First-Order Reasoning and Efficient Semi-Algebraic Proofs

Fedor Part
a) JetBrains Research
b) Institute of Mathematics
Czech Academy of Sciences
Czech Republic
Email: fedor.part@gmail.com

Neil Thapen
Institute of Mathematics
Czech Academy of Sciences
Czech Republic
Email: thapen@math.cas.cz

Iddo Tzameret
Department of Computing
Imperial College London
United Kingdom
Email: iddo.tzameret@gmail.com

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 [3]: constant degree semi-algebraic proofs lead to conjecturally optimal polynomial-time approximation algorithms for important NP-hard optimization problems (cf. [4]). 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 [7] dynamic-by-static simulation of polynomial calculus (PC) by SoS to PC with the radical rule.

I. 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 [11] 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 attracted a lot of attention in recent years. Semi-algebraic proofs have been brought to the attention of complexity theory from optimization [26], [25]; by the works of Pudlák [31] and Grigoriev and Vorobjov [17] (cf. [16]); and more recently through their connection to approximation algorithms with the work of Barak et al. [3] (see for example [29] and the excellent survey by Fleming, Kothari and Pitassi [13]).

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 (SDP), 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 [28]).

Due to its importance in algorithms design and approximation theory, bootstrapping SoS, namely the act of providing efficient low-degree SoS proofs of basic facts (see for example [29]) 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 [2]: “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. [8], [19], [22], [12]). On the one hand, bounded arithmetic constitutes the “proof-theoretic approach” to computational complexity in terms of developing the metamathematics 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:

\(^1\) A consequence of this is “Marley’s Corollary” on analyzing the performance of SoS algorithms [2].
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 [30]. Our translations are inspired in particular by Beckmann, Pudlák and Thapen [6]. Our theories on the other hand are inspired to a certain extent by works of Soltys and Cook [32] and Thapen and Soltys [33] 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 [10]. 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.

A. 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. For reasons of space most proofs, and some other technical parts, have been omitted. For more details please see the upcoming full version.

1) Propositional proofs: In Section II 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 measured, for example, by the number of monomials). In particular we introduce two natural extensions of the polynomial calculus (PC), as follows.

Let $PC_R$ be the polynomial calculus over the ring $R$. We introduce the system $PC_R^{rad}$ which is $PC_R$ plus the radial 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 $\sqrt{\langle J \rangle} = \{ q : q^k \in \langle J \rangle \}$ 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 6, 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 $PC_R^{rad+}$ which is $PC_R$ plus the radical rule and the sum-of-squares rule: from $p^2 + \sum q_i^2 = 0$ derive $p^2 = 0$, for $p,q$ polynomials. We define $PC^+_R$ to be $PC_R^{rad+}$ (that is, over the reals).

Recall that a proof system is implicationally complete if, whenever a set of equations $F$ implies an equation $q = 0$, there is a derivation $F \vdash q = 0$ in the system. It is known that $PC_R$ is implicationally complete in the presence of the Boolean axioms [5, Theorem 5.2], while in general it is not implicationally complete without them. We show that, in contrast, $PC_R^{rad}$ is implicationally complete if $R$ is an algebraically closed field, and $PC^+_R$ is implicationally complete (over the reals).

In Propositions 11 and 12 we show that whether the radical rule provides more strength to PC depends on the underlying ring. Finally, we extend a result by Berkholtz [7], and show that the static system SoS and the dynamic system $PC_R^{rad+}$ simulate each other (with respect to degree):

**Theorem** (Theorem 14 and proposition 13; informal). In the presence of the Boolean axioms, SoS and $PC^+_R$ simulate each other (with respect to degree).

2) The first-order theories: In Section III we define the first-order, algebraic theories $TPC_R$ 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 $R$ be an integral domain. $TPC_R$ is a two-sorted theory in the language $\mathcal{L}_R^\mathbb{N}$ 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 $i$th 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 $TPC_R$ 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 also occur, the axiom $\sum_{i \leq n} t(i)^2 = 0 \land j < n \supset t(j) = 0$. For technical reasons, we also add first-order Boolean axioms.

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

3) Propositional translations: In Section V we start to describe our translation, by showing how to translate formulas in our first-order language into families of polynomial equations. In Section VI we show how first-order $TPC_R$ proofs can be translated into constant-degree $PC_R^{rad+}$ refutations:

**Theorem** (Theorem 29; informal). Let $\varphi(i)$ be a certain “well-behaved” formula with free index variables $i$ and no free ring variables. Suppose $TPC_R \vdash \forall i \varphi(i)$. Then there is a constant degree $PC_R^{rad+}$ refutation of the propositional translation of $\varphi$.  

