First-Order Reasoning and Efficient Semi-Algebraic Proofs

Fedor Part[1, 2], Neil Thapen[2], and Iddo Tzameret[3]

[1]JetBrains Research
[2]Institute of Mathematics of the Czech Academy of Sciences
[3]Department of Computing, Imperial College London

May 16, 2021

Abstract

Semi-algebraic proof systems such as sum-of-squares (SoS) have attracted a lot of attention recently due to their relation to approximation algorithms: constant degree semi-algebraic proofs lead to conjecturally optimal polynomial-time approximation algorithms for important NP-hard optimization problems. Motivated by the need to allow a more streamlined and uniform framework for working with SoS proofs than the restrictive propositional level, we initiate a systematic first-order logical investigation into the kinds of reasoning possible in algebraic and semi-algebraic proof systems. Specifically, we develop first-order theories that capture in a precise manner constant degree algebraic and semi-algebraic proof systems: every statement of a certain form that is provable in our theories translates into a family of constant degree polynomial calculus or SoS refutations, respectively; and using a reflection principle, the converse also holds.

This places algebraic and semi-algebraic proof systems in the established framework of bounded arithmetic, while providing theories corresponding to systems that vary quite substantially from the usual propositional-logic ones.

We give examples of how our semi-algebraic theory proves statements such as the pigeonhole principle, we provide a separation between algebraic and semi-algebraic theories, and we describe initial attempts to go beyond these theories by introducing extensions that use the inequality symbol, identifying along the way which extensions lead outside the scope of constant degree SoS. Moreover, we prove new results for propositional proofs, and specifically extend Berkholz's dynamic-by-static simulation of polynomial calculus (PC) by SoS to PC with the radical rule.

1 Introduction

This work introduces and exemplifies first-order logical theories that capture algebraic and semi-algebraic propositional proofs. While algebraic proof systems such as the polynomial calculus [13] have played a central role in proof complexity, semi-algebraic proof systems and specifically *sum-of-squares* (also known as *Lassere*, or as a restriction of the *Positivstellensatz* proof system) have

The first and second authors are partially supported by grant 19-05497S of GA ČR. Part of this work was done on a visit of the third author to the Czech Academy of Sciences. The Institute of Mathematics of the Czech Academy of Sciences is supported by RVO: 67985840. A preliminary version of this work appears in *36th Ann. Symp. Logic Comput. Science (LICS) 2021 [33]*.

Author emails: fedor.part@gmail.com, thapen@math.cas.cz, iddo.tzameret@gmail.com.

attracted a lot of attention in recent years. Semi-algebraic proofs have been brought to the attention of complexity theory from optimization [28, 27]; by the works of Pudlák [34] and Grigoriev and Vorobjov [19] (cf. [18]); and more recently through their connection to approximation algorithms with the work of Barak *et al.* [5] (see for example [31] and the excellent survey by Fleming, Kothari and Pitassi [15]).

What makes SoS important, for example to polynomial optimization, is the fact that the existence of a degree-d SoS certificate can be formulated as the feasibility of a semidefinite program, and hence *can be solved in polynomial time*. In this sense, SoS is said to be an *automatable* proof system (see some restrictions on this in [30]).

Due to its importance in algorithm design and approximation theory, bootstrapping SoS, that is, providing efficient low-degree SoS proofs of basic facts (see for example [31]), is of central importance to these systems. It is thus natural to aspire for a more elegant and streamlined way to reason about SoS proofs, perhaps analogous to the established machinery of bounded arithmetic.

One particular motivation for this work is a kind of heuristic that appears in the literature about constructing sum-of-squares proofs. Quoting from Barak's lecture notes [4]: '"Theorem": If a polynomial P is non-negative and "natural" (i.e. constructed by methods known to Hilbert — not including probabilistic method), then there should be a low degree SOS proof for the fact [that P is non-negative].'[1] This work is an approach towards making this idea more formal.

Bounded arithmetic theories are weak first-order theories for natural numbers that serve as uniform versions of propositional proof systems (cf. [10, 21, 24, 14]). On the one hand, bounded arithmetic constitutes the "proof-theoretic approach" to computational complexity in terms of developing the meta-mathematics of complexity (demonstrating for example the minimal reasoning power sufficient to prove major results in computational complexity), while on the other hand it constitutes an elegant way to facilitate short propositional proofs that avoids the need to actually work in the somewhat cumbersome "machine code" level of propositional proofs themselves. This is achieved using *propositional translations*: first-order proofs in bounded arithmetic translate into corresponding short propositional proofs.

Propositional translations in bounded arithmetic have a long history and go back to Paris and Wilkie [32]. Our translations are inspired in particular by Beckmann, Pudlák and Thapen [8]. Our *theories* on the other hand are inspired to a certain extent by works of Soltys and Cook [35] and Thapen and Soltys [36] that showed how to incorporate arbitrary ring elements and their operations in bounded arithmetic theories, as well as by the work of Buss, Kolodziejczyk and Zdanowski [12]. It is worth mentioning that although our theories fit naturally into the framework of bounded arithmetic, they are not technically bounded; since we only care about degree of propositional proofs, not size, we allow unbounded quantifiers.

1.1 Our results

Our results contribute both to propositional proof complexity and to bounded arithmetic. We describe them in general terms below, referring to the specific sections for more details.

1.1.1 Propositional proofs

In Section 2 we define the propositional proof systems we study, and show some relationships between them. We note that we care only about the degree of derivations and not their size (as mea-

[1] A consequence of this is "Marley's Corollary" on analyzing the performance of SoS algorithms [4].

sured, for example, by the number of monomials). In particular we introduce two natural extensions of the polynomial calculus (PC), as follows.

Let $\mathsf{PC}_{\mathscr{R}}$ be the polynomial calculus over the ring $\mathscr{R}$. We introduce the system $\mathsf{PC}^{\mathrm{rad}}_{\mathscr{R}}$ which is $\mathsf{PC}_{\mathscr{R}}$ plus the *radical rule*[2]: from $p^2 = 0$ derive $p = 0$, for a polynomial p. This extension of PC is arguably a more natural proof system than PC, in the sense that the Nullstellensatz, which underlies the completeness of algebraic proof systems, states that if a polynomial p is implied by a set of polynomials J then p is in the radical of the ideal generated by J; that is, p is in $\sqrt{\langle J\rangle} = \{q : q^k \in \langle J\rangle \text{ for some } k \in \mathbb{N}\}$. This appearance of a radical is captured by the radical rule, and in particular PC with this rule is implicationally complete over algebraically closed fields, as we observe in Proposition 7, which is not true for PC without this rule unless we add the Boolean axioms. Moreover, this rule allows for simulation of logical contraction, which we need for our translation results.

We then introduce the system $\mathsf{PC}^{+}_{\mathscr{R}}$ which is $\mathsf{PC}_{\mathscr{R}}$ plus the radical rule and the sum-of-squares rule: from $p^2 + \sum_i q_i^2 = 0$ derive $p^2 = 0$, for p, q polynomials. We define PC^{+} to be $\mathsf{PC}^{+}_{\mathbb{R}}$ (that is, over the reals).

Recall that a proof system is *implicationally complete* if, whenever a set of equations $\mathscr{F}$ implies an equation $q = 0$, there is a derivation $\mathscr{F} \vdash q = 0$ in the system. It is known that $\mathsf{PC}_{\mathscr{R}}$ is implicationally complete in the presence of the Boolean axioms [6, Theorem 5.2], while in general it is not implicationally complete without them. We show that, in contrast, $\mathsf{PC}^{\mathrm{rad}}_{\mathscr{R}}$ is implicationally complete if $\mathscr{R}$ is an algebraically closed field, and PC^{+} is implicationally complete (over the reals).

In Propositions 12 and 13 we show that whether the radical rule provides more strength to PC depends on the underlying ring. Finally, we extend a result by Berkholz [9], and show that the static system SoS and the dynamic system $\mathsf{PC}^{+}_{\mathscr{R}}$ simulate each other (with respect to degree):

Theorem (Theorem 15 and proposition 14; informal)**.** *In the presence of the Boolean axioms,* SoS *and* PC^{+} *simulate each other (with respect to degree).*

1.1.2 The first-order theories

In Section 3 we define the first-order, algebraic theories $\mathsf{TPC}_{\mathscr{R}}$ and TSoS which we will later show capture reasoning in constant degree polynomial calculus and constant degree sum of squares propositional proof systems, respectively.

Specifically, let $\mathscr{R}$ be an integral domain. $\mathsf{TPC}_{\mathscr{R}}$ is a two-sorted theory in the language $\mathscr{L}^{\mathscr{R}}_{=}$ with a *ring* sort and an *index* sort. Index elements model natural numbers. Apart from the usual $+, \cdot$ operations the language contains the ring-valued oracle symbol $X(i)$ where i is an index-sort, as well as a ring-sort big-sum operator. The intended meaning of $X(i)$ is the ith element in an otherwise unspecified sequence of ring-sort values.

This language has the important property that terms translate into families of polynomials of bounded degree, in propositional variables $X(i)$, parametrized by their index arguments (the converse is also true). Similarly atomic formulas translate into families of polynomial equations.

The theory $\mathsf{TPC}_{\mathscr{R}}$ consists of the *basic axioms* containing the usual ring axioms, the integral domain axiom, an axiom inductively defining big sums, some background truth axioms for index sorts, and the *induction scheme* for a specific class of well-behaved formulas. The theory TSoS additionally contains the *sum-of-squares* scheme: for each ring-valued term $t(i)$, in which other parameters can

[2] Grigoriev and Hirsch [17] were the first to consider the radical rule, to the best of our knowledge, although in [17] this was done in the context of a much stronger system, namely PC over algebraic formulas. Independently of our work, Alekseev [1] also considered PC with the radical rule, and for similar reasons to us.

also occur, the axiom $\sum_{i<n} t(i)^2 = 0 \wedge j < n \supset t(j) = 0$. For technical reasons, we also add first-order Boolean axioms.

In Section 4 we give examples of what proofs look like in these first-order theories, by proving some versions of the pigeonhole principle.

1.1.3 Propositional translations

In Section 5 we start to describe our translation, by showing how to translate formulas in our first-order language into families of polynomial equations. In Section 6 we show how first-order $\mathsf{TPC}_{\mathscr{R}}$ proofs can be translated into constant-degree $\mathsf{PC}^{\mathrm{rad}}_{\mathscr{R}}$ refutations:

Theorem (Theorem 31; informal)**.** *Let $\varphi(\bar{i})$ be a certain "well-behaved" formula with free index variables $\bar{i}$ and no free ring variables. Suppose $\mathsf{TPC}_{\mathscr{R}} \vdash \forall \bar{i} \neg \varphi(\bar{i})$. Then there is a constant degree $\mathsf{PC}^{rad}_{\mathscr{R}}$ refutation of the propositional translation of φ.*

The proof is by first translating $\mathsf{TPC}_{\mathscr{R}}$ proofs into a Gentzen-style sequent calculus $\mathsf{LK}_{\mathscr{R}}$ and then translating $\mathsf{LK}_{\mathscr{R}}$ into $\mathsf{PC}^{\mathrm{rad}}_{\mathscr{R}}$ rule-by-rule.

In Section 7 we show that, conversely, any principle with constant-degree $\mathsf{PC}^{\mathrm{rad}}_{\mathscr{R}}$ refutations is refutable in $\mathsf{TPC}_{\mathscr{R}}$. This is done by showing that $\mathsf{TPC}_{\mathscr{R}}$ proves that $\mathsf{PC}^{\mathrm{rad}}_{\mathscr{R}}$ refutations are sound, or in other words, proving a reflection principle for $\mathsf{PC}^{\mathrm{rad}}_{\mathscr{R}}$ in $\mathsf{TPC}_{\mathscr{R}}$. This demonstrates that $\mathsf{TPC}_{\mathscr{R}}$ is the right theory, in that we showed in the previous section that every $\mathsf{TPC}_{\mathscr{R}}$ proof turns into a $\mathsf{PC}^{\mathrm{rad}}_{\mathscr{R}}$ proof, and now show essentially that every $\mathsf{PC}^{\mathrm{rad}}_{\mathscr{R}}$ proof can be obtained this way.

In Section 8 we show similar results for sum of squares. That is, first-order TSoS proofs can be translated into constant degrees SoS refutations with Boolean axioms (denoted $\mathsf{SoS} + \mathsf{Bool}$), and vice versa:

Theorem (Theorem 38; informal)**.** *Let $\varphi(i)$ be be a certain "well-behaved" formula with no ring quantifiers and with index variable i as its only free variable. Define $\mathscr{S}_n$ to be the propositional translation of φ (parametrized by n). Then $\mathscr{S}_n$ is refutable in $\mathsf{SoS} + \mathsf{Bool}$ in some fixed constant degree if and only if $\mathsf{TSoS} \vdash \forall i \neg \varphi(i)$.*

As a corollary of the propositional translation results we can conclude that TSoS is not conservative over $\mathsf{TPC}_{\mathscr{R}}$, even if we add first-order Boolean axioms to $\mathsf{TPC}_{\mathscr{R}}$, using the separation between $\mathsf{SoS} + \mathsf{Bool}$ and $\mathsf{PC} + \mathsf{Bool}$ (that is, PC with Boolean axioms) demonstrated, for example, by Grigoriev [16], who showed that algebraic proofs like $\mathsf{PC} + \mathsf{Bool}$ cannot simulate semi-algebraic proofs like $\mathsf{SoS} + \mathsf{Bool}$, because symmetric subset-sum instances such as $x_1 + \cdots + x_n = -1$ require linear degree (and exponential monomial size) (cf. [22]).

1.1.4 Beyond TSoS

It would seem natural for SoS reasoning to be able to reason *directly* about inequalities. However, the theories we introduced so far cannot do that, and TSoS does not even have an inequality symbol in the language. Motivated by this, in Section 9 we describe approaches to going beyond the basic theory TSoS, with the goal of achieving a semi-algebraic first-order theory that can reason naturally about inequalities. We stress that achieving this is a challenging goal and we demonstrate this by showing that naively adding inequalities leads to a theory which is strictly stronger than constant-degree SoS.

We then describe, as work in progress, a theory with weakened axioms about ordering. We propose that it is possible to work through a proof in this theory, and essentially to "witness" each formula of the form $r \le t$ by replacing it with a formula asserting that $t - r$ is an explicit sum-of-squares. This is simple for axioms, but becomes more difficult when dealing with, for example, induction.

As the main open problem in this direction of research we put forth the attempt to further improve the usability of the above theory so that it deals more naturally with inequalities. We briefly discuss one possibility to achieve this by moving to intuitionistic logic.

1.2 Relation to previous work

Our approach to translation of first-order into propositional logic goes back at least to Paris and Wilkie [32]. They studied theories of bounded arithmetic with a relation symbol $R(x, y)$ for an "oracle relation" with no defining axioms. First-order formulas can be thought of as describing a property of R, and can be translated into propositional formulas, where atomic formulas of the form $R(x, y)$ turn into propositional variables $r_{x.y}$, other atomic formulas are evaluated as $\top$ or $\bot$, and bounded quantifiers become propositional connectives of large fan-in. Furthermore first order proofs in suitable theories translate into small propositional proofs. Under this translation, standard bounded arithmetic theories correspond to quasipolynomial size constant-depth Frege proofs. In particular Krajíček developed close connections between theories around T^1_2 and T^2_2 and systems around resolution [23, 25, 26].

Such translations can be used to apply techniques from propositional proof complexity to show unprovability in first order theories; or in the other direction, to prove propositional upper bounds by using the first order theory as something like a "high level language" where it is easier to write proofs, which can then be compiled into the propositional system. We are interested in this second kind of application. Relatively recent examples are Müller and Tzameret [29], formalizing some linear algebra arguments in TC^0-Frege; Beckmann, Pudlák and Thapen [8], reasoning about parity games in resolution; and Buss, Kołodziejczyk and Zdanowski [12], formalizing Toda's theorem in depth-3 Frege with parity connectives. These would all have been difficult, or impossible, to do without the level of abstraction provided by the first order theory.

The work [12] in particular defines a hierarchy of theories, the bottom two levels of which correspond to small, low degree proofs in Nullstellensatz and polynomial calculus. These are inspirations for the current paper. One of the main differences is that [12] only works with finite fields, which are easy to formalize in standard arithmetic theories, while we are aiming for the reals. Another is that we care about degree and do not need to control size, so can use unbounded quantifiers; thus our theories are not really bounded arithmetic, although the principle of the translation is the same.

To talk about algebraic structures, we adopt a two-sorted theory, with a ring sort and an index sort; some of the ideas here are adapted from Soltys [35, 36].

