in Q} t_q q \mod I_n$$

where $r_i, t_q \in \mathbb{R}[S]$. We write $Q \vdash_S p \geq q$ if there is a proof of non-negativity of $p - q$ from Q over S. The proof is R-bounded if $\|t_q\| \leq R$ for each $q \in Q$. We need to consider explicitly bounded proofs in order to later be able to give a polynomial time proof search algorithm.

We prove first the important fact that every polynomial in $\mathbb{R}[S^2]$ has provable upper bounds over S modulo the Boolean ideal.

▶ **Lemma 6.** *For any $p \in \mathbb{R}[S^2]$ there is $r \in \mathbb{R}_+$ such that*

$$\emptyset \vdash_S r \geq p.$$

Proof. Let first $m \in S$, and let $a \in \mathbb{R}$. We want to show that there is some $b \in \mathbb{R}_+$ such that $Q \vdash_S b \geq am$. If $a < 0$, then $-am \equiv (\sqrt{-a}m)^2 \mod I_n$ and so $Q \vdash_S 0 \geq am$. On the other hand if $a > 0$, then $a - am \equiv (\sqrt{a} - \sqrt{a}m)^2 \mod I_n$, and so $Q \vdash_S a \geq am$.

Let then $m_1, m_2 \in S$ and $a \in \mathbb{R}$. We show again that there is some $b \in \mathbb{R}_+$ such that $Q \vdash_S b \geq am_1m_2$. If $a < 0$, then $-am_1 - 2am_1m_2 - am_2 \equiv (\sqrt{-a}m_1 + \sqrt{-a}m_2)^2 \mod I_n$. On the other hand, by the above paragraph, there are $b_1, b_2 \in \mathbb{R}_+$ such that $Q \vdash_S b_1 \geq -am_1$ and $Q \vdash_S b_2 \geq -am_2$. Hence $Q \vdash_S (b_1 + b_2)/2 \geq am_1m_2$. 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 there are $b_1, b_2 \in \mathbb{R}_+$ such that $Q \vdash_S b_1 \geq am_1$ and $Q \vdash_S b_2 \geq am_2$, and so $Q \vdash_S (b_1 + b_2)/2 \geq am_1m_2$. ◀

Now we define the objects that we consider to be the semantic counterparts of bounded refutations over a set of monomials. Let $\varepsilon > 0$. A linear functional $E\colon \mathbb{R}[S^2] \to \mathbb{R}$ is an ε-pseudoexpectation for Q over S if the following properties hold:

(i) $E(1) = 1$;
(ii) $E(p) = E(q)$ if $p \equiv q \mod I_n$;
(iii) $E(p^2) \geq 0$ for any $p \in \mathbb{R}[S]$;
(iv) $|E(mq)| \leq \varepsilon$ for any $m \in S$ and any $q \in Q$.

The following two lemmas show connections between ε-pseudoexpectations and proofs with bounded coefficients.

▶ **Lemma 7.** *If there is an ε-pseudoexpectation for Q over S, then there is no R-bounded refutation of Q over S for R less than $1/\varepsilon|S||Q|$.*

Proof. Let E be an ε-pseudoexpectation for Q over S, and suppose that

$$-1 \equiv \sum_{i\in[k]} r_i^2 + \sum_{q\in Q} t_q q \mod I_n$$

is a refutation over S with $\|t_q\| < 1/\varepsilon|S||Q|$ for any $q \in Q$. Now $|E(amq)| \leq |a|\varepsilon$ for each $m \in S$, $q \in Q$ and $a \in \mathbb{R}$. Hence $|E(t_q q)| < 1/|Q|$ for each $q \in Q$, and so $|E(\sum_{q\in Q} t_q q)| < 1$. Now applying E to both sides of the refutation we obtain that $-1 \geq \sum_{q\in Q} E(t_q q) > -1$. ◀

▶ **Lemma 8.** *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

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

and

$$B := \{-1 + \sum_{q\in Q} t_q q : t_q \in \mathbb{R}[S] \text{ and } \|t_q\| \leq R \text{ for every } q \in Q\}.$$

Now, by assumption, A and B are disjoint, A is a convex cone and B is a convex set. Hence, by the hyperplane separation theorem, there is a non-trivial linear functional $L\colon \mathbb{R}[S^2] \to \mathbb{R}$ such that $L(p) \geq 0$ for every $p \in A$, and $L(p') \leq 0$ for every $p' \in B$.