\(^2\) Grigoriev and Hirsch [15] were the first to consider the radial rule, to the best of our knowledge, although in [15] 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.
The proof is by first translating TPC$_R$ proofs into a Gentzen-style sequent calculus LK$_R$ and then translating LK$_R$ into PC$_R^{rad}$ rule-by-rule.

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

In Section VIII 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 SoS + Bool), and vice versa:

**Theorem** (Theorem 33; 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 $S_n$ to be the propositional translation of $\varphi$ (parametrized by $n$). Then $S_n$ is refutable in SoS + Bool in some fixed constant degree if and only if TSoS $\vdash \forall i \neg \varphi(i)$.

As a corollary of the propositional translation results we can conclude that TSoS is not conservative over TPC$_R$, even if we add first-order Boolean axioms to TPC$_R$, using the separation between SoS + Bool and PC + Bool (that is, PC with Boolean axioms) demonstrated, for example, by Grigoriev [14], who showed that algebraic proofs like PC + Bool cannot simulate semi-algebraic proofs like SoS + Bool, because symmetric subset-sum instances such as $x_1 + \cdots + x_n = -1$ require linear degree (and exponential monomial size) (cf. [20]).

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 can do that, and TSoS does not even have an inequality symbol in the language. Motivated by this, in Section IX 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 $r \leq t$ 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.

**B. Relation to previous work**

Our approach to translation of first-order into propositional logic goes back at least to Paris and Wilkie [30]. 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 $T_2^1$ and $T_2^2$ and systems around resolution [21], [23], [24].

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 [27], formalizing some linear algebra arguments in TC$^0$-Frege; Beckmann, Pudlák and Thapen [6], reasoning about parity games in resolution; and Buss, Kołodziejczyk and Zdanowski [10], 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 [10] 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 [10] 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 [32], [33].

**II. PROPOSITIONAL AND ALGEBRAIC SYSTEMS**

Let $\mathcal{R}$ be an integral domain, that is, a commutative ring with unity and no zero divisors. We will work with sets of equations over $\mathcal{R}$, of the form $\{p_i = 0 : i \in I\}$ where each $p_i$ is from $\mathcal{R}[x_1, \ldots, x_n]$, that is, a polynomial with coefficients from $\mathcal{R}$ 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 $p_i \geq 0$.

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 II-D 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 \( \mathcal{R} \), and satisfiable otherwise.

**Definition 1.** We define the product of two sets of equations to be \( \mathcal{P} \cdot \mathcal{Q} := \{ p \cdot q = 0 \mid p = 0 \in \mathcal{P}, \ q = 0 \in \mathcal{Q} \} \).

Notice that an assignment of values in \( \mathcal{R} \) to variables satisfies \( \mathcal{P} \cdot \mathcal{Q} \) if and only if it satisfies \( \mathcal{P} \) or \( \mathcal{Q} \), and that if \( \mathcal{S} \) is another set of equations, then \( \mathcal{P} \cdot (\mathcal{Q} \cup \mathcal{S}) = (\mathcal{P} \cdot \mathcal{Q}) \cup (\mathcal{P} \cdot \mathcal{S}) \). 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 rule; and as a series of steps, each following from previous steps by one of the rules

- **Addition rule** \( \frac{p = 0}{ap + br = 0} \)
- **Multiplication rule** \( \frac{p = 0}{px_i = 0} \)

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

A PC\(_\mathcal{R}\) refutation of a set of equations \( \mathcal{F} \) is a derivation of 1 = 0 from \( \mathcal{F} \).