2 Propositional and algebraic systems

Let $\mathscr{R}$ be an integral domain, that is, a commutative ring with unity and no zero divisors. We will work with sets of equations over $\mathscr{R}$, of the form $\{p_i = 0 : i \in I\}$ where each p_i is from $\mathscr{R}[x_1, \ldots, x_n]$, that is, a polynomial with coefficients from $\mathscr{R}$ and variables from some specified set $\{x_1, \ldots, x_n\}$. We work with equations $p_i = 0$, rather than just writing the polynomial p_i by itself, because we will later want to distinguish between the equation $p_i = 0$ and the inequality $p_i \ge 0$.

In general we will allow sets of equations to be infinite, but for the sake of clarity of presentation we will state definitions and results in the next few subsections for *finite* sets of equations. In Section 2.4 we explain why, in the cases we are interested in, nothing significant changes if we allow infinite sets. A set of equations is *unsatisfiable* if the equations have no common solution in $\mathscr{R}$, and *satisfiable* otherwise.

Definition 1. *We define the product of two sets of equations to be*

$$\mathscr{P} \cdot \mathscr{Q} := \{p \cdot q = 0 \mid p = 0 \in \mathscr{P},\ q = 0 \in \mathscr{Q}\}.$$

Notice that an assignment of values in $\mathscr{R}$ to variables satisfies $\mathscr{P} \cdot \mathscr{Q}$ if and only if it satisfies $\mathscr{P}$ or $\mathscr{Q}$, and that if $\mathscr{S}$ is another set of equations, then $\mathscr{P} \cdot (\mathscr{Q} \cup \mathscr{S}) = (\mathscr{P} \cdot \mathscr{Q}) \cup (\mathscr{P} \cdot \mathscr{S})$. We will use these observations later, when we will use products and unions to handle respectively disjunctions and conjunctions of formulas represented by sets of equations.

We will consider *refutations* and *derivations* from sets of equations in various proof systems. We informally divide proof systems into *dynamic systems*, where a derivation is presented as a series of steps, each following from previous steps by a rule; and *static systems*, where a derivation happens all at once, and typically has the form of a big polynomial equality. A refutation of a set (in a given proof system) is in particular a witness that the set is unsatisfiable.

We will often use notation like "a derivation $\Gamma \vdash e$" instead of writing out "a derivation of e from Γ". We will write $\pi : \Gamma \vdash e$ to mean "π is a derivation of e from Γ".

The set of equations $\{x_i^2 - x_i = 0 : i = 1, \ldots, n\}$ is called the *Boolean axioms*, and guarantees that the variables take only 0/1 values. The systems below are usually defined to always include these axioms. We do not include them in the definitions, as we will in general be working with variables ranging over the whole ring. However for some results about SoS we will need them, and we will say explicitly when we are using them.

2.1 Dynamic systems

Definition 2. *A* polynomial calculus ($\mathsf{PC}_{\mathscr{R}}$) derivation *of an equation $q = 0$ from a set of equations $\mathscr{F}$ is a sequence of equations $e_1, \ldots, e_t$ such that e_t is $q = 0$ and each e_i is either a member of $\mathscr{F}$, or is $0 = 0$, or follows from earlier equations by one of the rules*

$$\text{Addition rule} \quad \frac{p = 0 \qquad r = 0}{ap + br = 0}$$

$$\text{Multiplication rule} \quad \frac{p = 0}{px_i = 0}$$

where p and r are polynomials, x_i is any variable and a and b are any elements of $\mathscr{R}$.

A $\mathsf{PC}_{\mathscr{R}}$ refutation *of a set of equations $\mathscr{F}$ is a derivation of $1 = 0$ from $\mathscr{F}$.*

As $\mathscr{R}$ is a ring these rules are sound, in the sense that every assignment that satisfies the assumptions of a rule also satisfies the conclusion.

We will use two additional rules to define extensions of $\mathsf{PC}_{\mathscr{R}}$ as follows. The *radical rule* [17] is sound because $\mathscr{R}$ is an integral domain. The *sum-of-squares rule* is sound if $\mathscr{R}$ is additionally a formally real ring, that is, a ring in which $\sum_i a_i^2 = 0$ if and only if $a_i = 0$ for all i.

$$\text{Radical rule} \quad \frac{p^2 = 0}{p = 0}$$

$$\text{Sum-of-squares rule} \quad \frac{p^2 + \sum_i q_i^2 = 0}{p^2 = 0}$$

Definition 3. *The system* $\mathsf{PC}^{rad}_{\mathscr{R}}$ *is* $\mathsf{PC}_{\mathscr{R}}$ *plus the radical rule.*

Definition 4. *The system* $\mathsf{PC}^{+}_{\mathscr{R}}$ *is* $\mathsf{PC}_{\mathscr{R}}$ *plus the radical rule and the sum-of-squares rule.*

Recall that by default we do not add the Boolean axioms $x_i^2 - x_i = 0$ to our proof systems. $\mathsf{PC}^{\mathrm{rad}}_{\mathscr{R}}$ and $\mathsf{PC}^{+}_{\mathscr{R}}$ derivations and refutations are defined just as in Definition 2. We will only study $\mathsf{PC}^{+}_{\mathscr{R}}$ in the case in which the underlying ring $\mathscr{R}$ is the real numbers, and will write simply PC^{+} instead of $\mathsf{PC}^{+}_{\mathbb{R}}$.

Definition 5. *The* degree *of a derivation or refutation in any of the above systems is the maximum degree of any polynomial that appears in it. We define* $\mathsf{PC}_{\mathscr{R},d}$, $\mathsf{PC}^{rad}_{\mathscr{R},d}$ *and* $\mathsf{PC}^{+}_{\mathscr{R},d}$ *to be the restricted systems in which only polynomials of degree* d *or less may appear.*

Degree will be our main measure of the complexity of a derivation. *Size* is also an interesting measure, but is not one which we will use, and there are some subtleties about how it should be defined. A natural definition of the size of a polynomial is the number of monomials it contains, but, particularly for applications, one may also want to include in the measure the size of the notation for the coefficients from $\mathscr{R}$.

A proof system is *implicationally complete* if, whenever a set of equations $\mathscr{F}$ implies an equation $q = 0$, there is a derivation $\mathscr{F} \vdash q = 0$ in the system. It is known that $\mathsf{PC}_{\mathscr{R}}$ is implicationally complete in the presence of the Boolean axioms [6, Theorem 5.2], while in general it is not implicationally complete without them. To see the latter, observe for example that for every variable x, the polynomial x is not in the ideal $\langle x^2 \rangle$ (because every nonzero polynomial in this ideal has degree bigger than 1) while $x = 0$ is implied by $x^2 = 0$ over any integral domain. We show now that, in contrast, $\mathsf{PC}^{\mathrm{rad}}_{\mathscr{R}}$ is implicationally complete if $\mathscr{R}$ is an algebraically closed field, and PC^{+} is implicationally complete (over the reals).

We recall some standard concepts from commutative algebra (see for instance Ash [2, Chap. 8]). Let $\mathbb{F}$ be a field. Denote by $\langle r_1, \ldots, r_k \rangle$ the ideal generated by $r_1, \ldots, r_k$ and by $V(\langle r_1, \ldots, r_k \rangle)$ the *variety* of this ideal, that is, the set of tuples in $\mathbb{F}^n$ on which all the polynomials are zero. For a set $X \subseteq \mathbb{F}^n$ denote by $\mathscr{I}(X)$ the ideal of all polynomials vanishing on X. It is easy to see that if $X_1 \subseteq X_2$, then $\mathscr{I}(X_2) \subseteq \mathscr{I}(X_1)$.

If J is an ideal over a field $\mathbb{F}$, then the ideal $\sqrt{J} := \{p : p^k \in J \text{ for some } k \in \mathbb{N}\}$ is called the *radical* of J. If J is an ideal in $\mathbb{R}[x_1, \ldots, x_n]$, then the *real radical* of J is

$$\sqrt[\mathbb{R}]{J} := \left\{ p : p^{2k} + \textstyle\sum_i r_i^2 \in J \ \text{ for some } k \in \mathbb{N},\ r_1, \ldots, r_m \in \mathbb{R}[x_1, \ldots, x_n] \right\}.$$

For the next proposition we need Hilbert's Nullstellensatz, which roughly states that if two ideals over an algebraically closed field define the same variety then the ideals are the same "up to power":

Theorem 6 (Nullstellensatz; cf. Theorem 8.4.1 in [2])**.** *Let* $\mathbb{F}$ *be an algebraically closed field. For any ideal* J *in* $\mathbb{F}[x_1, \ldots, x_n]$ *it holds that* $\mathscr{I}(V(J)) = \sqrt{J}$.

Proposition 7. *If $\mathbb{F}$ is an algebraically closed field, then $\mathsf{PC}^{rad}_{\mathbb{F}}$ is implicationally complete.*

Proof. Let $p_1,\ldots,p_m,q \in \mathbb{F}[x_1,\ldots,x_n]$ be such that $p_1 = 0,\ldots,p_m = 0$ together imply $q = 0$, or in other words, $V(\langle p_1,\ldots,p_m\rangle) \subseteq V(\langle q\rangle)$.

By the Nullstellensatz, for any ideal J it holds that $\mathscr{I}(V(J)) = \sqrt{J}$. Thus

$$\langle q\rangle \subseteq \sqrt{\langle q\rangle} = \mathscr{I}(V(\langle q\rangle)) \subseteq \mathscr{I}(V(\langle p_1,\ldots,p_m\rangle)) = \sqrt{\langle p_1,\ldots,p_m\rangle}.$$

Therefore $q^k \in \langle p_1,\ldots,p_m\rangle$ for some k, which means that there exists a $\mathsf{PC}_{\mathbb{F}}$ derivation of $q^k = 0$ from $p_1 = 0,\ldots,p_m = 0$, and using the radical rule it is straightforward to extend this to a $\mathsf{PC}^{\mathrm{rad}}_{\mathbb{F}}$ derivation of $q = 0$: first use the multiplication rule to obtain $q^{k'}$ with $k' \geq k$ a power of 2, and then apply $\log k'$ times the radical rule to obtain $q = 0$. □

Proposition 8. *PC^+ is implicationally complete.*

Proof. Assume $p_1,\ldots,p_m,q \in \mathbb{R}[x_1,\ldots,x_n]$ and $p_1 = 0,\ldots,p_m = 0$ together imply $q = 0$. By the Real Nullstellensatz [7, Theorem 1], $\mathscr{I}(V(J)) = \sqrt[\mathbb{R}]{J}$ for any ideal J in $\mathbb{R}[x_1,\ldots,x_n]$. Thus, as above, $\langle q\rangle \subseteq \sqrt[\mathbb{R}]{\langle p_1,\ldots,p_m\rangle}$ and hence there exists a $\mathsf{PC}_{\mathbb{R}}$ derivation of $q^{2k} + \sum_i r_i^2 = 0$ from $p_1 = 0,\ldots,p_m = 0$ for some $k \in \mathbb{N}$ and $r_1,\ldots,r_s \in \mathbb{R}[x_1,\ldots,x_n]$. Using the sum-of-squares and radical rules this derivation can be extended to a PC^+ derivation of $q = 0$. □

2.2 Static systems

Below we write $\equiv$ to express identity of polynomials.

Definition 9. *A* Nullstellensatz derivation *of an equation $q = 0$ from a set of equations $\mathscr{S} = \{p_i = 0 : i \in I\}$ is a family of polynomials $(r_i)_{i\in I}$ such that $\sum_i r_i p_i \equiv q$. A* Nullstellensatz refutation *of $\mathscr{S}$ is a derivation of $1 = 0$ from $\mathscr{S}$.*

The sum-of-squares proof system SoS, introduced in Barak *et al.* [5] as a restricted fragment of Grigoriev and Vorobjov's Positivstellensatz proof system [20], is a semi-algebraic proof system operating with polynomial equalities and inequalities over the reals. We are going to consider in this work a simple variant of SoS that operates only with polynomial equalities as follows:

Definition 10. *A* sum of squares (SoS) derivation *of an inequality $q \geq 0$ over $\mathbb{R}$ from a set of equations $\mathscr{S} = \{p_i = 0 : i \in I\}$ over $\mathbb{R}$ is a family of polynomials $(r_i)_{i\in I}$ and a second family of polynomials $(s_j)_{j\in J}$, both over $\mathbb{R}$, such that*

$$\sum_i r_i p_i + \sum_j s_j^2 \equiv q.$$

A sum of squares refutation *of $\mathscr{S}$ is a derivation of $-1 \geq 0$ from $\mathscr{S}$.*

An SoS + Bool *derivation, or refutation, is one that also allows the use of the Boolean axioms $x_i^2 - x_i = 0$, as though they were members of $\mathscr{S}$.*

Sum of squares can also naturally be defined to take inequalities $p_i \geq 0$ as assumptions as well as equalities, but we will not use this.

Often when we talk about "the sum of squares derivation" of an inequality, we will really mean the formal sum on the left-hand side of the above equivalence. For example we will sometimes talk in this way about adding a term to a derivation, or forming the linear combination of two derivations. The *degree* of a SoS derivation is the highest degree of any term $r_i p_i$ or s_j^2 in this sum. We will write SoS_d for SoS limited to degree d or less. We allow ourselves, informally, to write inequalities in other forms than $q \geq 0$.

2.3 Relations between the systems

We are interested in whether or not a family of sets of equations is refutable in constant degree. Therefore for the purposes of this paper we will use the following definition of simulation of one system by another, rather than the more usual definition in proof complexity, which is based on refutation size.

Definition 11. *A system P* simulates *a system Q, written $P \geq Q$, if there is a function $f : \mathbb{N} \to \mathbb{N}$ such that, for any $d \in \mathbb{N}$, if a set of equations $\mathscr{F}$ is refutable in degree d in Q then $\mathscr{F}$ is refutable in degree $f(d)$ in P.*

Systems P and Q are equivalent, $P \equiv Q$, if both $P \geq Q$ and $Q \geq P$.

Trivially for any $\mathscr{R}$ we have $\mathsf{PC}_{\mathscr{R}} \leq \mathsf{PC}^{\mathrm{rad}}_{\mathscr{R}} \leq \mathsf{PC}^{+}_{\mathscr{R}}$ (but recall that $\mathsf{PC}^{+}_{\mathscr{R}}$ may or may not be sound, depending on $\mathscr{R}$). The main result of this section is to show that, for constant degree, the dynamic system PC^{+} is equivalent to the static system $\mathsf{SoS} + \mathsf{Bool}$ (Proposition 14 and Theorem 15).

Before proving this, we will say more about the radical rule. By implicational completeness, the rule is derivable in $\mathsf{PC}_{\mathscr{R}}$ in the presence of the Boolean axioms. However, potentially it can happen that all these derivations are of large degree. The following proposition shows that it can be derived in constant degree if $\mathscr{R}$ is a field of positive characteristic.

Proposition 12. *Suppose $\mathscr{R}$ is a field of positive characteristic. Then, in the presence of the Boolean axioms, $\mathsf{PC}_{\mathscr{R}} \equiv \mathsf{PC}^{rad}_{\mathscr{R}}$.*

Proof. Let $\mathscr{R}$ have characteristic p. It is sufficient to show that for any polynomial f in the x_i variables, we have $f^{p-2} \cdot f^2 \equiv f \mod \{x_i^2 - x_i \ : \ i \in \mathbb{N}\}$, and specifically that we can derive f from $f^{p-2} \cdot f^2$ in $\mathsf{PC}_{\mathscr{R}} + \mathsf{Bool}$ with a degree $O(p)$. For if this is true, then by multiplying f^2 with f^{p-2}, we get a $\mathsf{PC}_{\mathscr{R}} + \mathsf{Bool}$ derivation $f^2 = 0 \vdash f = 0$ of degree $O(\deg f)$. This will conclude the proof of the proposition since we can replace applications of the radical rule with derivations of this form.

Consider first the case that f has two monomials: $f = A + B$. Then, $f^p = (A+B)^p = A^p + \binom{p}{1}A^{p-1}B + \binom{p}{2}A^{p-2}B^2 + \cdots + \binom{p}{1}AB^{p-1} + B^p$. Note that for every $k > 0$, $\binom{p}{k}$ is a product of p, hence equals 0 modulo p. Thus, all monomials in the above equation have 0 coefficients, except for the first and last monomials, namely: $f^p = A^p + B^p$. Every variable power x^d in A, B, for some $d \leq \deg f$, appears in A^p and B^p as x^{dp}. By using the Boolean axiom enough times we can replace x^{dp} by x in A and B. We thus get to $A + B$, and the PC derivation has degree at most $O(\deg f)$ (recall that p is a constant).