We want to first argue that $L(1) \neq 0$. So suppose towards a contradiction that $L(1) = 0$. By Lemma 6, for any $p \in \mathbb{R}[S^2]$ there is some $R \in \mathbb{R}_+$ such that $\emptyset \vdash_S R \geq p \geq -R$. It follows that $L(R) \geq L(p) \geq L(-R)$, and so $L(p) = 0$ for every $p \in \mathbb{R}[S^2]$ against the non-triviality of L.

Now define $E(p) = L(p)/L(1)$ for any $p \in \mathbb{R}[S^2]$. We claim that E has the desired properties. We prove the last case. 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 $|E(mq)| \leq 1/R$. ◀

4.2 Feasible disjunction for SOS

In this section we prove a feasible disjunction property for SOS. For a refutation

$$-1 = \sum_{i\in[k]} r_i^2 + \sum_{q\in Q} t_q q + \sum_{i\in[n]} \left(u_i\left(x_i^2 - x_i\right) + v_i\left(x_i + \bar{x}_i - 1\right)\right)$$

the explicit monomials of the refutation are all the monomials appearing in the polynomials r_i, t_q, q, u_i, v_i, $x_i^2 - x_i$ and $x_i + \bar{x}_i - 1$, i.e. the explicit monomials are the monomials that appear in an explicit representation of the refutation.

▶ **Theorem 9.** *Let*

$$\begin{aligned}-1 = \sum_{i\in[k]} r_i^2 + \sum_{p(x)\in P(x)} t_p p(x) + \sum_{q(y)\in Q(y)} t_q q(y) + \\ \sum_{i\in[n]} \left(u_i\left(x_i^2 - x_i\right) + v_i\left(x_i + \bar{x}_i - 1\right)\right) \sum_{i\in[n']} \left(u_i'\left(y_i^2 - y_i\right) + v_i'\left(y_i + \bar{y}_i - 1\right)\right)\end{aligned}$$

be an SOS refutation of $P(x) \cup Q(y)$ with $\|t_p\|, \|t_q\| \leq R$ for every $p(x) \in P(x)$ and $q(y) \in Q(y)$, let S be the set of explicit monomials appearing in the refutation, and let $R' = 2R|P(x) \cup Q(y)||S|$. Then there is a R'-bounded refutation of $P(x)$ over S_x or a R'-bounded refutation of $Q(y)$ over S_y.

Proof. Suppose towards a contradiction that the conclusion does not hold. Then, by Lemma 8, there are $1/R'$-pseudoexpectations for $P(x)$ over S_x and $Q(y)$ over S_y. 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.

(i) $E(1) = 1$;
(ii) $E(m(x_i^2 - x_i)) = 0$ for any $m \in S$ and any variable x_i;
(iii) $E(m(x_i + \bar{x}_i - 1)) = 0$ for any $m \in S$ and any variable x;
(iv) $E(m(y_i^2 - y_i)) = 0$ for any $m \in S$ and any variable y_i;
(v) $E(m(y_i + \bar{y}_i - 1)) = 0$ for any $m \in S$ and any variable y_i;
(vi) $E(p^2) \geq 0$ for any $p \in \mathbb{R}[S]$;
(vii) $|E(m(p(x))| \leq 1/R'$ for any $m \in S$ and any $p(x) \in P(x)$;
(viii) $|E(m(q(y))| \leq 1/R'$ for any $m \in S$ and any $q(y) \in Q(y)$.