As \( \mathcal{R} \) 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 PC\(_\mathcal{R}\) as follows. The radical rule [15] is sound because \( \mathcal{R} \) is an integral domain. The sum-of-squares rule is sound if \( \mathcal{R} \) 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 \( i \).

| Rule           | PC\(_\mathcal{R}\) Formula | Radical rule | Sum-of-squares rule |
|----------------|-----------------------------|--------------|---------------------|
| Addition rule  | \( \frac{p = 0}{ap + br = 0} \) | \( \frac{p^2 = 0}{p = 0} \) | \( \frac{p^2 + \sum_i q_i^2 = 0}{p^2 = 0} \) |
| Multiplication rule | \( \frac{p = 0}{px_i = 0} \) |

**Definition 3.** The system PC\(_{\mathcal{R}\text{ad}}\) is PC\(_\mathcal{R}\) plus the radical rule.

**Definition 4.** The system PC\(_{\mathcal{R}+}\) is PC\(_\mathcal{R}\) 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. PC\(_{\mathcal{R}\text{ad}}\) and PC\(_{\mathcal{R}+}\) derivations and refutations are defined just as in Definition 2. We will only study PC\(_{\mathcal{R}+}\) in the case in which the underlying ring \( \mathcal{R} \) is the real numbers, and will write simply PC\(_+\) instead of PC\(_{\mathcal{R}+}\).

**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 PC\(_{\mathcal{R},d}\), PC\(_{\mathcal{R}\text{ad},d}\) and PC\(_{\mathcal{R}+,d}\) 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 \( \mathcal{R} \).

A proof system is implicationally complete if, whenever a set of equations \( \mathcal{F} \) implies an equation \( q = 0 \), there is a derivation \( \mathcal{F} \vdash q = 0 \) in the system. It is known that PC\(_\mathcal{R}\) is implicationally complete in the presence of the Boolean axioms [5, 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, PC\(_{\mathcal{R}\text{ad}}\) is implicationally complete if \( \mathcal{R} \) is an algebraically closed field, and PC\(_+\) is implicationally complete (over the reals).

**Proposition 6.** If \( \mathcal{F} \) is an algebraically closed field, then PC\(_{\mathcal{R}\text{ad}}\) is implicationally complete.

**Proposition 7.** PC\(_+\) is implicationally complete.

**B. Static systems**

Below we write \( \equiv \) to express identity of polynomials.

**Definition 8.** A Nullstellensatz derivation of an equation \( q = 0 \) from a set of equations \( \mathcal{S} = \{ p_i = 0 : i \in I \} \) is a family of polynomials \( (r_i)_{i \in I} \) such that \( \sum_i r_ip_i \equiv q \). A Nullstellensatz refutation of \( \mathcal{S} \) is a derivation of 1 = 0 from \( \mathcal{S} \).
The sum-of-squares proof system \( \text{SoS} \), introduced in Barak et al. [3] as a restricted fragment of Grigoriev and Vorobjov’s Positivstellensatz proof system [18], 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 \( \text{SoS} \) that operates only with polynomial equalities as follows:

**Definition 9.** A sum of squares (SoS) derivation of an inequality \( q \geq 0 \) over \( \mathbb{R} \) from a set of equations \( S = \{ p_i = 0 : i \in I \} \) 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 \( S \) is a derivation of \(-1 \geq 0\) from \( S \).

An \( \text{SoS} + \text{Bool} \) 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 \( S \).

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 \( \text{SoS}_d \) for SoS limited to degree \( d \) or less. We allow ourselves, informally, to write inequalities in other forms than \( q \geq 0 \).

**C. 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 10.** A system \( P \) simulates a system \( Q \), written \( P \geq Q \), if there is a function \( f : \mathbb{N} \rightarrow \mathbb{N} \) such that, for any \( d \in \mathbb{N} \), if a set of equations \( F \) is refutable in degree \( d \) in \( Q \) then \( F \) 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 \( \mathcal{R} \) we have \( \text{PC}_\mathcal{R} \leq \text{PC}^\text{rad}_\mathcal{R} \leq \text{PC}^+_{\mathcal{R}} \) (but recall that \( \text{PC}^\text{rad}_\mathcal{R} \) may or may not be sound, depending on \( \mathcal{R} \)).

The main result of this section is to show that, for constant degree, the dynamic system \( \text{PC}^+ \) is equivalent to the static system \( \text{SoS} + \text{Bool} \) (Proposition 13 and Theorem 14).

Before proving this, we will say more about the radical rule. By implicational completeness, the rule is derivable in \( \text{PC}_\mathcal{R} \) 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 \( \mathcal{R} \) is a field of positive characteristic.

**Proposition 11.** Suppose \( \mathcal{R} \) is a field of positive characteristic. Then, in the presence of the Boolean axioms, \( \text{PC}_\mathcal{R} \equiv \text{PC}^\text{rad}_\mathcal{R} \).