The same idea when f has more than two monomials applies as well, using induction on the number of monomials in f: write $f = A + C$ with A a monomial and C a polynomial. Then, by the same argument as above, we get $f^p = A^p + C^p$ in a PC derivation of degree at most $O(\deg f)$. Then, $A^p = A$ as above. And by induction hypothesis $C^p = C$ has a PC derivation of degree $O(\deg f)$. □

On the other hand, if $\mathscr{R}$ is a field of characteristic 0, then by the following lemma $\mathsf{PC}^{\mathrm{rad}}_{\mathscr{R}}$ is strictly stronger than $\mathsf{PC}_{\mathscr{R}}$ with respect to derivations, even in the presence of Boolean axioms. It is open whether there is a simulation if we only consider refutations.

Proposition 13. *If $\mathscr{R}$ is a field of characteristic 0, then $\mathsf{PC}_{\mathscr{R}}$ derivations of*

$$\{x_i^2 - x_i = 0 : i = 1, \ldots, n\} \cup \{(x_1 + \cdots + x_n + 1)^2 = 0\} \vdash x_1 + \cdots + x_n + 1 = 0$$

require degree $\Omega(n)$.

Proof. The argument is the same as for the $\mathsf{PC}_{\mathscr{R}}$ lower bound for the Subset Sum principle in [22]. By Lemma 5.2 in [22] if $q \in \mathscr{R}[x_1,\dots,x_n]$ is a multilinear polynomial of degree $d \le n/2$, then the degree of $ml(q\cdot(x_1+\cdots+x_n+1))$ is $d+1$, where ml is the multilinearization operator[3]. Consequently, if r is multilinear of degree $d \le n/2-1$, then the degree of $ml(r\cdot(x_1+\cdots+x_n+1)^2)$ is $d+2$.

Consider a $\mathsf{PC}_{\mathscr{R}}$ derivation π as in the statement of the proposition. We will work with multilinearizations of lines of π, since this allows us to ignore Boolean axioms. Thus multilinearizations of lines of π have the form $ml(r\cdot(x_1+\cdots+x_n+1)^2)$ for some multilinear r. Consider the first line in π such that $\deg(ml(r\cdot(x_1+\cdots+x_n+1)^2)) < \deg(r)+2$ — such a line exists, since the last line of π is $x_1+\cdots+x_n+1=0$, of degree 1. By the discussion above, Lemma 5.2 in [22] implies that $\deg(r) > n/2-1$.

Multilinearization of at least one of the premises of this line must satisfy $\deg(ml(r'\cdot(x_1+\cdots+x_n+1)^2)) = \deg(r')+2$ and $\deg(r') \ge \deg(r)-1 > n/2-2$. As multilinearization does not increase the degree, this proves that there is a line in π of degree at least $n/2-2$. □

We now show the simulations between SoS and PC^+.

Proposition 14. *If $\mathscr{S}$ is refutable in degree d in* SoS *then it is refutable in degree d in* PC^+. *Furthermore this refutation does not use the radical rule.*

Proof. Suppose $\mathscr{S} = \{p_i = 0 : i \in I\}$ has a SoS refutation expressed by an equality

$$\sum_i r_i p_i + \sum_j s_j^2 \equiv -1.$$

In PC^+, derive from $\mathscr{S}$ the equation $-\sum_i r_i p_i = 0$. By the above equality, this is equivalent to $1+\sum_j s_j^2 = 0$, so we can derive $1=0$ by a single application of the sum-of-squares rule. □

Theorem 15. SoS + Bool *simulates* PC^+, *and the simulation at most doubles the degree.*

Our argument for Theorem 15 is an extension of the simulation of $\mathsf{PC}_{\mathbb{R}}$ in SoS described in [9], which works by translating $\mathsf{PC}_{\mathbb{R}}$ derivations of $p=0$ into SoS + Bool derivations of $p^2 \le 0$. We additionally need to deal with the radical and sum-of-squares rules.

We first show that SoS + Bool "approximately simulates" PC^+ with respect to derivations, in that it can derive that p^2 is bounded by some arbitrarily small ϵ. Notice that although the degree is independent of ϵ, making ϵ smaller may increase the *size* of the proof (depending how size is measured) since it affects the coefficients.

Lemma 16. *Suppose $r=0$ is derivable from a set of equalities $\mathscr{S}$ by a PC^+ derivation of degree d. Then, for every $\epsilon > 0$, there exists a degree $2d$* SoS + Bool *derivation of $r^2 \le \epsilon$ from $\mathscr{S}$.*

Proof. Let $r_1 = 0,\dots,r_s = 0$ be the PC^+ derivation. We prove by induction on s that, for every $\epsilon > 0$, $-r_s^2+\epsilon \ge 0$ has an SoS + Bool proof of degree $2d$. The argument is by cases, depending on how $r_s = 0$ is derived. In case $r_s = 0$ is an axiom from $\mathscr{S}$, the SoS + Bool derivation is trivial.

Suppose $r_s = 0$ is derived by the multiplication rule, that is, $r_s \equiv x r_k$ for some earlier equality $r_k = 0$ and some variable x. By the inductive hypothesis there exists a SoS + Bool derivation π of $-r_k^2+\epsilon \ge 0$ of degree $2d$. We have

$$(r_k - x r_k)^2 + (-2r_k^2)(x^2 - x) \equiv r_k^2 - 2x r_k^2 + x^2 r_k^2 - 2x^2 r_k^2 + 2x r_k^2 \equiv r_k^2 - x^2 r_k^2$$

[3] This lemma is stated for reals in [22], but the proof applies to any field of characteristic 0.

so we can derive $-x^2 r_k^2 + \epsilon \geq 0$ by adding the expression $(r_k - x r_k)^2 + (-2r_k^2)(x^2 - x)$ to π.

Suppose $r_s = 0$ is derived by the addition rule, so $r_s \equiv a r_i + b r_j$ for some $i, j < s$ and some $a, b \in \mathbb{R}$. We will assume neither of a, b is 0 — the case when one of them is 0 is similar, and when both are 0 there is nothing to prove. By the inductive hypothesis there exist SoS + Bool derivations π of $-r_i^2 + \frac{\epsilon}{4a^2} \geq 0$ and π' of $-r_j^2 + \frac{\epsilon}{4b^2} \geq 0$, both of degree $2d$. We have

$$2a^2(-r_i^2 + \frac{\epsilon}{4a^2}) + 2b^2(-r_j^2 + \frac{\epsilon}{4b^2}) + (a r_i - b r_j)^2 \equiv -a^2 r_i^2 - b^2 r_j^2 + \epsilon - 2ab r_i r_j \equiv -r_s^2 + \epsilon.$$

Thus $2a^2\pi + 2b^2\pi' + (a r_i - b r_j)^2$ is a derivation of $-r_s^2 + \epsilon \geq 0$.

Suppose $r_s = 0$ is derived by the radical rule, so $r_k \equiv r_s^2$ for some $k < s$. We have

$$\tfrac{1}{2\epsilon}[-r_k^2 + \epsilon^2 + (\epsilon - r_k)^2] \equiv -r_k + \epsilon.$$

By the inductive hypothesis there is an SoS + Bool derivation π of $-r_k^2 + \epsilon^2 \geq 0$. By the equivalence above, $\frac{1}{2\epsilon}[\pi + (\epsilon - r_k)^2]$ is a derivation of $-r_k + \epsilon \geq 0$, that is, of $-r_s^2 + \epsilon \geq 0$.

Finally suppose $r_s = 0$ is derived by the sum-of-squares rule, so $r_s = p^2$ and $r_k = p^2 + \sum_i q_i^2$ for some $k < s$ and some polynomials $p, q_1, \ldots, q_m$. By the inductive hypothesis there is an SoS + Bool derivation π of $-(p^2 + \sum_i q_i^2)^2 + \epsilon \geq 0$. This can be rewritten as $-p^4 - A + \epsilon \geq 0$ for some sum of squares A. Hence $\pi + A$ is a derivation of $-p^4 + \epsilon \geq 0$. □

Proof of Theorem 15. We are given a PC^+ derivation of $1 = 0$, in degree d, from a set of equalities $\mathscr{S}$. By Lemma 16, setting $\epsilon = \frac{1}{2}$, there is a SoS + Bool derivation π of $-1 + \frac{1}{2} \geq 0$ from $\mathscr{S}$ in degree at most $2d$. Thus 2π is the required SoS + Bool refutation of $\mathscr{S}$. □

2.4 Infinite sets and large derivations

So far we have worked with derivations from *finite* sets of assumptions. However, for technical reasons to do with our translation we also want to allow infinite sets $\mathscr{F}$. So we extend the definitions of refutations and derivations by defining, for all systems, a derivation $\mathscr{F} \vdash e$ to be a derivation $\mathscr{F}' \vdash e$ for some finite $\mathscr{F}' \subseteq \mathscr{F}$. This does not change anything significant above.

Propositions 7 and 8, the implicational completeness of $\mathsf{PC}_{\mathbb{F}}^{\mathrm{rad}}$ (for $\mathbb{F}$ an algebraically closed field) and PC^+, still hold in the infinite case, because of the algebraic fact that if the underlying ring $\mathscr{R}$ is a field then $\mathscr{R}[x_1, \ldots, x_n]$ is Noetherian (every ideal is finitely generated). So the proofs still go through. The simulation results still hold, because they are about degree rather than size.

We also introduce the notion of a derivation of a (possibly infinite) set of equations $\mathscr{G}$ from a set of equations $\mathscr{F}$. We formally take this to be a function associating a derivation $\mathscr{F} \vdash e$ to each equation $e \in \mathscr{G}$; we may sometimes think of it in a less structured way, as a set of derivations. We define derivations of sets of inequalities similarly. The degree of a derivation $\mathscr{F} \vdash \mathscr{G}$ is the maximum of the degrees of the derivations it contains, if this maximum exists.

3 Algebraic and semi-algebraic first-order theories

Let $\mathscr{R}$ be an integral domain. We introduce $\mathsf{TPC}_{\mathscr{R}}$, a two-sorted theory in the language $\mathscr{L}_{=}^{\mathscr{R}}$ described below, with a *ring* sort and an *index* sort. We will talk about *ring elements*, *ring variables*, *ring-valued terms* and on the other hand *index elements* etc. and these have the obvious meanings. Index elements model natural numbers. As much as possible we will use names $i, j, k, \ldots$ for elements or variables of the index sort, and $a, b, c, \ldots$ or $x, y, z, \ldots$ for the ring sort.

3.1 The language $\mathscr{L}_{=}^{\mathscr{R}}$

The language contains:

- The usual algebraic operations $+, -, \cdot$ on the ring sort.
- A ring-valued *oracle symbol* $X(i)$, where i is index-sort.
- A special *big sum* operator Σ used to form new terms expressing the sum of a family of terms. This is not strictly part of the language — see the formal definition below.
- Equality symbols $=_{\text{ind}}$ and $=_{\text{ring}}$ for the two sorts. We will usually omit the subscripts.
- A set F_{ind} containing, for every arity $k \in \mathbb{N}$ and *every* function $f : \mathbb{N}^k \to \mathbb{N}$, a function symbol for f, mapping k-tuples of index elements to an index element.
- A set F_{ring} containing, for every arity $k \in \mathbb{N}$ and *every* function $f : \mathbb{N}^k \to \mathscr{R}$, a function symbol for f, mapping k-tuples of index elements to a ring element.

The intended meaning of $X(i)$ is the ith element in an otherwise unspecified sequence of ring-sort values. Atomic formulas in the language will correspond to polynomial equations in propositional variables $X(i)$. Notice that F_{ind} and F_{ring} are uncountable, that F_{ind} contains an index-sort constant for every $i \in \mathbb{N}$ and that F_{ring} contains a ring-sort constant for every $a \in \mathscr{R}$.

Definition 17. *Formally $\mathscr{L}_{=}^{\mathscr{R}}$ is defined inductively as follows.*

- *It contains the symbols from $\{+, -, \cdot, X, =_{\text{ind}}, =_{\text{ring}}\}$, F_{ind} and F_{ring} as defined above.*
- *For every ring-valued $\mathscr{L}_{=}^{\mathscr{R}}$ term $t(i, \bar{m}, \bar{z})$, taking index variables $\bar{m}$ and ring variables $\bar{z}$ and also a distinguished index variable i, it contains a ring-sort function symbol $\sum_{t,i}(n, \bar{m}, \bar{z})$, where n is an index variable.*

We will usually write $\sum_{t,i}(n, \bar{m}, \bar{z})$ in a more conventional way as $\sum_{i<n} t(i, \bar{m}, \bar{z})$, and this is its intended meaning. Note that we may freely use standard relations on the index sort such as $i < n$, as they have characteristic functions in F_{ind}, and that the term t in Definition 17 may itself contain the big sum symbol, so we can have nested big sums in the language.

We work in the standard setting of first-order (two sorted) logic. Hence, the class of $\mathscr{L}_{=}^{\mathscr{R}}$ *terms* are constructed by the function symbols $+, \cdot, -$, the function symbols in F_{ind} and F_{ring}, the oracle symbol X, the big sum terms, and the variables (of both sorts) that can also occur in function symbols. The class of $\mathscr{L}_{=}^{\mathscr{R}}$ *formulas* consists of the *atomic formulas*, which are equalities (of either sort) between terms, and general formulas which are constructed as usual from atomic formulas and the logical connectives and quantifiers (for both sorts) $\vee, \wedge, \neg$ and $\exists, \forall$.

Definition 18. *Let σ be an $\mathscr{L}_{=}^{\mathscr{R}}$-symbol or a variable. We inductively say that an $\mathscr{L}_{=}^{\mathscr{R}}$-expression* mentions *$\sigma$ if it either contains σ, or contains a symbol $\sum_{s,i}$ for a term s that mentions σ.*

Definition 19. *A* standard model *for $\mathscr{L}_{=}^{\mathscr{R}}$ is a structure $\langle \mathbb{N}, \mathscr{R}, A \rangle$ where $\mathbb{N}$ interprets the index sort, $\mathscr{R}$ interprets the ring sort, A is a function $\mathbb{N} \to \mathscr{R}$ interpreting the symbol X, and all the other symbols have their natural interpretations. We say that a sentence which does not mention X is* true in the standard model *if it is true in any standard model $\langle \mathbb{N}, \mathscr{R}, A \rangle$.*

Our language has the important property that terms translate into families of polynomials of bounded degree parametrized by their index arguments (the converse is also true). We now use this to define a class $\Phi_=^{\mathscr{R}}$ of $\mathscr{L}_=^{\mathscr{R}}$ formulas with the property that every formula in the class translates into a system of polynomial equations of bounded degree. For the formal translations see Sections 5.1 and 5.2.

Definition 20. *The class $\Phi_=^{\mathscr{R}}$ is defined inductively by:*

- *All atomic formulas are in $\Phi_=^{\mathscr{R}}$*
- *All formulas, of any logical complexity, which do not mention the oracle X or any ring variable, are in $\Phi_=^{\mathscr{R}}$*
- *If $\varphi_1, \varphi_2 \in \Phi_=^{\mathscr{R}}$, then $\varphi_1 \vee \varphi_2 \in \Phi_=^{\mathscr{R}}$ and $\varphi_1 \wedge \varphi_2 \in \Phi_=^{\mathscr{R}}$*
- *If $\varphi(v) \in \Phi_=^{\mathscr{R}}$, where v may have either sort, then $\forall v \varphi(v) \in \Phi_=^{\mathscr{R}}$.*

Notice that existential quantifiers and negation symbols can appear in such a formula, because this is allowed by the second item; but ring variables and the symbol X cannot be mentioned in the scope of any of these symbols.

We will show that even when the ring is infinite, $\forall v \varphi(v)$ in Definition 20 can be translated adequately into a set of polynomials of bounded-degree, and the fact that the set of polynomials is infinite does not constitute an obstacle to our results.

3.2 The axioms of $\mathsf{TPC}_{\mathscr{R}}$ and TSoS

The theory $\mathsf{TPC}_{\mathscr{R}}$ consists of the *basic axioms* and the *induction scheme*. The theory TSoS additionally contains the Boolean axiom and the *sum-of-squares* scheme. The axioms and schemes are listed below. If we say that a formula with free variables is an axiom, we really mean that its universal closure is.

Basic axioms

- The standard ring axioms for $0, 1 \in \mathscr{R}$ and $+, -, \cdot$.
- The integral domain axiom $xy = 0 \supset (x = 0 \vee y = 0)$.
- The big sum defining axiom scheme. This contains, for each ring-valued term $t(i)$, in which other parameters can also occur, the axioms
$$\sum_{i<0} t(i) = 0 \qquad \sum_{i<j+1} t(i) = \sum_{i<j} t(i) + t(j).$$
- Every sentence σ such that
  (i) σ does not mention the oracle symbol X or any ring variable, and
  (ii) σ is true in the standard model.