The cases (i)-(v) are easy to see. For (vi), 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 su ch that $E_y(m_y m'_y) = \sum_u u_m u_{m'}$. Now we have

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

Finally (vii) holds, since

$$|E(m(p(x)| = |E_x(m_x(p(x))||E_y(m_y)| \leq 1/R',$$

where the last inequality holds since E_x is an $1/R'$-pseudoexpectation for $P(x)$ over S_x and $|E_y(m_y)| \leq 1$ for all $m \in S$. Case (viii) is proved similarly.

Now the existence of such E is in contradiction with the assumptions about the given refutation of $P(x) \cup Q(y)$. Although the mapping E does not necessarily fulfill the condition (ii) of an ε-pseudoexpectation, as E is defined for all the summands in the given refutation, we reach a contradiction by a similar argument as in Lemma 7. ◀

4.3 Proof search over S with bounded coefficients

In this section we show how to find the bounded refutation, whose existence is guaranteed by Theorem 9, in time polynomial in the size of S and $\log R$. Again we tacitly assume that the size of S is at least the number of distinct variables appearing in S. For proof search we use the ellipsoid algorithm. Before we can apply the algorithm we need to show that we can bound the other coefficients appearing in the proof using the bound on the t_q polynomials.

As a first step we show that we can bound the coefficients appearing in the sum of squares part of a given refutation. The next lemma is a simple special case of the main theorem of [14].

▶ **Lemma 10.** *Let $p \in \mathbb{R}[S^2]$. If there is a proof of non-negativity of p from $\emptyset$ over S, then there are $r_i \in \mathbb{R}[S]$ such that*

$$p \equiv \sum_{i \in [k]} r_i^2 \mod I_n$$

and $\|r_i\|$ is at most polynomial in $2^{\mathrm{poly}(|S|)}$ and $\|p\|$ for any $i \in [k]$.

Proof. The proof is practically the same as the proof of the main theorem of [14] with only small differences. We'll sketch the proof for completeness.

Let $\mathbf{v}_S$ be a vector of all the monomials in S, and let C be a PSD matrix such that $p \equiv \langle C, \mathbf{v}_S \mathbf{v}_S^T \rangle \mod I_n$. Now denote by M_S the averaged matrix $\mathbb{E}_{\alpha \in \{0,1\}^n} \mathbf{v}_S(\alpha) \mathbf{v}_S^T(\alpha)$ over all Boolean assignments. Now, by Lemma 6 of [14], the smallest non-zero eigenvalue δ of M_S is at least $1/2^{\mathrm{poly}(|S|)}$.

Let now $P = \sum uu^T$ be a projection to the zero eigenspace of M_S. Now, for each u, $u^T \mathbf{v}_S$ is zero on all Boolean assignments, and thus $u^T \mathbf{v}_S \equiv 0 \mod I_n$. Hence

$$\begin{aligned} \langle C, \mathbf{v}_S \mathbf{v}_S^T \rangle &\equiv \langle C, (P + P^\perp) \mathbf{v}_S \mathbf{v}_S^T (P + P^\perp) \rangle \mod I_n \\ &\equiv \langle C, P^\perp \mathbf{v}_S \mathbf{v}_S^T P^\perp \rangle \mod I_n \\ &\equiv \langle P^\perp C P^\perp, \mathbf{v}_S \mathbf{v}_S^T \rangle \mod I_n \end{aligned}$$