**Proof sketch.** Let \( \mathcal{R} \) have characteristic \( p \). Then, 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 this equality is derivable in \( \text{PC}_\mathcal{R} \) with degree \( O(\rho) \) proofs (this can be shown by induction on the number of variables in \( f \)). Hence, there is a \( \text{PC}_\mathcal{R} \) derivation \( f^2 = 0 \vdash f = 0 \) of degree \( O(\deg f) \). We replace applications of the radical rule with derivations of this form.

On the other hand, if \( \mathcal{R} \) is a field of characteristic 0, then by the following lemma \( \text{PC}^\text{rad}_\mathcal{R} \) is strictly stronger than \( \text{PC}_\mathcal{R} \) 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 12.** If \( \mathcal{R} \) is a field of characteristic 0, then \( \text{PC}_\mathcal{R} \) derivations of \( x_1 + \cdots + x_n + 1 = 0 \) from \( \{ x_i^2 - x_i = 0 : i = 1, \ldots, n \} \) require degree \( \Omega(n) \).

The proof is similar to that in the \( \text{PC}_\mathcal{R} \) lower bound for the Subset Sum principle in [20]. We now show the simulations between \( \text{SoS} \) and \( \text{PC}^+ \).

**Proposition 13.** If \( S \) is refutable in degree \( d \) in \( \text{SoS} \) then it is refutable in degree \( d \) in \( \text{PC}^+ \). Furthermore this refutation does not use the radical rule.

**Theorem 14.** \( \text{SoS} + \text{Bool} \) simulates \( \text{PC}^+ \), and the simulation at most doubles the degree.

We omit the proof of Proposition 13. Our argument for Theorem 14 is an extension of the simulation of \( \text{PC}_\mathcal{R} \) in \( \text{SoS} \) described in [7], which works by translating \( \text{PC}_\mathcal{R} \) derivations of \( p = 0 \) into \( \text{SoS} + \text{Bool} \) derivations of \( p^2 \leq 0 \). We additionally need to deal with the radical and sum-of-squares rules.

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

**Lemma 15.** Suppose \( r = 0 \) is derivable from a set of equalities \( S \) by a \( \text{PC}^+ \) derivation of degree \( d \). Then, for every \( \epsilon > 0 \), there exists a degree \( 2d \) \( \text{SoS} + \text{Bool} \) derivation of \( r^2 \leq \epsilon \) from \( S \).

**Proof.** Let \( r_1, \ldots, r_n = 0 \) be the \( \text{PC}^+ \) derivation. We prove by induction on \( s \) that, for every \( \epsilon > 0 \), \( -r_s^2 + \epsilon \geq 0 \) has a \( \text{SoS} + \text{Bool} \) 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 \( S \), the \( \text{SoS} + \text{Bool} \) 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 $\pi$ of $-r_k^2 + \epsilon \geq 0$ of degree $2d$. We have

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

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

Suppose $r_s = 0$ is derived by the addition rule, so $r_s \equiv ar_i + br_j$ 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 $\pi$ of $-r_i^2 + \frac{\epsilon}{4a^2} \geq 0$ and $\pi'$ of $-r_j^2 + \frac{\epsilon}{4b^2} \geq 0$, both of degree $2d$. We have

$$ 2a^2(-r_i^2 + \frac{\epsilon}{4a^2}) + 2b^2(-r_j^2 + \frac{\epsilon}{4b^2}) + (ar_i - br_j)^2 $$

$$ \equiv -a^2r_i^2 - b^2r_j^2 + \epsilon - 2abr_ir_j \equiv -r_s^2 + \epsilon. $$

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

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

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

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

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 $\pi$ 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 14.** We are given a PC$^+$ derivation of $1 = 0$, in degree $d$, from a set of equalities $\mathcal{S}$. By Lemma 15, setting $\epsilon = \frac{1}{2}$, there is a SoS + Bool derivation $\pi$ of $-1 + \frac{\epsilon}{2} \geq 0$ from $\mathcal{S}$ in degree at most $2d$. Thus $2\pi$ is the required SoS + Bool refutation of $\mathcal{S}$.

**D. 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 $\mathcal{F}$. So we extend the definitions of refutations and derivations by defining, for all systems, a derivation $\mathcal{F} \vdash \epsilon$ to be a derivation $\mathcal{F}' \vdash \epsilon$ for some finite $\mathcal{F}' \subseteq \mathcal{F}$. This does not change anything significant above.