  We call (i), (ii) the *background truth* axioms.
- The ring-sort and index-sort equality axiom schemes. That is, all formulas of the forms
$$x = x \qquad i = i \qquad \overline{x} = \overline{y} \wedge \overline{i} = \overline{j} \supset f(\overline{x}, \overline{i}) = f(\overline{y}, \overline{j})$$
  where f is a function symbol and each $=$ is either $=_{\text{ind}}$ or $=_{\text{ring}}$ as appropriate.

Induction scheme

- For every formula $\varphi(i)$ in the class $\Phi^{\mathscr{R}}_{=}$, in which other parameters can also occur, the induction axiom

$$\varphi(0) \wedge \forall i\,(\varphi(i) \supset \varphi(i+1)) \;\supset\; \forall n\,\varphi(n).$$

Sum-of-squares scheme and Boolean axiom

- For each ring-valued term $t(i)$, in which other parameters can also occur, the axiom

$$\sum_{i<n} t(i)^2 = 0 \wedge j < n \;\supset\; t(j) = 0.$$

- The axiom $X(i)(1 - X(i)) = 0$.

In the presence of the integral domain axiom, the Boolean axiom is equivalent to asserting that X is 0/1 valued.

4 Examples of first-order proofs

We will discuss how some versions of the pigeonhole principle (PHP, for short) can be proved in $\mathsf{TPC}_{\mathscr{R}}$ and TSoS, to give some simple examples of how the theories and translations work. We present a less-trivial proof in Section 7 below, showing that these theories prove respectively that every (definable) constant-degree $\mathsf{PC}_{\mathscr{R}}$ or SoS refutation is sound. It will follow that everything provable in the theory is provable in constant-degree in the corresponding proof system (including, as is well-known, the versions of PHP described here).

We first establish some basic properties of big sums in $\mathsf{TPC}_{\mathscr{R}}$.

Lemma 21. *The following are provable in* $\mathsf{TPC}_{\mathscr{R}}$*, for all terms* s, t*.*

1. $\sum_{i<n}\big(s(i)+t(i)\big) = \sum_{i<n} s(i) + \sum_{i<n} t(i)$
2. $\big(\sum_{i<n} s(i)\big)\cdot t = \sum_{i<n}\big(s(i)\cdot t\big)$
3. $\sum_{i<m}\big(\sum_{j<n} t(i,j)\big) = \sum_{j<n}\big(\sum_{i<m} t(i,j)\big)$
4. *If* $m < n$*,* $t(m) = 1$ *and* $t(i) = 0$ *if* $i < n$ *and* $i \neq m$*, then* $\sum_{i<n} t(i) = 1$*.*

Proof. These are proved by straightforward inductions. Items 1. and 2. are easy. For item 3. we have

$$\begin{aligned}
\sum_{i<m+1}\Big(\sum_{j<n} t(i,j)\Big) &= \sum_{i<m}\Big(\sum_{j<n} t(i,j)\Big) + \sum_{j<n} t(m,j)\\
&= \sum_{j<n}\Big(\sum_{i<m} t(i,j)\Big) + \sum_{j<n} t(m,j)\\
&= \sum_{j<n}\Big(\sum_{i<m} t(i,j) + t(m,j)\Big)\\
&= \sum_{j<n}\Big(\sum_{i<m+1} t(i,j)\Big),
\end{aligned}$$

where the equations follow from respectively the big sum axiom, the inductive hypothesis (note that 3. is an atomic formula, hence in the class $\Phi^{\mathscr{R}}_{=}$), item 1. of the lemma, and the big sum axiom (together with the equality axiom scheme).

For item 4., let $\delta(i,j)$ be a function symbol in F_{ring} that the standard truth axioms prove is 0 if $i \leq j$ and 1 if $i > j$. Use induction on i on the equality $\sum_{j<i} t(j) = \delta(i,m)$. □

Definition 22. *We define* $\rho(n)$ *to be the term* $\sum_{j<n} 1$.

The term ρ expresses the natural homomorphism from the index sort to the ring sort given by the map $n \mapsto 1 + \cdots + 1$, where there are n many 1s in the sum (note that the ring $\mathscr{R}$ we work over may have positive characteristic, hence n and $\rho(n)$ may not be equal as numbers).

4.1 Bijective and graph PHP in $\mathsf{TPC}_{\mathscr{R}}$

To match the conventions of propositional proof complexity, we will present the principles in this section as contradictions to be refuted rather than tautologies to be proved.

Let $\theta(i,j)$ be a term. The *bijective pigeonhole principle* for θ and m,n, or $\text{bPHP}(\theta,m,n)$, asserts that $\theta(i,j)$ is the graph of a bijection between a set $[0,m)$ of pigeons and a set $[0,n)$ of holes, with m,n,i,j of index-sort. Precisely, it is the conjunction of the formulas:

1. for all $i < m$, $j < n$, either $\theta(i,j) = 0$ or $\theta(i,j) = 1$
2. for all $i < m$, $\theta(i,j) = 1$ for some $j < n$
3. for all $i < m$ and all $j, j' < n$, if $j \neq j'$ then $\theta(i,j) = 0$ or $\theta(i,j') = 0$
4. for all $j < n$, $\theta(i,j) = 1$ for some $i < m$
5. for all $j < n$ and all $i, i' < m$, if $i \neq i'$ then $\theta(i,j) = 0$ or $\theta(i',i) = 0$.

Notice that provability of bPHP in $\mathsf{TPC}_{\mathscr{R}}$ is only an interesting question if the term $\theta(i,j)$ mentions X or has a ring parameter. Otherwise it is trivially refutable using the background truth axioms (that is, its negation is a background truth axiom).

Proposition 23. $\mathsf{TPC}_{\mathscr{R}}$ *proves that if* $\rho(m) \neq \rho(n)$ *then* $\text{bPHP}(\theta,m,n)$ *is false.*

Proof. As we are working with classical logic, to show provability of a statement in $\mathsf{TPC}_{\mathscr{R}}$ it is enough to show that it holds in every model of $\mathsf{TPC}_{\mathscr{R}}$. Consider an arbitrary model of $\mathsf{TPC}_{\mathscr{R}}$, pick any index elements m,n and suppose for a contradiction that (in the model) $\rho(m) \neq \rho(n)$ and $\text{bPHP}(\theta,m,n)$ is true. Then for each pigeon i, by item 4. of Lemma 21 we have $\sum_{j<n} \theta(i,j) = 1$, and hence $\sum_{i<m}(\sum_{j<n} \theta(i,j)) = \rho(m)$. Similarly we have $\sum_{j<n}(\sum_{i<m} \theta(i,j)) = \rho(n)$. This contradicts item 3. of Lemma 21. □

Now let G_n be any sequence of bipartite graphs between $[0,m)$ and $[0,n)$ with degree bounded by d, where $d \in \mathbb{N}$ is fixed (and m is a function of n). We will define a first-order *bijective graph pigeonhole principle* for G_n, expressing that G_n has a perfect matching. Unlike bPHP as defined above, this formula will be $\Phi^{\mathscr{R}}_{=}$. This means that we can use the propositional translations defined in subsequent sections. The formula translates into the usual propositional bijective graph pigeonhole principle for G_n, and the existence of a first-order refutation in $\mathsf{TPC}_{\mathscr{R}}$ implies the existence of a constant-degree family of $\mathsf{PC}_{\mathscr{R}}$ refutations of these propositional formulas.

There are functions $h_1,\ldots,h_d,p_1,\ldots,p_d,m \in F_{\text{ind}}$ and $G \in F_{\text{ring}}$, all taking n as an unwritten argument, which describe the structure of the graphs G_n. Pigeon i has holes $h_1(i),\ldots,h_d(i)$ as neighbours and hole j has pigeons $p_1(j),\ldots,p_d(j)$ as neighbours, where these lists can contain repetitions. The ring-valued term $G(i,j)$ is 0 or 1 depending whether the edge (i,j) exists in G.

The formula $\text{bPHP}_G(n)$ expresses that X describes a perfect matching of G_n. We use a pairing function (which exists in F_{ind}) to treat X as a binary function symbol $X(i,j)$. The formula is the conjunction of:

1. For all $i < m$, for some $k \in [1,d]$, $X(i,h_k(i)) = 1$
2. For all $i < m$, for each pair $k,k' \in [1,d]$ either $h_k(i) = h_{k'}(i)$ or $X(i,h_k(i)) = 0$ or $X(i,h_{k'}(i)) = 0$
3. For all $j < n$, for some $k \in [1,d]$, $X(p_k(j),j) = 1$
4. For all $j < n$, for each pair $k,k' \in [1,d]$ either $p_k(j) = p_{k'}(j)$ or $X(p_k(j),j) = 0$ or $X(p_{k'}(i),i) = 0$.

Here we formalize "for some $k \in [1,d]$" as a disjunction of size d, and we formalize bounded index quantifiers of the form $\forall i < t\, \varphi(i)$ as $\forall i(i \geq t \vee \varphi(i))$. Thus the formula is $\Phi^{\mathscr{R}}_{=}$ and its propositional translation, under the assignment that maps the variable n to the natural number n, as described in the next section, is the usual bijective graph pigeonhole CNF on G_n.

Proposition 24. $\mathsf{TPC}_{\mathscr{R}}$ *proves that if* $\rho(m) \neq \rho(n)$ *then* $\text{bPHP}_G(n)$ *is false.*

Proof. Suppose $\text{bPHP}_G(n)$ is true. Let $\theta(i,j)$ be the term $X(i,j)\cdot G(i,j)$, which takes the value of X on edges of G_n and is otherwise 0. Then the basic axioms of $\mathsf{TPC}_{\mathscr{R}}$ are enough to show that items 1.–5. from the definition of $\text{bPHP}(\theta,m,n)$ are true. The result follows by Proposition 23. □

Using the translations in Sections 5 and 6 below we obtain the well-known propositional refutation of $\text{bPHP}_G(n)$ as a corollary. Recall that m is the cardinality of set of pigeons in G_n.

Corollary 25. *Suppose* $\rho(m) \neq \rho(n)$ *for all* $n \in \mathbb{N}$. *Then* $\mathsf{TPC}_{\mathscr{R}}$ *proves* $\forall n \neg \text{bPHP}_G(n)$. *Hence the propositional family* $\text{bPHP}(G_n)$ *has refutations in* $\mathsf{PC}_{\mathscr{R},d}$ *in some fixed degree* d.

Proof. Under the assumption, $\rho(m) \neq \rho(n)$ is one of the standard truth axioms. □

4.2 Functional PHP in TSoS

We now fix the ring $\mathscr{R}$ to be the reals, and work in TSoS. Recall that this is $\mathsf{TPC}_{\mathbb{R}}$ plus the sum of squares axiom scheme and the Boolean axiom (Section 3.2). The *functional pigeonhole principle* for θ and m,n, or $\text{fPHP}(\theta,m,n)$, consists of items 1., 2., 3. and 5. from the definition of the bijective pigeonhole principle at the start of the previous subsection (it omits item 4., surjectivity). It asserts that θ is the graph of an injective function from $[0,m)$ to $[0,n)$.

We will use a kind of counting lemma.

Lemma 26. $\mathsf{TPC}_{\mathscr{R}}$ *proves the following. Suppose for all* $i,j < n$ *we have* $t(i)^2 = t(i)$ *and* $t(i)t(j) = 0$ *if* $i \neq j$. *Then* $\sum_{i<n} t(i) = 1 - (\sum_{i<n} t(i) - 1)^2$.

Proof. Expanding the right hand side shows it is enough to derive $(\sum_{i<n} t(i))^2 = \sum_{i<n} t(i)$. Using item 2. of Lemma 21, for each $j < n$ we have $t(j)\sum_{i<n} t(i) = \sum_{i<n} t(i)t(j)$. This equals $t(j)$, which can be shown by the assumptions about t and an induction over the partial sums, as in the proof of item 4. of Lemma 21. Summing these terms together gives the result, again by item 2. □

Of course this lemma also holds for TSoS, and in the context of that theory we can informally interpret the conclusion of the lemma as "$\sum_{i<n} t(i) \leq 1$", since we have shown it is 1 minus a sum of squares. What we would like to be able to do (and the general goal of this research) is to enrich TSoS to a theory with an ordering symbol on the ring sort, which allows us to *formally* write the conclusion as $\sum_{i<n} t(i) \leq 1$ and reason naturally about inequalities rather than about explicitly written sums of squares. We describe an approach to this goal in Section 9.

Proposition 27. TSoS *proves that if* $m > n$ *then* fPHP(θ, m, n) *is false.*

Proof. As in the proof of Proposition 23, for each pigeon $i < m$ we derive $\sum_{j<n} \theta(i,j) = 1$ and sum to get $\sum_{i<m}(\sum_{j<n} \theta(i,j)) = \rho(m)$.

Now consider a hole $j < n$. We have $\theta(i,j)^2 = \theta(i,j)$ for each $i < m$, since the values are all 0 or 1, and we know $\theta(i,j)\theta(i',j) = 0$ for distinct $i, i' < m$. Thus by Lemma 26 we have $\sum_{i<m} \theta(i,j) = 1 - A(j)^2$ for some term $A(j)$.

Hence $\sum_{j<n}(\sum_{i<m} \theta(i,j)) = \rho(n) - \sum_{j<n} A(j)^2$. Using Lemma 21 we can change the order of summations, so we can combine this with the sum over pigeons to get $\rho(m) - \rho(n) + \sum_{j<n} A(j)^2 = 0$. But since $m > n$ we have $\rho(m) - \rho(n) = \rho(m-n)$ which is a nontrivial sum of squares $1 + \cdots + 1$. Thus, by the sum-of-squares axiom, all of the terms in the sum $1 + \cdots + 1 + A(0)^2 + \cdots + A(n-1)^2$ are 0, and in particular $1 = 0$. □

As before, for a sequence of bipartite graphs G_n we can define a first-order *functional graph pigeonhole principle* for G_n, or fPHP$_G(n)$, expressing that X is the graph of an injective mapping from m to n along edges of G_n. This consists of 1., 2. and 3. from the definition of bPHP$_G(n)$ above, together with the condition that $X(i,j)$ always takes the value 0 or 1 on G_n.

Proposition 28. TSoS *proves that if* $m > n$ *then* fPHP$_G(n)$ *is false.*

Proof. As before it is enough to define $\theta(i,j)$ to be $X(i,j) \cdot G(i,j)$ and check that this satisfies all the conditions of fPHP(θ, m, n). □

Corollary 29. *Suppose* $m > n$ *for all* $n \in \mathbb{N}$. *Then* TSoS *proves* $\forall n \neg$fPHP$_G(n)$. *Hence the propositional family* fPHP(G_n) *has refutations in* SoS + Bool *in some fixed degree* d.

5 Propositional translations of formulas

Let α be an assignment of values in $\mathbb{N}$ to all index variables, and values in $\mathscr{R}$ to all ring variables. We will define a translation $\langle\cdot\rangle_\alpha$ of certain $\mathscr{L}_=^{\mathscr{R}}$ expressions into our propositional language, with the following form:

- For an index-valued term t, $\langle t \rangle_\alpha$ is an integer
- For a ring-valued term t, $\langle t \rangle_\alpha$ is a polynomial in $\mathbb{R}[x_0, x_1, \ldots]$ of bounded degree
- For a formula $\varphi \in \Phi_=^{\mathscr{R}}$, $\langle \varphi \rangle_\alpha$ is a set of equations of bounded degree.

"Bounded degree" here means that the degree does not depend on α.

5.1 Translation of terms

First suppose t is an index-valued term. We define $\langle t \rangle_\alpha$ to be simply the number in $\mathbb{N}$ given by evaluating t under α. This is possible because, by construction, t is formed only by composing functions in F_{ind} and in particular cannot have any ring arguments.

Now suppose t is a ring-valued term. We will inductively define a translation of t into a polynomial $\langle t \rangle_\alpha$ in $\mathscr{R}[x_0, x_1, \dots]$, whose degree is bounded by a number which depends only on the nesting of the multiplication symbol in t. (On the other hand the *size* of $\langle t \rangle_\alpha$ as measured by, say, the number of monomials in it, may be unbounded as α varies.)

- If t has the form $f(s_1, \dots, s_k)$ where $f \in F_{\text{ring}}$ and $s_1, \dots, s_k$ are index-valued, then $\langle t \rangle_\alpha$ is the constant polynomial $f(\langle s_1 \rangle_\alpha, \dots, \langle s_k \rangle_\alpha)$.
- If t has the form $X(s)$ where s is index-valued, then $\langle t \rangle_\alpha$ is the variable x_j where $j = \langle s \rangle_\alpha$.
- If t is a ring variable y_i then $\langle t \rangle_\alpha$ is the constant polynomial $\alpha(y_i)$.
- Ring operations $+, -, \cdot$ are translated as the corresponding operations on polynomials.
- We define $\langle \sum_{t,i}(n) \rangle_\alpha$ to be the sum $\langle t(0) \rangle_\alpha + \dots + \langle t(n-1) \rangle_\alpha$.