Let $C' = P^{\perp}CP^{\perp}$, so that $p \equiv \langle C', \mathbf{v}_S\mathbf{v}_S^T\rangle$. Now, by taking averages on both sides, we obtain that

$$\mathbb{E}_{\alpha\in\{0,1\}^n}[p(\alpha)] = \langle C', M_S\rangle.$$

Now the left hand side is at most polynomial in $\|p\|$ and $|S|$. On the other hand the right hand side is at least $\delta\mathrm{Tr}(C')$, since every non-zero eigenvalue of M_S is at least δ and the zero eigenspace of C' is included in the zero-eigenspace of M_S. Since the Frobenius norm of C' is bounded by $\mathrm{Tr}(C')$ we have that each entry of C' is at most polynomial in $2^{\mathrm{poly}(|S|)}$ and $\|p\|$. Now let $r_i, i \in [k]$ be such that $\sum_{i\in[k]} r_i^2 = \langle C', \mathbf{v}_S\mathbf{v}_S^T\rangle$. Now each coefficient of r_i is bounded by a polynomial in $2^{\mathrm{poly}(|S|)}$ and $\|p\|$. ◀

▶ **Corollary 11.** *Let $p \in \mathbb{R}[S^2]$. If there is an R-bounded proof of p from Q over S, then there are $r_i \in \mathbb{R}[S]$ such that*

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

and the absolute value of all the coefficients appearing in each r_i is at most polynomial in $2^{\mathrm{poly}(|S|)}$, R and $\|p\|$.

Proof. If $p \equiv \sum_{i\in[k]} r_i^2 + \sum_{q\in Q} t_q q \mod I_n$, then $p - \sum_{q\in Q} t_q q \equiv \sum_{i\in[k]} r_i^2 \mod I_n$, and the result follows from the previous lemma. ◀

Secondly we need to restrict the search space for the lifts of the Boolean axioms. In our definition of a proof over a set of monomials, we worked over the Boolean ideal, and thus did not restrict the lifts of the Boolean axioms in any way. However since the Boolean axioms form a Gröbner basis for the Boolean ideal, we can show that there is a well-behaved set $\bar{S}$ of monomials computable from S in time polynomial in $|S|$ such that for any $p \in \mathbb{R}[S^2]$ with $p \equiv 0 \mod I_n$ there are $u_i, v_i \in \mathbb{R}[\bar{S}]$ such that

$$p = u_i(x_i^2 - x_i) + v_i(x_i + \bar{x}_i - 1)$$

To see this consider any monomial ordering $<$ such that B_n forms a Gröbner basis for I_n with respect to $<$, and define the set S_m for any monomial m with the following algorithm.

Algorithm 2 Construction of the set S_m.

```
Initially $I = \{m\}$ and $S_m = \emptyset$;
while leading monomial of some Boolean axiom divides $\mathrm{LM}(I)$ do
    Let $p$ be the first Boolean axiom such that $\mathrm{LM}(p)$ divides $\mathrm{LM}(I)$;
    Let $m'$ be such that $\mathrm{LM}(I) = m'\mathrm{LM}(p)$;
    Let $p' = m - m'p$;
    Add $m'$ to $S_m$;
    Add all the monomials in $p'$ to $I$;
end
Output $S_m$;
```

The runtime of the above algorithm is polynomial in the degree of m. Now define $\bar{S} = \bigcup_{m\in S^2} S_m$. Now, if S is a set of multilinear monomials, set $\bar{S}$ can be computed in time polynomial in $|S|$.

▶ **Lemma 12.** *For each $p \in \mathbb{R}[S^2]$ such that $p \equiv 0 \mod I_n$ there are $u_i, v_i \in \mathbb{R}[\bar{S}]$ such that*

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

Moreover the absolute value of the coefficients in u_i and v_i is bounded by a polynomial in $\|p\|$, $|S|$ and the degree of p.