Propositions 6 and 7, the implicational completeness of PCOrd (for $\mathcal{F}$ an algebraically closed field) and PC$^+$, still hold in the infinite case, because of the algebraic fact that if the underlying ring $\mathcal{R}$ is a field then $\mathcal{R}[x_1, \ldots, x_n]$ is Noetherian (every ideal is finitely generated) and 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 $\mathcal{G}$ from a set of equations $\mathcal{F}$. We formally take this to be a function associating a derivation $\mathcal{F} \vdash \epsilon$ to each equation $\epsilon \in \mathcal{G}$; 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 $\mathcal{F} \vdash \mathcal{G}$ is the maximum of the degrees of the derivations it contains, if this maximum exists.

**III. ALGEBRAIC AND SEMI-ALGEBRAIC FIRST-ORDER THEORIES**

Let $\mathcal{R}$ be an integral domain. We introduce TPC$\mathcal{R}$, a two-sorted theory in the language $\mathcal{L}_2^\mathcal{R}$ 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.

**A. The language $\mathcal{L}_2^\mathcal{R}$**

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 $\Sigma$ 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 $\approx_{\text{ind}}$ and $\approx_{\text{ring}}$ for the two sorts. We will usually omit the subscripts.
- A set $F_{\text{ind}}$ 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 $F_{\text{ring}}$ 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 a ring element.

The intended meaning of $X(i)$ is the $i$th 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 $F_{\text{ind}}$ and $F_{\text{ring}}$ are uncountable, that $F_{\text{ind}}$ contains an index-sort constant for every $i \in \mathbb{N}$ and that $F_{\text{ring}}$ contains a ring-sort constant for every $a \in \mathcal{R}$.

**Definition 16.** Formally $\mathcal{L}_2^\mathcal{R}$ is defined inductively as follows.
- It contains the symbols from $\{+, -, \cdot, X, \approx_{\text{ind}}, \approx_{\text{ring}}\}$.
- For every ring-valued $\mathcal{L}_2^\mathcal{R}$ 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 $\sum_{i \in \mathcal{N}}(n, \bar{m}, \bar{z})$, where $n$ is an index variable.

We will usually write $\sum_{i \in \mathcal{N}}(n, \bar{m}, \bar{z})$ 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 $F_{\text{ind}}$, and that the term $t$ in Definition 16 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 $\mathcal{L}_2^\mathcal{R}$ terms are constructed by
the function symbols \(+,\cdot,\,-\), the function symbols in \(F_{\text{ind}}\)
and \(F_{\text{ring}}\), the oracle symbol \(X\), the big sum terms, and
the variables (of both sorts) that can also occur in function
symbols. The class of \(\mathcal{L}^R_{=}\) 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) \(\lor, \land, \neg\) and \(\exists, \forall\).

**Definition 17.** Let \(\sigma\) be an \(\mathcal{L}^R_{=}\)-symbol or a variable. We
inductively say that an \(\mathcal{L}^R_{=}\)-expression mentions \(\sigma\) if it either
contains \(\sigma\), or contains a symbol \(\sum_{s,i}T\) for a term \(s\) that
mentions \(\sigma\).

**Definition 18.** A standard model for \(\mathcal{L}^R_{=}\) is a structure
\((\mathbb{N}, R, A)\) where \(\mathbb{N}\) interprets the index sort, \(R\) interprets
the ring sort, \(A\) is a function \(\mathbb{N} \to R\) 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 \((\mathbb{N}, R, A)\).

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 \(\Phi^R_{=}\) of \(\mathcal{L}^R_{=}\) 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 V-A and V-B.

**Definition 19.** The class \(\Phi^R_{=}\) is defined inductively by:

- All atomic formulas are in \(\Phi^R_{=}\).
- All formulas, of any logical complexity, which do not
  mention the oracle symbol \(X\) or any ring variable, are in \(\Phi^R_{=}\).
- If \(\varphi_1, \varphi_2 \in \Phi^R_{=}\), then \(\varphi_1 \lor \varphi_2 \in \Phi^R_{=}\) and \(\varphi_1 \land \varphi_2 \in \Phi^R_{=}\).
- If \(\varphi(v) \in \Phi^R_{=}\), where \(v\) may have either sort, then
  \(\forall \varphi(v) \in \Phi^R_{=}\).

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, \(\forall \varphi(v)\)
in Definition 19 can be translated adequately into a set of
polynomials of bounded-degree, and the fact that the set of
polynomials of infinite does not constitute an obstacle to our
results.

**B. The axioms of TPC\(_R\) and TSoS**

The theory TPC\(_R\) 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.