Lemma 30. *For $d, k \in \mathbb{N}$ let $p_{i_1,\dots,i_k}$ be any family of polynomials in $\mathscr{R}[x_1, x_2, \dots]$ all of degree d or less. Then there is a single ring-valued term $t(i_1, \dots, i_k)$ such that $\langle t \rangle_\alpha = p_{n_1,\dots,n_k}$ for any assignment α mapping i_j to n_j for each j.*

Proof. Let $q_{\bar{n}}$ be a family of polynomials in $\mathscr{R}[x_0, x_1, \dots]$ in which every monomial has degree exactly d. Then $p_{n_1,\dots,n_k}$ is a finite sum of such polynomials. By the definitions of F_{ind} and F_{ring}, we can find function symbols $N, \nu_1, \dots, \nu_d \in F_{\text{ind}}$ and $a \in F_{\text{ring}}$ such that $q_{\bar{n}} \equiv \langle \sum_{j < N(\bar{i})} a(\bar{i}, j) \cdot X(\nu_1(\bar{i}, j)) \cdot \dots \cdot X(\nu_d(\bar{i}, j)) \rangle_\alpha$. □

5.2 Translation of formulas

We translate $\Phi^{\mathscr{R}}_{=}$ formulas φ into sets of equations. First suppose φ does not mention X or any ring variable. We evaluate φ under α in the standard model, and set $\langle \varphi \rangle_\alpha := \{0 = 0\}$ if it is true and $\langle \varphi \rangle_\alpha := \{1 = 0\}$ if it is false.

Below, for an assignment α, we will use the notation $\alpha[i \mapsto n]$ for α with the value of i changed to n. We will also do this for ring variables, and will write for example $\alpha[\bar{i}, \bar{y} \mapsto \bar{n}, \bar{a}]$ when we want to change several index and ring values at once. If we omit α and just write an assignment in square brackets, this means that all other variables are mapped to 0 (or arbitrarily).

Now suppose that φ does mention X or a ring variable. The translation of φ is defined inductively. Recall that for sets of equations $\mathscr{P}$ and $\mathscr{Q}$, the product $\mathscr{P} \cdot \mathscr{Q}$ is $\{p \cdot q = 0 : p = 0 \in \mathscr{P},\ q = 0 \in \mathscr{Q}\}$.

- Suppose φ is an atomic formula $t = r$. By the condition on φ, both t and r are ring-valued, since all index-valued function symbols are in F_{ind} and none of them takes any ring arguments. We put $\langle \varphi \rangle_\alpha := \{\langle t \rangle_\alpha - \langle r \rangle_\alpha = 0\}$.
- If $\varphi = \psi \wedge \psi'$ then $\langle \varphi \rangle_\alpha := \langle \psi \rangle_\alpha \cup \langle \psi' \rangle_\alpha$.
- If $\varphi = \psi \vee \psi'$ then $\langle \varphi \rangle_\alpha := \langle \psi \rangle_\alpha \cdot \langle \psi' \rangle_\alpha$.
- If $\varphi = \forall i\, \psi(i)$ for an index variable i, then $\langle \varphi \rangle_\alpha := \bigcup_{n \in \mathbb{N}} \langle \psi \rangle_{\alpha[i \mapsto n]}$.

- If $\varphi = \forall y\, \psi(y)$ for a ring variable y, then $\langle\varphi\rangle_\alpha := \bigcup_{a\in\mathscr{R}} \langle\psi\rangle_{\alpha[y\mapsto a]}$.

Notice that, by the last item, $\langle\varphi\rangle_\alpha$ may be infinite.

This translation captures the semantics of φ, in the sense that if we fix an oracle A, and identify A with the assignment mapping $x_0 \mapsto A(0), x_1 \mapsto A(1), \ldots$, then φ is true under α in the standard model $\langle\mathbb{N}, \mathscr{R}, A\rangle$ if and only if all polynomial equations in $\langle\varphi\rangle_\alpha$ are satisfied by A.

6 Propositional translations of proofs

We prove the following theorem. Note that if $\mathscr{R}$ has positive characteristic then by Proposition 12 we get a version of this with $\mathsf{PC}_\mathscr{R} + \mathsf{Bool}$ in place of $\mathsf{PC}^{\mathrm{rad}}_\mathscr{R}$.

Theorem 31. *Let $\varphi(\bar{i})$ be a $\Phi^\mathscr{R}_=$ formula with free index variables $\bar{i}$ and no free ring variables. Suppose $\mathsf{TPC}_\mathscr{R} \vdash \forall \bar{i} \neg\varphi(\bar{i})$. Then for some $d \in \mathbb{N}$, for every tuple $\bar{n} \in \mathbb{N}$ there is a $\mathsf{PC}^{rad}_{\mathscr{R},d}$ refutation of $\langle\varphi\rangle_{[\bar{i}\mapsto\bar{n}]}$.*

The proof is by first translating $\mathsf{TPC}_\mathscr{R}$ proofs into a Gentzen-style sequent calculus $\mathsf{LK}_\mathscr{R}$ and then translating $\mathsf{LK}_\mathscr{R}$ into $\mathsf{PC}^{\mathrm{rad}}_\mathscr{R}$ rule-by-rule.

6.1 The sequent calculus $\mathsf{LK}_\mathscr{R}$

$\mathsf{LK}_\mathscr{R}$ is a two-sorted sequent calculus with an index and a ring sort. To satisfy a technical condition necessary for our cut-elimination theorem to hold [11], we define it so that the axioms, and the class of formulas for which we have an induction rule, are closed under substitutions of terms for free variables. It is defined as follows:

- $\mathsf{LK}_\mathscr{R}$ contains the usual structural and logical rules of two-sorted logic.
- Any axiom of $\mathsf{TPC}_\mathscr{R}$ which is not an integral domain, equality, or induction axiom is the universal closure of a $\Phi^\mathscr{R}_=$ formula $\varphi(\bar{i}, \bar{x})$. For each such φ, $\mathsf{LK}_\mathscr{R}$ contains the axiom

$$\emptyset \longrightarrow \varphi(\bar{s}, \bar{t})$$

  for all tuples of index-valued terms $\bar{s}$ and ring-valued terms $\bar{t}$ of appropriate arity.
- $\mathsf{LK}_\mathscr{R}$ contains every substitution of terms for variables in the integral domain axiom

$$xy = 0 \longrightarrow x = 0, y = 0$$

  and the equality schemes

$$\emptyset \longrightarrow x = x \qquad\qquad \emptyset \longrightarrow i = i$$
$$\bar{x} = \bar{y}, \bar{i} = \bar{j} \longrightarrow f(\bar{x}, \bar{i}) = f(\bar{y}, \bar{j}).$$

- $\mathsf{LK}_\mathscr{R}$ contains the $\Phi^\mathscr{R}_=$-induction rule

$$\frac{\Gamma, \varphi(i) \longrightarrow \varphi(i+1), \Delta}{\Gamma, \varphi(0) \longrightarrow \varphi(t), \Delta}$$

where t is any index-valued term, $\varphi \in \Phi_=^{\mathscr{R}}$ may contain other parameters, and i is an index variable which does not occur in the bottom sequent.

Lemma 32. *Let φ be any formula such that the universal closure of φ is provable in $\mathsf{TPC}_{\mathscr{R}}$. Then the sequent $\emptyset \longrightarrow \varphi$ is derivable in $\mathsf{LK}_{\mathscr{R}}$. If furthermore φ is a negation $\neg\psi$, then the sequent $\psi \longrightarrow \emptyset$ is derivable in $\mathsf{LK}_{\mathscr{R}}$.*

Proof. Since $\mathsf{LK}_{\mathscr{R}}$ is complete with respect to pure logic it is enough to check that, for every axiom σ of $\mathsf{TPC}_{\mathscr{R}}$, the sequent $\emptyset \longrightarrow \sigma$ is derivable in $\mathsf{LK}_{\mathscr{R}}$. This is standard. □

6.2 Translation of $\mathsf{LK}_{\mathscr{R}}$ into $\mathsf{PC}^{\mathbf{rad}}_{\mathscr{R}}$

Consider a sequent $\Gamma \to \Delta$. We treat cedents as multisets of formulas. We define

$$\langle\Gamma\rangle^L_\alpha := \bigcup_{\varphi\in\Gamma} \langle\varphi\rangle_\alpha \qquad \text{and} \qquad \langle\Delta\rangle^R_\alpha := \prod_{\varphi\in\Delta} \langle\varphi\rangle_\alpha.$$

The superscripts L and R stand for *Left* and *Right*, and in general we use the translation $\langle\Gamma\rangle^L_\alpha$ if Γ is an antecedent, and $\langle\Delta\rangle^R_\alpha$ if Δ is a succedent. Notice that $\langle\Gamma\rangle^L_\alpha = \langle\bigwedge_{\varphi\in\Gamma}\varphi\rangle_\alpha$ and $\langle\Delta\rangle^R_\alpha = \langle\bigvee_{\varphi\in\Delta}\varphi\rangle_\alpha$.

Theorem 33. *Let Π be a $\mathsf{LK}_{\mathscr{R}}$ derivation of the sequent $\Gamma \longrightarrow \Delta$ in which all formulas are in $\Phi_=^{\mathscr{R}}$ and such that all formulas in Γ and Δ have free index-variables $\bar{i}$ and free ring-variables $\bar{x}$. Then there exists $d \in \mathbb{N}$ such that for every assignment α for $\bar{x}$ and $\bar{i}$ there exists a $\mathsf{PC}^{rad}_{\mathscr{R},d}$ derivation*

$$\langle\Gamma\rangle^L_\alpha \vdash \langle\Delta\rangle^R_\alpha.$$

Assuming Theorem 33 we are able to prove Theorem 31, the translation of $\mathsf{TPC}_{\mathscr{R}}$ into $\mathsf{PC}^{\mathrm{rad}}_{\mathscr{R}}$.

Proof of Theorem 31. Let $\varphi(\bar{i})$ be a $\Phi_=^{\mathscr{R}}$ formula with free index variables $\bar{i}$ and no free ring variables. Suppose $\mathsf{TPC}_{\mathscr{R}} \vdash \forall\bar{i}\neg\varphi(\bar{i})$.

By Lemma 32 there is an $\mathsf{LK}_{\mathscr{R}}$-derivation of the sequent $\varphi(\bar{i}) \to \emptyset$. By the two-sorted version of the free-cut elimination theorem (see [11]), we may assume that this derivation contains no free cuts. All formulas in the non-logical axioms and the induction rule of $\mathsf{LK}_{\mathscr{R}}$ are $\Phi_=^{\mathscr{R}}$. Therefore, by the subformula property of free-cut free proofs, every formula in this derivation is $\Phi_=^{\mathscr{R}}$. Hence we can apply Theorem 33 and conclude that there is a $d \in \mathbb{N}$ such that for every tuple $\bar{n} \in \mathbb{N}$, we have a $\mathsf{PC}^{\mathrm{rad}}_{\mathscr{R},d}$ refutation of $\langle\varphi\rangle_{[\bar{i}\mapsto\bar{n}]}$. □

It remains to prove Theorem 33, which is proved by induction on the length of the derivation. The proof is modelled on the translation of a first-order theory into resolution in [8]. The main differences are that we do not need to deal with existential quantifiers, and that we are using multiplication $\cdot$ instead of disjunction $\vee$, so need to use the radical rule to deal with contraction.

We first record a technical lemma about syntax.

Lemma 34. *Let σ be any $\Phi_=^{\mathscr{R}}$ expression in which index variable i does not occur. Then for any assignment α and any $n \in \mathbb{N}$, $\langle\sigma\rangle_\alpha = \langle\sigma\rangle_{\alpha[i\mapsto n]}$. The same is true for ring variables.*

Proof. The only time this is not obviously true is when a variable is *mentioned* in σ but does not *occur* in σ. By Definitions 17 and 18 this can only happen for an index variable i which is the "bound" variable in a big sum symbol $\sum_{t,i}(n)$, expressing $\sum_{i<n} t(i)$. Writing β for $\alpha[i \mapsto n]$, we have

$$\langle\sum_{i<n} t(i)\rangle_\beta = \sum_{j<\langle n\rangle_\beta} \langle t(i)\rangle_{\beta[i\mapsto j]} = \sum_{j<\langle n\rangle_\alpha} \langle t(i)\rangle_{\alpha[i\mapsto j]} = \langle\sum_{i<n} t(i)\rangle_\alpha.$$ □

Proof of Theorem 33. We proceed by induction on the length of the derivation. We divide into cases, depending on the rule by which the final sequent $\Gamma \to \Delta$ was derived.

Logical axioms. These have the form $\varphi \to \varphi$. The translations of the antecedent and succedent are the same, so there is nothing to prove.

Ring axioms and big sum defining scheme. These all have the form $\emptyset \to s = t$, so we need to show that we can derive the equation $\langle s \rangle_\alpha - \langle t \rangle_\alpha = 0$ from no assumptions. But in each case $\langle s \rangle_\alpha \equiv \langle t \rangle_\alpha$, so $\langle s \rangle_\alpha - \langle t \rangle_\alpha = 0$ simplifies to $0 = 0$. For example, consider a substitution instance of the distributivity axiom,

$$\emptyset \to r(s+t) = rs + rt$$

where r, s and t are ring-valued $\mathscr{L}_=^{\mathscr{R}}$-terms. Looking at the definition of the translation, we see that $\langle r(s+t) \rangle_\alpha \equiv \langle rs + rt \rangle_\alpha$.

Integral domain axioms. These have the form

$$st = 0 \to s = 0, t = 0$$

where s and t are ring-valued $\mathscr{L}_=^{\mathscr{R}}$-terms. From the definitions, the translations $\langle st = 0 \rangle_\alpha^L$ and $\langle s = 0, t = 0 \rangle_\alpha^R$ are the same set $\{\langle s \rangle_\alpha \langle t \rangle_\alpha = 0\}$, so there is nothing to prove.

Equality scheme. This contains three forms of axiom,

$$s = s \qquad t = t \qquad \bar{s} = \bar{s}', \bar{t} = \bar{t}' \to f(\bar{s}, \bar{t}) = f(\bar{s}', \bar{t}')$$

for all ring-valued terms $\bar{s}, \bar{s}'$, index-valued terms $\bar{t}, \bar{t}'$ and function symbols f. The first two axioms always translate to $\{0 = 0\}$, in the ring case because the translation is $\{\langle s \rangle_\alpha - \langle s \rangle_\alpha = 0\}$ and in the index case because the equality is true. For the third axiom:

- If f is X, or from F_{ind} or F_{ring}, then no terms $\bar{s}, \bar{s}'$ can appear, and $\bar{t}, \bar{t}'$ do not mention X or ring variables, so are simply evaluated under α. If their evaluations are different then one of the premises becomes $\{1 = 0\}$, so we can derive anything. If their evaluations are the same then the conclusion is $\{0 = 0\}$, for similar reasons to the first two axioms.
- If f is $\cdot$, the axiom is $s_1 = s_1', s_2 = s_2' \longrightarrow s_1 \cdot s_2 = s_1' \cdot s_2'$. We need a derivation

  $$\{\langle s_1 \rangle_\alpha - \langle s_1' \rangle_\alpha = 0,\ \langle s_2 \rangle_\alpha - \langle s_2' \rangle_\alpha = 0\} \vdash \langle s_1 \cdot s_2 \rangle_\alpha - \langle s_1' \cdot s_2' \rangle_\alpha = 0.$$

  This is straightforward: multiply the first assumption by $\langle s_2 \rangle_\alpha$, multiply the second assumption by $\langle s_1' \rangle_\alpha$, and add the results. The functions $+$ and $-$ are similar.
- If f has the form $\sum_{r,i}$, then the axiom is

  $$\bar{s} = \bar{s}', \bar{t} = \bar{t}' \longrightarrow \sum_{i<n} r(\bar{s}, \bar{t}, i) = \sum_{i<n} r(\bar{s}', \bar{t}', i)$$

  where $n \in \mathbb{N}$ is the evaluation of the bounding term under α, which we may assume is the same on both sides, and i does not occur in $\bar{s}, \bar{s}', \bar{t}, \bar{t}'$. By induction on the complexity of r, for some $d \in \mathbb{N}$ for each $j < n$ there is a degree d derivation

  $$\langle \bar{s} = \bar{s}', \bar{t} = \bar{t}' \rangle_\alpha^L \vdash \langle r(\bar{s}, \bar{t}, i) \rangle_{\alpha[i \mapsto j]} - \langle r(\bar{s}', \bar{t}', i) \rangle_{\alpha[i \mapsto j]} = 0.$$

  We do all these derivations and sum the results.