Proof. The proof follows since, as the Boolean axioms form a Gröbner basis for I_n with respect to $<$, we have that $p \equiv 0 \mod I_n$ if and only if p reduces to 0 with the multivariate division algorithm with respect to the monomial ordering $<$. The multivariate division algorithm will construct u_i and v_i that are linear combinations of monomials from $\bar{S}$. The last part follows from the fact that the algorithm halts after polynomially many steps in the degree of p and $|S|$. ◀

Now as a corollary to Corollary 11 and Lemma 12 we have the following

▶ **Corollary 13.** *Let $p \in \mathbb{R}[S^2]$. If there is an R-bounded proof of p from Q over S, then there are $r_i \in \mathbb{R}[S]$ and $u_i, v_i \in \mathbb{R}[\bar{S}]$ such that*

$$p = \sum_{i \in [k']} r_i^2 + \sum_{q \in Q} t_q q + \sum_{i \in [n]} \left(u_i \left(x_i^2 - x_i\right) + v_i \left(x_i + \bar{x}_i - 1\right)\right),$$

and the absolute value of all the coefficients appearing in each s_i, u_i and v_i is at most polynomial in $2^{\mathrm{poly}(|S|)}$, R and $\|p\|$.

Now the existence of a proof given by Corollary 13 can be expressed as feasibility of a set of linear and semidefinite constraints over explicitly bounded variables and so we can find an approximate solution to the set of constraints in polynomial time using the ellipsoid algorithm. We will sketch some details below. For details on ellipsoid algorithm see [7].

For each $q \in Q$, let $\bar{q} \in \mathbb{R}^S$ such that $\bar{q}^T \mathbf{v}_S = q$, and introduce a vector x_q of variables. Similarly for each $m, m' \in S$, introduce a variable $x_{m,m'}$. In addition, introduce variables y_{m,x_i^2}, y_{m,x_i} for each i and $m \in \bar{S}$ and variables $z_{m,x_i}, z_{m,\bar{x}_i}, z_{m,i}$ for each $i \in [n]$ and $m \in \bar{S}$ Now let $p = \sum_{k \in S^2} a_k k$ and introduce for every $k \in S^2$ a constraint $C_k = a_k$, where

$$\begin{aligned} C_k = & \sum_{\substack{m,m' \in S \\ mm'=k}} (x_{m,m'} + \sum_{q \in Q} \bar{q}_m x_{q,m'}) \\ & \qquad + \sum_{i \in [n]} (\sum_{\substack{m, \in \bar{S} \\ mx_i^2 = k}} y_{m,x_i^2} + \sum_{\substack{m \in \bar{S} \\ mx_i = k}} (z_{m,x_i} - y_{m,x_i}) + \sum_{\substack{m \in \bar{S} \\ m\bar{x}_i = k}} z_{m,\bar{x}_i} - \sum_{\substack{m \in \bar{S} \\ m = k}} z_{m,i}). \end{aligned}$$

Let X be the matrix $X_{m,m'} = x_{m,m'}$, and add the constraint $X \succeq 0$. Finally add the bounding constraints $-R' \leq x \leq R'$ for each variable for R' of magnitude polynomial in $2^{\mathrm{poly}(|S|)}$, R and $\|p\|$. Now any feasible solution gives a proof of p from Q with all coefficients bounded by R' and vice versa.

For $\varepsilon > 0$, an ε-relaxation of the above constraints is the set of constraints $|C_k - a_k| \leq \varepsilon$, $X \succeq 0$ and $-R' - \varepsilon \leq x \leq R' + \varepsilon$ for every variable x. Now if there is a feasible solution for the original set of constraints, the set of solutions of the ε-relaxation has volume at least $1/2^{\mathrm{poly}(\log(1/\varepsilon),|S|)}$.

Choose now $\varepsilon = 1/2^{\mathrm{poly}(|S|)}$. Now the ellipsoid method can find a feasible solution to the ε-relaxation in time polynomial in $|S|$, $\log R$ and $\log \|p\|$. Any such solution translates into a polynomial $p + q$, where $\|q\| \leq \varepsilon$. Now for each am that appears in q, define q_m as follows: if $a > 0$ let $q_m = a(1-m)^2$, and if $a < 0$ let $q_m = -a(m)^2$. Now adding all q_m to $p + q$ gives Sums-of-Squares proof of $p - \varepsilon'$ for some $\varepsilon' = 1/2^{\mathrm{poly}(|S|)}$.