- **a) Basic axioms:**
  - The standard ring axioms for \(0, 1 \in \mathbb{R}\) and \(+, -, \cdot\).
  - The integral domain axiom \(xy = 0 \supset (x = 0 \lor y = 0)\).
  - The big sum defining axiom scheme. This contains, for
each ring-valued term \(t(i)\), in which other parameters can
also occur, the axioms
    \[
    \sum_{i < 0} t(i) = 0 \quad \sum_{i < j + 1} t(i) = \sum_{i < j} t(i) + t(j).
    \]
  - Every sentence \(\sigma\) such that
    (i) \(\sigma\) does not mention the oracle symbol \(X\) or any ring
    variable, and
    (ii) \(\sigma\) 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
    \[
    x = x \quad i = i \quad \sum_{i < n} t(i) = f((\sum_{i < n} \sigma(i, \bar{t})) = f(\sum_{i < n} \sigma(i, \bar{t}))
    \]
    where \(f\) is a function symbol and each \(=\) is either \(=\) or \(=\) as appropriate.

- **b) Induction scheme:**
  - For each formula \(\varphi(i)\) in the class \(\Phi^R_{=}\), in which other
    parameters can also occur, the induction axiom
    \[
    \varphi(0) \land \forall i (\varphi(i) \supset \varphi(i + 1)) \supset \forall n \varphi(n).
    \]
- **c) Sum-of-squares scheme and Boolean axiom:**
  - For each ring-valued term \(t(i)\), in which other parameters
    can also occur, the axiom
    \[
    \sum_{i < n} t(i)^2 = 0 \lor j < n \supset j(t) = 0.
    \]
  - The axiom \(X(i)(1 - X(i)) = 0\).

In the presence of the integral domain axiom, the Boolean
axiom is equivalent to asserting that \(X = 0\) valued.

**IV. EXAMPLES OF FIRST-ORDER PROOFS**

We will discuss how some versions of the pigeonhole
principle (PHP, for short) can be proved in TPC\(_R\) and TSoS,
to give some simple examples of how the theories and trans-
lations work. We present a less-trivial proof in Section VII
below, showing that these theories prove respectively that
every (definable) constant-degree PC\(_R\) 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
TPC\(_R\). These are proved by straightforward inductions.

**Lemma 20.** The following are provable in TPC\(_R\), for all
terms \(s, t\).

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

**Definition 21.** We define \(\rho(n)\) to be the term \(\sum_{s < n} 1\).
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 \( R \) we work over may have positive characteristic, hence \( n \) and \( ρ(n) \) may not be equal as numbers).

A. Bijective and graph PHP in TPCR

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 \( θ(i, j) \) be a term. The bijective pigeonhole principle for \( θ \) and \( m, n \), or bPHP(\( θ, m, n \)), asserts that \( θ(i, j) \) 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 \( θ(i, j) = 0 \) or \( θ(i, j) = 1 \)
2. For all \( i < m \), \( θ(i, j) = 1 \) for some \( j < n \)
3. For all \( i < m \) and all \( j, j' < n \), if \( j \neq j' \) then \( θ(i, j) = 0 \) or \( θ(i, j') = 0 \)
4. For all \( j < n \), \( θ(i, j) = 1 \) for some \( i < m \)
5. For all \( j < n \) and all \( i, i' < m \), if \( i \neq i' \) then \( θ(i, j) = 0 \) or \( θ(i', j) = 0 \).

Notice that provability of bPHP in TPCR is only an interesting question if the term \( θ(i, j) \) 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 22. TPCR proves that if \( ρ(m) \neq ρ(n) \) then bPHP(\( θ, m, n \)) is false.

Proof. As we are working with classical logic, to show provability of a statement in TPCR it is enough to show that it holds in every model of TPCR. Consider an arbitrary model of TPCR, pick any index elements \( m, n \) and suppose for a contradiction that (in the model) \( ρ(m) \neq ρ(n) \) and bPHP(\( θ, m, n \)) is true. Then for each pigeon \( i \), by item 4. of Lemma 20 we have \( \sum_{j < n} θ(i, j) = 1 \), and hence \( \sum_{i < m} (\sum_{j < n} θ(i, j)) = ρ(m) \). Similarly we have \( \sum_{j < n} (\sum_{i < m} θ(i, j)) = ρ(n) \). This contradicts item 3. of Lemma 20.