Remaining axioms. These have the form $\emptyset \longrightarrow \sigma$ for a sentence σ which does not mention X or any ring variable and which is true in the standard model. Thus $\langle\sigma\rangle^R_\alpha = \{0 = 0\}$.

Weak structural rules. We do not need exchange rules, as we are treating cedents as multisets. Left exchange and left weakening are trivial. This leaves:

$$\frac{\Gamma \longrightarrow \Delta, \varphi, \varphi}{\Gamma \longrightarrow \Delta, \varphi} \text{ (Right contraction)} \qquad \frac{\Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta, \varphi} \text{ (Right weakening)}$$

Right contraction. By the induction hypothesis for some d there exists a $\mathsf{PC}^{\mathrm{rad}}_{\mathscr{R},d}$ derivation $\langle\Gamma\rangle^L_\alpha \vdash \langle\Delta\rangle^R_\alpha \cdot (\langle\varphi\rangle_\alpha)^2$. By multiplication we derive $(\langle\Delta\rangle^R_\alpha)^2 \cdot (\langle\varphi\rangle_\alpha)^2$, in degree at most $2d$. Finally we apply the radical rule to obtain $\langle\Gamma\rangle^L_\alpha \vdash \langle\Delta\rangle^R_\alpha \cdot \langle\varphi\rangle_\alpha$.

Right weakening. We use a similar multiplication, this time without the radical rule.

Left and right $\wedge$-introduction rules.

$$\frac{\varphi, \Gamma \longrightarrow \Delta}{\varphi \wedge \psi, \Gamma \longrightarrow \Delta} \text{ (Left)} \qquad \frac{\Gamma \longrightarrow \Delta, \varphi \quad \Gamma \longrightarrow \Delta, \psi}{\Gamma \longrightarrow \Delta, \varphi \wedge \psi} \text{ (Right)}$$

Left. Since $\langle\varphi, \Gamma\rangle^L_\alpha \subseteq \langle\varphi \wedge \psi, \Gamma\rangle^L_\alpha$ the derivation of $\langle\varphi, \Gamma\rangle^L_\alpha \vdash \langle\Delta\rangle^R_\alpha$ is already a derivation of $\langle\varphi \wedge \psi, \Gamma\rangle^L_\alpha \vdash \langle\Delta\rangle^R_\alpha$.

Right. We have $\langle\Delta, \varphi \wedge \psi\rangle^R_\alpha = \langle\Delta, \varphi\rangle^R_\alpha \cup \langle\Delta, \psi\rangle^R_\alpha$. Thus the derivation of $\langle\Gamma\rangle^L_\alpha \vdash \langle\Delta, \varphi \wedge \psi\rangle^R_\alpha$ is just the union of the derivations of $\langle\Gamma\rangle^L_\alpha \vdash \langle\Delta, \varphi\rangle^R_\alpha$ and of $\langle\Gamma\rangle^L_\alpha \vdash \langle\Delta, \psi\rangle^R_\alpha$.

Left and right $\vee$-introduction rules.

$$\frac{\varphi, \Gamma \longrightarrow \Delta \qquad \psi, \Gamma \longrightarrow \Delta}{\varphi \vee \psi, \Gamma \longrightarrow \Delta} \text{ (Left)} \qquad \frac{\Gamma \longrightarrow \Delta, \varphi}{\Gamma \longrightarrow \Delta, \varphi \vee \psi} \text{ (Right)}$$

Left. By the induction hypothesis there are derivations

$$\pi_1 : \langle\varphi\rangle_\alpha \cup \langle\Gamma\rangle^L_\alpha \vdash \langle\Delta\rangle^R_\alpha \quad \text{and} \quad \pi_2 : \langle\psi\rangle_\alpha \cup \langle\Gamma\rangle^L_\alpha \vdash \langle\Delta\rangle^R_\alpha.$$

Let us use the notation $\pi_1 \cdot p$ for the derivation formed by multiplying every line of π_1 by the polynomial p, and $\pi_1 \cdot \langle\psi\rangle_\alpha$ for the union $\bigcup_{p \in \langle\psi\rangle_\alpha} \pi_1 \cdot p$. Thus we can form derivations

$$\pi_1 \cdot \langle\psi\rangle_\alpha : \langle\varphi\rangle_\alpha \cdot \langle\psi\rangle_\alpha \cup \langle\Gamma\rangle^L_\alpha \cdot \langle\psi\rangle_\alpha \vdash \langle\Delta\rangle^R_\alpha \cdot \langle\psi\rangle_\alpha$$

$$\text{and} \quad \pi_2 \cdot \langle\Delta\rangle^R_\alpha : \langle\psi\rangle_\alpha \cdot \langle\Delta\rangle^R_\alpha \cup \langle\Gamma\rangle^L_\alpha \cdot \langle\Delta\rangle^R_\alpha \vdash (\langle\Delta\rangle^R_\alpha)^2.$$

Combining these, and observing that it is easy to derive $\langle\Gamma\rangle^L_\alpha \vdash \langle\Gamma\rangle^L_\alpha \cdot \langle\psi\rangle_\alpha$ and $\langle\Gamma\rangle^L_\alpha \vdash \langle\Gamma\rangle^L_\alpha \cdot \langle\Delta\rangle^R_\alpha$, gives a derivation

$$\langle\varphi\rangle_\alpha \cdot \langle\psi\rangle_\alpha \cup \langle\Gamma\rangle^L_\alpha \vdash (\langle\Delta\rangle^R_\alpha)^2$$

and all that remains is to derive $(\langle\Delta\rangle^R_\alpha)^2 \vdash \langle\Delta\rangle^R_\alpha$ by applications of the radical rule.

Right. It is enough to derive $\langle\Delta\rangle^R_\alpha \cdot \langle\varphi\rangle_\alpha \vdash \langle\Delta\rangle^R_\alpha \cdot \langle\varphi\rangle_\alpha \cdot \langle\psi\rangle_\alpha$, which is easy.

Left and right index $\forall$-introduction rules.

$$\frac{\varphi(t), \Gamma \longrightarrow \Delta}{\forall j\, \varphi(j), \Gamma \longrightarrow \Delta} \quad \text{(Left)} \qquad \frac{\Gamma \longrightarrow \Delta, \varphi(i)}{\Gamma \longrightarrow \Delta, \forall j\, \varphi(j)} \quad \text{(Right)}$$

where t is any index term and variable i does not occur in the conclusion of the (Right) rule.

Left. $\langle \varphi(t) \rangle_\alpha$ is a subset of $\langle \forall i\, \varphi(i) \rangle_\alpha$, so the inductive step is trivial.

Right. By the induction hypothesis there exist derivations $\langle \Gamma \rangle^L_{\alpha[i \mapsto n]} \vdash \langle \Delta, \varphi(i) \rangle^R_{\alpha[i \mapsto n]}$ for all assignments α and all $n \in \mathbb{N}$, all in some fixed depth d. Since i does not occur in Γ or Δ, we have $\langle \Delta, \varphi(i) \rangle^R_{\alpha[i \mapsto n]} = \langle \Delta \rangle^R_\alpha \cdot \langle \varphi(i) \rangle_{\alpha[i \mapsto n]}$ and $\langle \Gamma \rangle^L_{\alpha[i \mapsto n]} = \langle \Gamma \rangle^L_\alpha$. Thus for each $n \in \mathbb{N}$ there is a depth d derivation $\langle \Gamma \rangle^L_\alpha \vdash \langle \Delta \rangle^R_\alpha \cdot \langle \varphi(i) \rangle_{\alpha[i \mapsto n]}$. Thus there is a depth d derivation $\langle \Gamma \rangle^L_\alpha \vdash \langle \Delta \rangle^R_\alpha \cdot \bigcup_{n \in \mathbb{N}} \langle \varphi(i) \rangle_{\alpha[i \mapsto n]}$, as required.

Left and right ring $\forall$-introduction rules.

$$\frac{\varphi(t), \Gamma \longrightarrow \Delta}{\forall x\, \varphi(x), \Gamma \longrightarrow \Delta} \quad \text{(Left)} \qquad \frac{\Gamma \longrightarrow \Delta, \varphi(x)}{\Gamma \longrightarrow \Delta, \forall y\, \varphi(y)} \quad \text{(Right)}$$

where t is any ring term and variable x does not occur in Γ or Δ in the (Right) rule.

This case is analogous to the previous one.

Induction rule.

$$\frac{\Gamma, \varphi(i) \longrightarrow \varphi(i+1), \Delta}{\Gamma, \varphi(0) \longrightarrow \varphi(t), \Delta}$$

where t is an index-valued term and the variable i does not occur in Γ or Δ.

Let α be any assignment. By the induction hypothesis for each $n \in \mathbb{N}$ there is a derivation

$$\pi_n : \langle \Gamma \rangle^L_\alpha \cup \langle \varphi(i) \rangle_{\alpha[i \mapsto n]} \vdash \langle \varphi(i+1) \rangle_{\alpha[i \mapsto n]} \cdot \langle \Delta \rangle^R_\alpha$$

(where we are using that i does not appear in Γ or Δ). Notice that, by the definition of the translation, $\langle \varphi(i+1) \rangle_{\alpha[i \mapsto n]} = \langle \varphi(i) \rangle_{\alpha[i \mapsto (n+1)]}$. Thus, multiplying everything by $\langle \Delta \rangle^R_\alpha$ we have

$$\pi_n \cdot \langle \Delta \rangle^R_\alpha : \langle \Gamma \rangle^L_\alpha \cdot \langle \Delta \rangle^R_\alpha \cup \langle \varphi(i) \rangle_{\alpha[i \mapsto n]} \cdot \langle \Delta \rangle^R_\alpha \vdash \langle \varphi(i) \rangle_{\alpha[i \mapsto (n+1)]} \cdot (\langle \Delta \rangle^R_\alpha)^2.$$

Adding an easy derivation $\langle \Gamma \rangle^L_\alpha \vdash \langle \Gamma \rangle^L_\alpha \cdot \langle \Delta \rangle^R_\alpha$ and applying the radical rule gives a derivation

$$\pi'_n : \langle \Gamma \rangle^L_\alpha \cup \langle \varphi(i) \rangle_{\alpha[i \mapsto n]} \cdot \langle \Delta \rangle^R_\alpha \vdash \langle \varphi(i) \rangle_{\alpha[i \mapsto (n+1)]} \cdot \langle \Delta \rangle^R_\alpha.$$

Let $m = \langle t \rangle_\alpha$. Concatenating $\pi'_0, \ldots, \pi'_{m-1}$ gives a derivation

$$\langle \Gamma \rangle^L_\alpha \cup \langle \varphi(i) \rangle_{\alpha[i \mapsto 0]} \cdot \langle \Delta \rangle^R_\alpha \vdash \langle \varphi(i) \rangle_{\alpha[i \mapsto m]} \cdot \langle \Delta \rangle^R_\alpha$$

and now we just need to observe that $\langle \varphi(i) \rangle_{\alpha[i \mapsto 0]} = \langle \varphi(0) \rangle_\alpha$, that $\langle \varphi(i) \rangle_{\alpha[i \mapsto m]} = \langle \varphi(t) \rangle_\alpha$, and that there is an easy derivation $\langle \varphi(0) \rangle_\alpha \vdash \langle \varphi(0) \rangle_\alpha \cdot \langle \Delta \rangle^R_\alpha$.

Cut rule.

$$\frac{\Gamma \longrightarrow \Delta, \varphi \qquad \varphi, \Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta}$$

This is handled like an application of the induction rule with $t = 2$. □

7 Formalizing $\mathsf{PC}^{\mathbf{rad}}_{\mathscr{R}}$ in $\mathsf{TPC}_{\mathscr{R}}$

We claim that everything refutable in $\mathsf{PC}^{\mathrm{rad}}_{\mathscr{R}}$ in constant degree is also refutable in $\mathsf{TPC}_{\mathscr{R}}$, in the sense of the following theorem. The formula φ in the statement should be understood as expressing something about the oracle sequence X, using a size parameter i.

Theorem 35. *Let $\varphi(i)$ be any $\Phi^{\mathscr{R}}_{=}$ formula with no ring quantifiers and with index variable i as its only free variable. Suppose that there is a fixed $d \in \mathbb{N}$ such that every set of equations $\langle\varphi\rangle_{[i\mapsto n]}$ is refutable in $\mathsf{PC}^{rad}_{\mathscr{R}}$ by some refutation π_n of degree d. Then $\mathsf{TPC}_{\mathscr{R}} \vdash \forall i \neg\varphi(i)$.*

This result does not require any assumptions on the uniformity of the refutations π_n because we have included all functions F_{ind} and F_{ring} in our language and all true statements about them (of a certain form) in our theory. In particular, this means that the theory automatically knows everything it needs to know about the sequence of objects $\pi_0, \pi_1, \ldots$.

The theorem essentially states that $\mathsf{TPC}_{\mathscr{R}}$ proves the soundness of constant depth $\mathsf{PC}^{\mathrm{rad}}_{\mathscr{R}}$. The proof is a formalization of the usual proof of soundness. That is, we assume that we have an assignment (given by X) which satisfies every initial equation, and we prove inductively that it satisfies every equation in the refutation, which gives a contradiction when we reach the last equation $1 = 0$. For this we need a formula expressing "equation i is satisfied by X", on which we can do a suitable induction. Writing such a formula is straightforward but technically messy.

Consider a family P of polynomials indexed by $\bar{n} \in \mathbb{N}$, of degree at most $d \in \mathbb{N}$, with the polynomial with index $\bar{n}$ lying in $\mathscr{R}[x_1, \ldots, x_{t(\bar{n})}]$. For brevity, we will refer to such a family P simply as a polynomial. Fix an ordering (such as lexicographical degree order) of all monomials. Let $a_P(i, \bar{n})$ be the function in F_{ring} which outputs the coefficient of the i^{th} monomial in P. In general, for any such polynomials P, Q and elements $\alpha, \beta \in \mathscr{R}$ there are functions $a_{\alpha P + \beta Q}(i, \bar{n})$ and $a_{P \cdot Q}(i, \bar{n})$ in F_{ring} similarly representing the polynomials $\alpha P + \beta Q$ and $P \cdot Q$. The following equalities are axioms of $\mathsf{TPC}_{\mathscr{R}}$, since they are true in the standard model:

- $a_{\alpha P + \beta Q}(i, \bar{n}) = \alpha a_P(i, \bar{n}) + \beta a_Q(i, \bar{n})$
- $a_{P \cdot Q}(i, \bar{n})$
$$= \sum_{j < M_d(\bar{n})} \sum_{k < M_d(\bar{n})} \delta_{\odot(j,k)=i} \cdot a_P(j, \bar{n}) \cdot a_Q(k, \bar{n}).$$

Here $M_d(\bar{n}) \in F_{\mathrm{ind}}$ is a bound on the indices of monomials of degree d in these variables and $\delta_{\odot(j,k)=i} \in F_{\mathrm{ring}}$ is 1 if the i^{th} monomial is the product of j^{th} monomial and k^{th} monomial, and is otherwise 0.

We want to reason about evaluating polynomials under the assignment given by the oracle X. Let $D(i) \in F_{\mathrm{ind}}$ be the degree of monomial m_i and let $v(i, j) \in F_{\mathrm{ind}}$ list the variables in m_i, so that

m_i is the product $\prod_{j=1}^{D(i)} x^{\nu(i,j)}$. To evaluate a monomial m_i of degree d or less under X we define the following term $m_i[X]_d$, which formally has i as its only argument:

$$m_i[X]_d := \prod_{1 \le j \le d} \Big(1 + \delta_{j \le D(i)} \cdot (X(\nu(i,j)) - 1)\Big)$$

Here $\delta_{j \le D(i)} \in F_{\text{ring}}$ is 1 if $j \le D(i)$ and is 0 otherwise, so that the expression in large brackets is, provably in $\mathsf{TPC}_{\mathscr{R}}$, equal to $X(\nu(i,j))$ if if $j \le D(i)$ and equal to 1 otherwise. To evaluate the polynomial P under X, we use the term

$$P[X]_d := \sum_{i < M_d(\bar{n})} a_P(i, \bar{n}) \cdot m_i[X]_d.$$

Now let $\odot(i,j) \in F_{\text{ind}}$ be such that $m_{\odot(i,j)} = m_i \cdot m_j$. Then, for P of degree d or less, the following statements are provable in $\mathsf{TPC}_{\mathscr{R}}$, since they are true in the standard model:

- If $D(i) > d$ then $a_P(i) = 0$
- If $k = \odot(i,j)$ and $D(k) \le d$ then $D(k) = D(i) + D(j)$ and, considered as multisets,

$$\{\nu(k,1), \ldots, \nu(k, D(k))\} = \{\nu(i,1), \ldots, \nu(i, D(i))\} \cup \{\nu(j,1), \ldots, \nu(j, D(j))\}.$$

Thus $\mathsf{TPC}_{\mathscr{R}}$ proves, for $d, e \in \mathbb{N}$, that if $D(i) \le d$ and $D(j) \le e$ then

$$m_i[X]_d \cdot m_j[X]_e = m_{\odot(i,j)}[X]_{d+e}.$$

Lemma 36. *Let P, Q be polynomials of degree respectively $d, e \in \mathbb{N}$. Then $\mathsf{TPC}_{\mathscr{R}}$ proves*

1. *If P and Q have the same coefficients, then $P[X]_d = Q[X]_e$*
2. *$(P+Q)[X]_{\max(d,e)} = P[X]_d + Q[X]_e$*
3. *$(P \cdot Q)[X]_{d+e} = P[X]_d \cdot Q[X]_e$.*

Proof. Items 1. and 2. follow by a simple induction and Lemma 21.