4.4 Feasible interpolation

Finally we obtain the feasible interpolation property for SOS as a corollary to Theorem 9 and section 4.3. For the theorem below $P(x,z)$ and $Q(y,z)$ are sets of multilinear polynomials over Boolean variables, where x, y and z are disjoint sequences of variables.

▶ **Theorem 14.** *Let $P(x,z)$ and $Q(y,z)$ be sets of multilinear polynomials. There is a polynomial time algorithm that given an SOS-refutation of $P(x,z) \cup Q(y,z)$ and an assignment a to the variables z outputs an SOS-refutation of $P(x,a)$ or an SOS-refutation of $Q(y,a)$.*

5 Concluding remarks

We have seen that both Polynomial Calculus and Sums-of-Squares admit a strong form of feasible interpolation. Using similar methods we can also prove that Sherali-Adams proof system admits equally strong feasible interpolation property. The proof can be obtained by a simple modification of the proof for Sums-of-Squares. The proof is actually considerably simpler since the problem of too large coefficients does not appear with Sherali-Adams proofs.

Sums-of-Squares proofs cannot admit monotone feasible interpolation, since the Clique-Coloring formulas have small Sums-of-Squares refutations. Pudlák and Sgall prove in [13] that degree bounded Polynomial Calculus admits monotone feasible interpolation with respect to monotone polynomial programs. An interesting open question is whether one can prove monotone feasible interpolation for Polynomial Calculus with respect to monotone circuits.

We only prove feasible interpolation for SOS for sets of equality constraints. If there are inequality constraints, we can only prove a feasible disjunction property with respect to monomial size: if there is a refutation of $P(x,z) \cup Q(y,z)$ of monomial size s, then for any a there is a refutation of $P(x,a)$ or a refutation of $Q(y,a)$ of monomial size $O(s)$. The problem is that we don't have nice counterparts of the ε-pseudoexpectations when we add inequality constraints.

Finally we want to emphasize that although we proved the feasible interpolation for Sums-of-Squares only over the $\{0,1\}$-values, importantly the argument works also for Boolean values over the ± 1 basis.

References

1 Paul Beame, Stephen A. Cook, Jeff Edmonds, Russell Impagliazzo, and Toniann Pitassi. The relative complexity of NP search problems. In Frank Thomson Leighton and Allan Borodin, editors, *Proceedings of the Twenty-Seventh Annual ACM Symposium on Theory of Computing, 29 May-1 June 1995, Las Vegas, Nevada, USA*, pages 303–314. ACM, 1995. doi:10.1145/225058.225147.

2 Maria Luisa Bonet, Carlos Domingo, Ricard Gavaldà, Alexis Maciel, and Toniann Pitassi. Non-automatizability of bounded-depth frege proofs. *Computational Complexity*, 13(1-2):47–68, 2004. doi:10.1007/s00037-004-0183-5.

3 Maria Luisa Bonet, Toniann Pitassi, and Ran Raz. On interpolation and automatization for frege systems. *SIAM J. Comput.*, 29(6):1939–1967, 2000. doi:10.1137/S0097539798353230.

4 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.

5 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.

6 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.

7 Martin Grötschel, László Lovász, and Alexander Schrijver. *Geometric Algorithms and Combinatorial Optimization*, volume 2 of *Algorithms and Combinatorics*. Springer, 1988. doi:10.1007/978-3-642-97881-4.

8 Jan Krajíček 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.

9 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.

10 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.

11 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.

12 Pavel Pudlák. Lower bounds for resolution and cutting plane proofs and monotone computations. *J. Symb. Log.*, 62(3):981–998, 1997. doi:10.2307/2275583.

13 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.

14 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.

15 Alexander A. Razborov. Lower bounds for the polynomial calculus. *Computational Complexity*, 7(4):291–324, 1998. doi:10.1007/s000370050013.