Now let \( G_0 \) 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 \( G_0 \), expressing that \( G_0 \) has a perfect matching. Unlike bPHP as defined above, this formula will be \( \Phi^\leq_{\leq} \). 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 \( G_0 \), and the existence of a first-order refutation in TPCR implies the existence of a constant-degree family of PCR 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 \( G_0 \). 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 bPHP(\( G(n) \)) expresses that \( X \) describes a perfect matching of \( G_n \). We use a pairing function (which exists in \( F_{\text{ind}} \)) to treat \( X \) as a binary function symbol \( X(i, j) \).

The formula is the conjunction of:

1. For all \( i < m, \) for some \( k \in [1, d], \) either \( h_k(i) = h_k(i) \) or \( X(i, h_k(i)) = 0 \) or \( X(i, h_k(i)) = 0 \)
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 \( X(p_k(j), i) = 0 \).

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 \( \forall i \geq t \lor \varphi(i) \). Thus the formula is \( \Phi^R \) 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 23. TPCR proves that if \( ρ(m) \neq ρ(n) \) then bPHP(\( G(n) \)) is false.

Proof. Suppose bPHP(\( G(n) \)) is true. Let \( θ(i, j) \) 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 TPCR are enough to show that items 1.–5. from the definition of bPHP(\( θ, m, n \)) are true, and the result follows by Proposition 22.

Using the translations in Sections V and VI below we obtain the well-known propositional refutation of bPHP(\( G(n) \)) as a corollary. Recall that \( m \) is the cardinality of set of pigeons in \( G_n \).

Corollary 24. Suppose \( ρ(m) \neq ρ(n) \) for all \( n \in \mathbb{N} \). Then TPCR proves \( \forall n \neg \text{bPHP}(G(n)). \) Hence the propositional family bPHP(\( G_n \)) has refutations in PCR,\( d \) in some fixed degree \( d \).

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

B. Functional PHP in TSoS

We now fix the ring \( R \) to be the reals, and work in TSoS. Recall that this is TPCR plus the sum of squares axiom scheme and the Boolean axiom (Section III-B). The functional pigeonhole principle for \( θ \) and \( m, n \), or \( \exists \text{PHP}(\theta, m, n) \), 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 25. TPCR 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 20, 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 20. 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 write 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 \( \sum_{i < n} \theta(i,j) = \rho(m) \) and reason naturally about inequalities rather than about explicitly written sums of squares. We describe an approach to this goal in Section IX.

**Proposition 26.** TSoS proves that if \( m > n \) then \( \text{fPHP}(\theta, m, n) \) is false.

**Proof.** As in the proof of Proposition 22, 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 \( i \) 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 25 we have \( \sum_{i < m} \theta(i,j) = 1 - A(j)^2 \) for some term \( A(j) \).

Hence \( \sum_{j < n} \sum_{i < m} \theta(i,j) = \rho(m) - \sum_{j < n} A(j)^2 \). Using Lemma 20 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 \( \text{fPHP}(G_n) \), 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 \( b\text{PHP}(G_n) \) above, together with the condition that \( X(i,j) \) always takes the value 0 or 1 on \( G_n \).

**Proposition 27.** TSoS proves that if \( m > n \) then \( \text{fPHP}(G_n) \) 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 \( \text{fPHP}(\theta, m, n) \).

**Corollary 28.** Suppose \( m > n \) for all \( n \in \mathbb{N} \). Then TSoS proves \( \forall n \cdot \text{fPHP}(G_n) \). Hence the propositional family \( \text{fPHP}(G_n) \) has refutations in SoS+Bool in some fixed degree \( d \).

V. PROPOSITIONAL TRANSLATIONS OF FORMULAS

Let \( \alpha \) be an assignment of values in \( \mathbb{N} \) to all index variables, and values in \( \mathbb{R} \) to all ring variables. We will define a translation \( \langle \cdot \rangle_{\alpha} \) of certain \( \mathcal{L}_{\mathbb{R}} \) 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 \( \varphi \in \Phi_{\mathbb{R}} \), \( \langle \varphi \rangle_{\alpha} \) is a set of equations of bounded degree.

“Bounded degree” here means that the degree does not depend on \( \alpha \).

A. 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 \( \alpha \). This is possible because, by construction, \( t \) is formed only by composing functions in \( F_{\text{ind}} \) 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 \( \mathbb{R}[x_0, x_1, \ldots] \), 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 \( \alpha \) varies.