For 3., working in $\mathsf{TPC}_{\mathscr{R}}$ and using the distributivity shown in Lemma 21,

$$\begin{aligned} P[X]_d \cdot Q[X]_e &= \Big(\sum_{i < M_d(\bar{n})} a_P(i,\bar{n}) \cdot m_i[X]_d\Big) \cdot \Big(\sum_{i < M_e(\bar{n})} a_Q(i,\bar{n}) \cdot m_i[X]_e\Big) \\ &= \sum_{i < M_d(\bar{n})} \sum_{j < M_e(\bar{n})} a_P(i,\bar{n}) \cdot a_Q(j,\bar{n}) \cdot m_i[X]_d \cdot m_j[X]_e. \end{aligned}$$

If $D(i) > d$ or $D(j) > e$ then the product $a_P(i,\bar{n}) \cdot a_Q(j,\bar{n})$ is 0. On the other hand if $D(i) \le d$ and $D(j) \le e$ then $m_i[X]_d \cdot m_j[X]_e = m_{\odot(i,j)}[X]_{d+e}$. Thus

$$\begin{aligned} P[X]_d \cdot Q[X]_e &= \sum_{i < M_d(\bar{n})} \sum_{j < M_e(\bar{n})} a_P(i,\bar{n}) \cdot a_Q(j,\bar{n}) \cdot m_{\odot(i,j)}[X]_{d+e} \\ &= \sum_{i < M_d(\bar{n})} \sum_{j < M_e(\bar{n})} a_P(i,\bar{n}) \cdot a_Q(j,\bar{n}) \cdot \sum_{k < M_{d+e}(\bar{n})} \delta_{\odot(i,j)=k}\ m_k[X]_{d+e} \\ &= \sum_{k < M_{d+e}(\bar{n})} m_k[X]_{d+e} \sum_{i < M_d(\bar{n})} \sum_{j < M_e(\bar{n})} a_P(i,\bar{n}) \cdot a_Q(j,\bar{n}) \cdot \delta_{\odot(i,j)=k} \\ &= (P \cdot Q)[X]_{d+e}. \end{aligned}$$

□

We now prove the soundness of $\mathsf{PC}^{\mathrm{rad}}_{\mathscr{R},d}$ in $\mathsf{TPC}_{\mathscr{R}}$. To avoid some technical complications, we consider a slightly more limited form of soundness than usually appears in the proof complexity literature. Typically a soundness or reflection principle says that you cannot simultaneously have a formula, a refutation of it, and a satisfying assignment of it, and all three things are encoded as oracles (in the first-order setting) or as propositional variables (in the propositional setting); see for example [3] and [14, Chap. 10] for a systematic treatment of reflection principles. In contrast we only show the soundness of formulas and refutations that are definable in our language.

In particular, for us soundness is a "scheme", rather than a single sentence. For each definable family of formulas and and each definable family of refutations, we show that if the refutations refute the formulas (with correct syntax), then the oracle cannot encode a satisfying assignment for the formulas. This is enough for our purposes, because we deliberately made our language rich enough to define every family of formulas and refutations that exists in the standard world.

Theorem 37. *Fix $d \in \mathbb{N}$. Let $n(m), s(m), t(m) \in F_{\mathrm{ind}}$. For $m \in \mathbb{N}$, let $\mathscr{S}_m := (\mathscr{S}_{m,0}, \ldots, \mathscr{S}_{m,s(m)})$ and $\pi_m = (\pi_{m,0}, \ldots, \pi_{m,t(m)})$ be sequences of degree d equations in $x_1, \ldots, x_{n(m)}$. The equations are described by functions $a_{\mathscr{S}}(m,i,j), a_{\pi}(m,i,j) \in F_{\mathrm{ring}}$ where $a_{\mathscr{S}}(m,i,j)$ is the coefficient of the j^{th} monomial in $\mathscr{S}(m,i)$, and similarly for a_π and π.*

Suppose that, for each m, π_m is a $\mathsf{PC}^{rad}_{\mathscr{R}}$ refutation of $\mathscr{S}_m$. Then $\mathsf{TPC}_{\mathscr{R}}$ proves that, for every m, there is $i \le s(m)$ such that $\mathscr{S}_{m,i}$ is not satisfied by X.

Proof. There are functions in F_{ind} describing the structure of the refutation π_m, that is, which rule or axiom each line was derived from, which two lines were used as assumptions in applications of the addition rule, etc. We may assume that every syntactic property of the refutation that we want to use is provable in $\mathsf{TPC}_{\mathscr{R}}$, since in particular none of these properties mentions the symbol X. To save notation we will treat $\mathscr{S}_{m,i}$ and $\pi_{m,i}$ as names of polynomials, rather than of equations.

Working in $\mathsf{TPC}_{\mathscr{R}}$, fix m and suppose that $\mathscr{S}_{m,i}[X]_d = 0$ for every $i \le s$. We will derive a contradiction by induction on k in the formula $\forall i < k, \pi_{m,i}[X]_d = 0$. For $k = 0$ there is nothing to prove. If $\pi_{m,i}$ is an axiom from $\mathscr{S}_m$, we use Lemma 36 part 1. If $\pi_{m,i}$ was derived by the addition rule from $\pi_{m,i'}$ and $\pi_{m,i''}$ then we use Lemma 36 part 2. If $\pi_{m,i}$ was derived by multiplying $\pi_{m,i'}$ by x_j, then $\pi_{m,i'}[X]_d = 0$ by the inductive hypothesis, so by Lemma 36 part 3., $\pi_{m,i}[X]_d = 0$, regardless of the evaluation of x_j. The radical rule is similar, but in this case we also need the integral domain axiom.

Thus from the last line of the refutation we conclude that the constant polynomial 1 evaluates to 0, which is impossible. □

Proof of Theorem 35. Let $\mathscr{S}_m$ be the set of equations $\langle \varphi(i) \rangle_{[i \mapsto m]}$. Suppose that every set $\mathscr{S}_m$ is refutable in $\mathsf{PC}^{\mathrm{rad}}_{\mathscr{R},d}$ by some refutation π_m. Working in $\mathsf{TPC}_{\mathscr{R}}$, fix m. Suppose for a contradiction that $\varphi(m)$ is true. We must show that every equation in $\langle \varphi(i) \rangle_{[i \mapsto m]}$ is satisfied by X, and we do this by proving, in $\mathsf{TPC}_{\mathscr{R}}$, the properties of the translation of the language. This is routine, but we go through the details.

We first deal with terms. For each ring-valued term $t(\bar{i}, \bar{y})$ there is a function $a_{\langle t \rangle}(\bar{i}, \bar{y}, j) \in F_{\mathrm{ring}}$ computing the coefficient of monomial M_j in the polynomial $\langle t(\bar{i}', \bar{y}') \rangle_{[\bar{i}', \bar{y}' \mapsto \bar{i}, \bar{y}]}$. To save on notation, we will simply write $\langle t(\bar{i}, \bar{y}) \rangle$ to mean this polynomial. We will prove in $\mathsf{TPC}_{\mathscr{R}}$ that $t(\bar{i}, \bar{y}) = \langle t(\bar{i}, \bar{y}) \rangle [X]_d$, where d is the degree of $\langle t(\bar{i}, \bar{y}) \rangle$.

Suppose t is a term $X(f(\bar{i}))$ for $f \in F_{\mathrm{ind}}$. Then $\mathsf{TPC}_{\mathscr{R}}$ proves that $a_{\langle t \rangle}(\bar{i}, j)$ is 1 for j such that M_j is the monomial $X_{f(\bar{i})}$, and is 0 otherwise, since this is true in the standard model. Thus $\mathsf{TPC}_{\mathscr{R}}$ proves $t(\bar{i}) = \langle t(\bar{i}) \rangle [X]_1$.

If t is $f(\bar{i})$ for $f \in F_{\text{ring}}$, then $\langle t(\bar{i})\rangle$ is the constant polynomial $f(\bar{i})$, and this is provable in $\mathsf{TPC}_{\mathscr{R}}$ as it is true in the standard model. It evaluates to $f(\bar{i})$.

Suppose t has the form $r \cdot s$, where the terms may have index and ring parameters. Then $\langle t\rangle \equiv \langle r\rangle \cdot \langle s\rangle$ and this, stated as a property of their coefficients, is provable in $\mathsf{TPC}_{\mathscr{R}}$. Hence $\mathsf{TPC}_{\mathscr{R}}$ proves $\langle t\rangle[X]_{d+e} = \langle r\rangle[X]_d \cdot \langle s\rangle[X]_e$ by Lemma 36, where d, e and $d+e$ are respectively the degrees of $\langle r\rangle$, $\langle s\rangle$ and $\langle t\rangle$. Addition is handled similarly.

Finally suppose t has the from $\sum_{k<n} s(k)$. Then, working with the coefficients of M_j as above, $\mathsf{TPC}_{\mathscr{R}}$ proves that $a_{\langle t\rangle}(j) = \sum_{k<n} a_{\langle s\rangle}(k,j)$ and hence that

$$\langle t\rangle[X]_d = \sum_{k<n} \langle s(k)\rangle[X]_d = \sum_{k<n} s(k) = t$$

where the first equality comes from applying Lemma 21 to the sum of monomials.

Now we will show, by induction on the complexity of φ, that for each $\Phi^{\mathscr{R}}_{=}$ formula $\varphi(\bar{i},\bar{y})$ with the free variables shown, $\mathsf{TPC}_{\mathscr{R}}$ proves that $\varphi(\bar{i},\bar{y})$ is true if and only if every equation in $\langle\varphi(\bar{i},\bar{y})\rangle$ is satisfied by X (we are still using the simplified notation for translations). For the purposes of this formalization, a set of polynomials means a set of the form $\{\sum_j M_j \cdot a(\bar{i},\bar{y},j) : \bar{i} \in \mathbb{N}, \bar{y} \in \mathscr{R}\}$ for some $a \in F_{\text{ring}}$ which may have more parameters, where M_j is the j^{th} polynomial. We can handle finite sets by having the coefficients be 0 for all but finitely many tuples $(\bar{i},\bar{y})$.

Suppose $\varphi(\bar{i},\bar{y})$ is an atomic formula $t(\bar{i},\bar{y}) = 0$, for a ring-valued term t with the parameters shown. Then its translation is the singleton set $\{\langle t(\bar{i},\bar{y})\rangle = 0\}$. Let d be the degree of $\langle t(\bar{i},\bar{y})\rangle$. We have shown above that, provably in $\mathsf{TPC}_{\mathscr{R}}$, $t(\bar{i},\bar{y}) = 0$ if and only if $\langle t(\bar{i},\bar{y})\rangle[X]_d = 0$.

Suppose φ is a disjunction $\psi \vee \chi$. If ψ and χ are both false, then there is are equations $p = 0 \in \langle\psi\rangle$ and $q = 0 \in \langle\chi\rangle$ such that $p[X]_d \neq 0$ and $q[X]_e \neq 0$, where d and e are the degree bounds on respectively $\langle\psi\rangle$ and $\langle\chi\rangle$. Hence by Lemma 36 and the integral domain axioms $(p \cdot q)[X]_{d+e} \neq 0$. The other direction is similar.

The cases of conjunction and universal quantifiers are straightforward.

Now, starting from the assumption that $\varphi(m)$ is true, we know that every equation in the set $\langle\varphi(i)\rangle_{[i\mapsto m]}$ (which may be infinite) is satisfied by X. We are also given a derivation of $1 = 0$ from $\langle\varphi(i)\rangle_{[i\mapsto m]}$. This derivation necessarily only uses finitely many equations from $\langle\varphi(i)\rangle_{[i\mapsto m]}$, and these equations can be pointed to by some function of m in F_{ind}, since $\varphi(i)$ does not contain any ring quantifiers (otherwise the set $\langle\varphi(i)\rangle_{[i\mapsto m]}$ could be defined by the parameters ranging over ring elements). Hence we get a contradiction using Theorem 37. □

8 Translations to and from constant degree SoS

Recall that the theory TSoS is in the same language as $\mathsf{TPC}_{\mathbb{R}}$ – in particular, we do not add any ordering symbol for the ring sort. TSoS extends $\mathsf{TPC}_{\mathbb{R}}$ by adding the Boolean axiom and the sum-of-squares axiom scheme defined in Section 3, which expresses that if a sum of squares is 0, then every square in the sum is 0. We emphasize that this axiom applies to "big sums", not just finite sums of fixed size.

We will show the same connection between TSoS and constant degree SoS + Bool as we showed between $\mathsf{TPC}_{\mathscr{R}}$ and $\mathsf{PC}^{\text{rad}}_{\mathscr{R}}$.

Theorem 38. *Let $\varphi(i)$ be any $\Phi^{\mathscr{R}}_{=}$ formula with no ring quantifiers and with index variable i as its only free variable. Define $\mathscr{S}_n$ to be the set of equations $\langle\varphi\rangle_{[i\mapsto n]}$. Then every set $\mathscr{S}_n$ is refutable in* SoS + Bool *in some fixed constant degree if and only if* $\mathsf{TSoS} \vdash \forall i \neg\varphi(i)$.

Proof. Suppose $\mathsf{TSoS} \vdash \forall i \neg \varphi(i)$. We extend the proof of Theorem 31 to deal with the the sum-of-squares scheme and the Boolean axiom. For the sum-of-squares scheme, we extend the sequent calculus $\mathsf{LK}_{\mathbb{R}}$ by adding the sequents

$$\sum_{i<r} t(i)^2 = 0, s < r \longrightarrow t(s) = 0$$

as axioms, for all ring-valued terms t and index-valued terms r, s, where all these terms may have other parameters. We must then show that, given such an axiom, there is $d \in \mathbb{N}$ such that for every assignment α there is a depth d SoS derivation of $\langle \sum_{i<r} t(i)^2 = 0 \rangle_\alpha \cup \langle s < r \rangle_\alpha \vdash \langle t(s) = 0 \rangle_\alpha$. If $\langle s \rangle_\alpha \geq \langle r \rangle_\alpha$ in the standard model, then $\langle s < r \rangle_\alpha$ is $\{1 = 0\}$ and the derivation is trivial. Otherwise, working through the translations, we need derivations $\sum_{i<n} \langle t(i) \rangle_\alpha^2 = 0 \vdash \langle t(m) \rangle_\alpha = 0$ for some $m < n \in \mathbb{N}$, which can be done using the sum-of-squares rule and the radical rule. For the Boolean axiom, we further extend $\mathsf{LK}_{\mathbb{R}}$ by adding the sequent

$$\emptyset \longrightarrow X(r)(1 - X(r)) = 0$$

for every index-valued term r. This straightforwardly translates into a propositional Boolean axiom.

For the other direction, we need to extend the corresponding proof of PC soundness in the theory by showing that TSoS can prove the soundness of the sum-of-squares rule and the propositional Boolean axioms. This is straightforward. □

9 Theories that reason directly about inequalities

We have developed a first-order theory, TSoS, with the property that the sentences about X (of a suitable form) which are refutable in TSoS are precisely the principles that are refutable in constant depth SoS. This gives us a new way of constructing TSoS refutations. But this theory has the disadvantage of being somewhat unnatural, as intuitively a natural theory for SoS would allow us to reason directly about inequalities on the ring sort. This is something TSoS obviously cannot do, as it does not even have an inequality symbol in its language. Instead we have to reason explicitly about sums of squares, as was illustrated by the proof of the functional pigeonhole principle in Section 4.2, and in this sense we have not gained much from working in SoS.

In this section we sketch some approaches for getting a more “usable" theory than TSoS. Our goal is to construct a theory T which extends TSoS but has a richer language with in particular some kind of ring-inequality symbol $\leq$ which allows us to talk explicitly about inequalities between ring terms. We should be able to reason robustly about inequalities, meaning that there should be natural ordering axioms for $\leq$ and we should be able to do induction on formulas nontrivially involving $\leq$. The expanded theory T should preserve the property of TSoS that every sentence refutable in T (of a suitable form) translates into a principle with constant degree $\mathsf{SoS} + \mathsf{Bool}$ refutations.

We do not take this approach here, but a natural way to achieve this would be for T to be conservative over TSoS, that is, for every relevant sentence in the language of TSoS that is provable in T to be already provable in TSoS. A suggestive model is the Artin-Schreier Theorem, which in particular shows that a formally real field (that is, one in which -1 is not a sum of squares) can be ordered; but the presence of big sums and the oracle X are obstacles to adapting this to our theories.

9.1 $\mathsf{TSoS}_{\geq}$ - unrestricted use of ordering

We first consider what happens if we introduce ordering in a naive way. We define a language $\mathscr{L}_{\geq}$ by taking $\mathscr{L}_{=}^{\mathbb{R}}$ and adding a binary relation symbol $\geq$ for an partial order on the ring sort. We define $\Phi_{\geq}$ in the same was as $\Phi_{=}^{\mathbb{R}}$ except that we also allow the $\geq$ symbol in all places that $\Phi_{=}^{\mathbb{R}}$ allows the ring equality symbol $=_{\text{ring}}$. In particular, formulas made from atomic formulas of the form $s \geq t$, for ring terms s, t, and closed under $\wedge$, $\vee$ and $\forall$ are $\Phi_{\geq}$ formulas.

The theory $\mathsf{TSoS}_{\geq}$ is TSoS with the addition of

- Axioms for a partially ordered ring, namely
  - i. $\geq$ is a partial order
  - ii. $x \geq y \supset x + z \geq y + z$
  - iii. $x \geq 0 \wedge y \geq 0 \supset x \cdot y \geq 0$
  - iv. $x^2 \geq 0$
- *Background truth* axioms in the new language, that is, every sentence which does not mention the oracle symbol X or any ring variable and which is true in the standard model
- Induction for every formula $\varphi(i)$ in $\Phi_{\geq}$ (with other parameters allowed).

The next proposition shows that $\mathsf{TSoS}_{\geq}$ is too strong, because it proves the soundness of resolution. Since resolution is complete (and we do not care about proof size) this means that it proves that every unsatisfiable set of clauses is not satisfied by X. In particular, this means that if $\mathscr{S}$ is any constant-degree set of polynomial equations that are unsatisfiable over 0/1 assignments, then $\mathsf{TSoS}_{\geq}$ proves that $\mathscr{S}$ is not satisfied by X. Hence if a version of our translation theorem for TSoS, Theorem 38, held for $\mathsf{TSoS}_{\geq}$, it would imply that $\mathscr{S}$ has a constant-degree refutation in $\mathsf{SoS} + \mathsf{Bool}$, which is not in general true.

This theory seems rather to correspond to the fully dynamic version of constant-degree SoS, which is a very strong system. For example, the (complete) Lovasz-Schrijver proof system is the degree 2 fragment of it [18].

Proposition 39. *Let $C_1, \ldots, C_m$ be a sequence of clauses in variables $x_1, \ldots, x_n$ which are refutable in resolution (we assume that the structure of these clauses, and of the resolution refutation, is naturally described by functions in F_{ind} which take n as a parameter). Then* TSoS *refutes the statement that all clauses $C_1, \ldots, C_m$ are satisfied by the assignment given by X.*

Proof. Suppose the resolution refutation is a sequence of clauses $C_1, \ldots, C_t$. Using functions available in F_{ind}, we can construct a ring-valued term

$$\gamma(i) := \sum_{x_j \in C_i} X(j) + \sum_{\bar{x}_j \in C_i} (1 - X(j))$$

where the first sum is for variables appearing positively in C_i and the second is for variables appearing negatively.

By the integral domain and Boolean axioms, for each j we have $X(j) \geq 0$ and $1 - X(j) \geq 0$. Let C_j be an initial clause. From the assumption, $X(i) = 1$ for some variable x_i appearing positively in C_j (or we argue similarly if it is a negative literal that is satisfied). Using induction and the ordering axioms, we can conclude that $\gamma(j) \geq 1$.

Now we do induction on k the formula $\varphi(k) := \forall i \leq k\,(\gamma(i) \geq 1)$. This formula is $\Phi_{\geq}$, as we can handle bounded index quantifiers the same way as we did in Section 4.1. The formula is true for all $k \leq m$, as already shown. The inductive step comes down to showing that $\varphi(k)$ implies $\gamma(k+1) \geq 1$, and this can be shown by arguing by cases on the value of $X(j)$, where x_j is the variable resolved on to derive C_{k+1}, just as in the usual proof of the soundness of resolution. From $\varphi(t)$ we conclude that $\gamma(t) \geq 1$, and thus that $0 \geq 1$ since C_t is empty. This is a contradiction, since $1 \geq 0$ and $1 \neq 0$. □

9.2 Other theories

In this section we discuss some ongoing work on how to weaken a theory like $\mathsf{TSoS}_{\geq}$ described above, into something which (a) still allows robust reasoning about orderings; (b) still proves the soundness of SoS; but (c) admits a translation into constant degree SoS, similar to Theorem 38.

A first observation is that the integral domain axiom plays a big role in the proof of Proposition 39, but we do not seem to need it for task (b). In particular if we replace it with the *radical axiom* $x^2 = 0 \supset x = 0$ we still seem to be able to do the important parts of the soundness proof in Section 7. Furthermore the integral domain axiom is the only place in which a disjunction explicitly appears in our sequent calculus (it is implicitly allowed in $\Phi_{=}^{\mathbb{R}}$ formulas) and removing nontrivial disjunctions makes the theory more constructive, which is useful for task (c). However the theory still seems to be too strong with just this change, since it is possible to prove Proposition 39 in a constructive way, replacing the argument by cases in the inductive step with an algebraic manipulation.

Another, extreme change is to replace the single ordering symbol $\geq$ with a family $\{\geq_d : d \in \mathbb{N}\}$ of symbols, each one labelled with a degree d. The intuitive meaning of $s \geq_d t$ is that $s - t$ is a sum of squares of degree d or less, and we take axioms reflecting this:

i. $\geq_d$ is a partial order and $x \geq_d y \supset x \geq_e y$ for each $e > d$

ii. $x \geq_d y \supset x + z \geq_d y + z$

iii. $x \geq_d 0 \wedge y \geq_d 0 \supset x \cdot y \geq_{d+e} 0$

iv. $t^2 \geq_{2d} 0$ for terms t of degree d.

Our general approach to task (c) is to be able to translate inequalities $s \leq_d t$ in the first-order proof as equations $\langle s \rangle - \langle t \rangle - U = 0$, where the polynomial U is an explicit sum of squares, constructed from the proof. The index d tells us that we should be able to do this with U of degree d – in particular we never need degree higher than the maximum d appearing in this way in the first-order proof. The disadvantage is that this is not at all a natural way to think about orderings; and also the (non-constructive) proof of Proposition 39 still goes through if we replace $\geq$ there with $\geq_2$.

We can also limit how orderings can appear in induction formulas, for example, adding a constraint that in an induction formula, in any subformula of the form $\varphi \vee \psi$ at most one of φ and ψ can contain an inequality (in fact we may need the stronger condition that at most one of φ and ψ can mention ring variables or the oracle X).

We believe that weakening $\mathsf{TSoS}_{\geq}$ along these lines gives a theory with (b) and (c) (that is, with the strength of constant-degree SoS). Furthermore there is a promising approach to get closer to (a) (robust reasoning about inequalities), which is to only allowing reasoning in intuitionistic, rather than classical, logic. Briefly, this is helpful because our basic problem is how to witness inequalities with explicit sums of squares, and more constructive first-order proofs make this easier. We expect

that moving to a fully intuitionistic setting would allow induction for a more robust class of formulas, involving the $\supset$ and $\neg$ connectives (but so far still requiring the "levelled" orderings $\geq_d$).

Let us call this formula-class $\Phi^{(i)}_{\geq}$ and the theory $\mathsf{TSoS}^{(i)}_{\geq}$. The translations of $\Phi^{(i)}_{\geq}$ formulas and $\mathsf{TSoS}^{(i)}_{\geq}$ proofs substantially differ from the translations we dealt with in the classical case. These translations are done according to the Brouwer-Heyting-Kolmogorov interpretation of intuitionistic logic [37] and can be described informally as follows. The translation $\langle\varphi\rangle_\alpha(\omega)$ of a formula is parameterized by what we call a *realizing function* ω. The translation theorem for $\mathsf{TSoS}^{(i)}_{\geq}$ proofs then says that, for example, if there is a $\mathsf{TSoS}^{(i)}_{\geq}$ proof of $\varphi_1 \supset \varphi_2$, where φ_1, φ_2 are $\Phi^{(i)}_{\geq}$ formulas not containing $\supset$, then for every α and ω_1 there exists ω_2 and a constant degree PC^+ derivation of $\langle\varphi_2\rangle_\alpha(\omega_2)$ from $\langle\varphi_1\rangle_\alpha(\omega_1)$. It gets a more complicated with nested $\supset$ symbols: for example, in case $(\varphi_1 \supset \varphi_2) \supset (\varphi_3 \supset \varphi_4)$. We believe that a certain generalization of PC^+ derivations would work for this, however the detailed exposition of this is technical and is beyond the scope of this paper.

Acknowledgments The authors would like to thank Leszek Kołodziejczyk for helpful discussions during the preliminary stages of this work.

References

[1] Yaroslav Alekseev. A lower bound for polynomial calculus with extension rule. Technical report, 2020. arXiv:2010.05660. 2

[2] Robert Ash. *Basic Abstract Algebra: For Graduate Students and Advanced Undergraduates*. Dover Books on Mathematics, 2006. 2.1, 6

[3] Albert Atserias and Maria Luisa Bonet. On the automatizability of resolution and related propositional proof systems. *Information and Computation*, 189:182–201, 2004. 7

[4] Boaz Barak. Sum of squares upper bounds, lower bounds, and open questions. Lecture notes, 2014. 1, 1

[5] 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 *STOC*, pages 307–326, 2012. 1, 2.2

[6] Paul Beame, Russell Impagliazzo, Jan Krajíček, Toniann Pitassi, and Pavel Pudlák. Lower bounds on Hilbert's Nullstellensatz and propositional proofs. *Proc. London Math. Soc. (3)*, 73(1):1–26, 1996. 1.1.1, 2.1

[7] Eberhard Becker and Joachim Schmid. On the real Nullstellensatz. In B. Heinrich Matzat, Gert-Martin Greuel, and Gerhard Hiss, editors, *Algorithmic Algebra and Number Theory*, pages 173–185, Berlin, Heidelberg, 1999. Springer Berlin Heidelberg. 2.1

[8] Arnold Beckmann, Pavel Pudlák, and Neil Thapen. Parity games and propositional proofs. *ACM Transactions on Computational Logic*. 1, 1.2, 6.2

[9] 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. 1.1.1, 2.3

[10] Samuel R. Buss. *Bounded Arithmetic*, volume 3 of *Studies in Proof Theory*. Bibliopolis, 1986. 1

[11] Samuel R. Buss. An introduction to proof theory. In *Handbook of proof theory*, volume 137 of *Stud. Logic Found. Math.*, pages 1–78. North-Holland, Amsterdam, 1998. 6.1, 6.2

[12] Samuel R. Buss, Leszek Aleksander Kolodziejczyk, and Konrad Zdanowski. Collapsing modular counting in bounded arithmetic and constant depth propositional proofs. *Transactions of the AMS*, (367):7517–7563, 2015. 1, 1.2

[13] Matthew Clegg, Jeffery Edmonds, and Russell Impagliazzo. Using the Groebner basis algorithm to find proofs of unsatisfiability. In *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing (Philadelphia, PA, 1996)*, pages 174–183, New York, 1996. ACM. 1

[14] Stephen Cook and Phuong Nguyen. *Logical Foundations of Proof Complexity*. ASL Perspectives in Logic. Cambridge University Press, 2010. 1, 7

[15] Noah Fleming, Pravesh Kothari, and Toniann Pitassi. Semialgebraic proofs and efficient algorithm design. *Found. Trends Theor. Comput. Sci.*, 14(1-2):1–221, 2019. 1

[16] Dima Grigoriev. Complexity of Positivstellensatz proofs for the knapsack. *Comput. Complexity*, 10(2):139–154, 2001. 1.1.3

[17] Dima Grigoriev and Edward A. Hirsch. Algebraic proof systems over formulas. *Theoret. Comput. Sci.*, 303(1):83–102, 2003. Logic and complexity in computer science (Créteil, 2001). 2, 2.1

[18] Dima Grigoriev, Edward A. Hirsch, and Dmitrii V. Pasechnik. Complexity of semialgebraic proofs. *Mosc. Math. J.*, 2(4):647–679, 805, 2002. 1, 9.1

[19] Dima Grigoriev and Nicolai Vorobjov. Complexity of Null- and Positivstellensatz proofs. *Ann. Pure Appl. Logic*, 113(1-3):153–160, 2002. 1

[20] Dima Grigoriev and Nicolai Vorobjov. Complexity of Null- and Positivstellensatz proofs. *Ann. Pure Appl. Logic*, 113(1-3):153–160, 2002. First St. Petersburg Conference on Days of Logic and Computability (1999). 2.2

[21] Petr Hájek and Pavel Pudlák. *Metamathematics of First-order Arithmetic*. Perspectives in Mathematical Logic. Springer-Verlag, Berlin, 1993. 1

[22] Russell Impagliazzo, Pavel Pudlák, and Jiří Sgall. Lower bounds for the polynomial calculus and the gröbner basis algorithm. *Computational Complexity*, 8(2):127–144, 1999. 1.1.3, 2.3, 3

[23] Jan Krajíček. Lower bounds to the size of constant-depth propositional proofs. *The Journal of Symbolic Logic*, 59(1):73–86, 1994. 1.2

[24] Jan Krajíček. *Bounded arithmetic, propositional logic, and complexity theory*, volume 60 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1995. 1

[25] 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. 1.2

[26] Jan Krajíček. On the weak pigeonhole principle. *Fund. Math.*, 170(1-2):123–140, 2001. 1.2

[27] László Lovász. Stable sets and polynomials. *Discrete Mathematics*, 124:137–153, 1994. 1

[28] László Lovász and Alexander Schrijver. Cones of matrices and set-functions and 0–1 optimization. *SIAM Journal on Optimization*, 1:166–190, 1991. 1

[29] Sebastian Müller and Iddo Tzameret. Short propositional refutations for dense random 3CNF formulas. *Annals of Pure and Applied Logic*, 165:1864–1918, 2014. Extended abstract in Proceedings of the 27th Annual ACM-IEEE Symposium on Logic In Computer Science (LICS), 2012. 1.2

[30] Ryan O'Donnell. SOS is not obviously automatizable, even approximately. *Electron. Colloquium Comput. Complex.*, 23:141, 2016. 1

[31] 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. 1

[32] Jeff Paris and Alex Wilkie. Counting problems in bounded arithmetic. In *Methods in mathematical logic (Caracas, 1983)*, volume 1130 of *Lecture Notes in Math.*, pages 317–340. Springer, Berlin, 1985. 1, 1.2

[33] Fedor Part, Neil Thapen, and Iddo Tzameret. First-order reasoning and efficient semi-algebraic proofs. In *Proceedings of the 36th Annual ACM/IEEE Symposium on Logic In Computer Science (LICS) (to appear)*, 2021.

[34] Pavel Pudlák. On the complexity of the propositional calculus. In *Sets and proofs (Leeds, 1997)*, volume 258 of *London Math. Soc. Lecture Note Ser.*, pages 197–218. Cambridge Univ. Press, Cambridge, 1999. 1

[35] Michael Soltys and Stephen Cook. The proof complexity of linear algebra. *Ann. Pure Appl. Logic*, 130(1-3):277–323, 2004. 1, 1.2

[36] Neil Thapen and Michael Soltys. Weak theories of linear algebra. *Arch. Math. Log.*, 44(2):195–208, 2005. 1, 1.2

[37] Anne Sjerp Troelstra and Dirk van Dalen. *Constructivism in Mathematics, An Introduction*. Studies in Logic and the Foundation of Mathematics 121. North-Holland, 1988. 9.2