- If \( t \) has the form \( f(s_1, \ldots, s_k) \) where \( f \in F_{\text{ring}} \) and \( s_1, \ldots, s_k \) are index-valued, then \( \langle t \rangle_{\alpha} \) is the constant polynomial \( f(\langle s_1 \rangle_{\alpha}, \ldots, \langle s_k \rangle_{\alpha}) \).
- 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 +, −, · are translated as the corresponding operations on polynomials.
- We define \( \langle \sum t_i \rangle_{\alpha} \) to be the sum \( \langle t_0 \rangle_{\alpha} + \cdots + \langle t(n-1) \rangle_{\alpha} \).

B. Translation of formulas

We translate \( \Phi_{\mathbb{R}} \) formulas \( \varphi \) into sets of equations. First suppose \( \varphi \) does not mention \( X \) or any ring variable. We evaluate \( \varphi \) under \( \alpha \) 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 \( \alpha \), we will use the notation \( \alpha[i \mapsto n] \) for \( \alpha \) with the value of \( i \) changed to \( n \). We will also do this for ring variables, and will write for example \( \alpha[i, y \mapsto n, a] \) when we want to change several index and ring values at once. If we omit \( \alpha \) and just write an assignment in square brackets, this means that all other variables are mapped to 0 (or arbitrarily).

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

- Suppose \( \varphi \) is an atomic formula \( t = r \). By the condition on \( \varphi \), both \( t \) and \( r \) are ring-valued, since all index-valued function symbols are in \( F_{\text{ind}} \) and none of them takes any ring arguments. We put \( \langle \varphi \rangle_{\alpha} := \{ \langle t \rangle_{\alpha} - \langle r \rangle_{\alpha} = 0 \} \).
- If \( \varphi = \psi \land \psi' \) then \( \langle \varphi \rangle_{\alpha} := \langle \psi \rangle_{\alpha} \cup \langle \psi' \rangle_{\alpha} \).
- If \( \varphi = \psi \lor \psi' \) 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 \( \langle \varphi \rangle_{\alpha} := \bigcup_{n \in \mathbb{N}} \langle \psi \rangle_{\alpha[\bar{i} \mapsto n]} \).
If \( \varphi = \forall y \psi(y) \) for a ring variable \( y \), then 
\[ \langle \varphi \rangle_{\alpha} := \bigcup_{a \in \mathbb{R}} \langle \psi \rangle_{\alpha[y-a]} \]
Notice that, by the last item, \( \langle \varphi \rangle_{\alpha} \) may be infinite.

This translation captures the semantics of \( \varphi \), 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 \( \varphi \) is true under \( \alpha \) in the standard model \( \langle N, R, A \rangle \) if and only if all polynomial equations in \( \langle \varphi \rangle_{\alpha} \) are satisfied by \( A \).

VI. PROPOSITIONAL TRANSLATIONS OF PROOFS

We prove the following theorem. Note that if \( R \) has positive characteristic then by Proposition 11 we get a version of this with \( \text{PC}_\mathbb{R} + \text{Boo}l \) in place of \( \text{PC}_\mathbb{R}^{\text{rad}} \).

**Theorem 29.** Let \( \varphi(i) \) be a \( \Phi_\mathbb{R} \) formula with free index variables \( i \) and no free ring variables. Suppose \( \text{TPC}_\mathbb{R} \models \forall i \neg \varphi(i) \). Then for some \( d \in \mathbb{N} \), for every tuple \( \bar{n} \in \mathbb{N} \) there is a \( \text{PC}_\mathbb{R,d}^{\text{rad}} \) refutation of \( \langle \varphi \rangle_{\bar{n} \rightarrow \bar{a}} \).

The proof is by first translating \( \text{TPC}_\mathbb{R} \) proofs into a Gentzen-style sequent calculus \( \text{LK}_\mathbb{R} \) and then translating \( \text{LK}_\mathbb{R} \) into \( \text{PC}_\mathbb{R,d}^{\text{rad}} \) rule-by-rule.

A. The sequent calculus \( \text{LK}_\mathbb{R} \)

\( \text{LK}_\mathbb{R} \) 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 [9], 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:

- \( \text{LK}_\mathbb{R} \) contains the usual structural and logical rules of two-sorted logic.
- Any axiom of \( \text{TPC}_\mathbb{R} \) which is not an integral domain, equality, or induction axiom is the universal closure of a \( \Phi_\mathbb{R} \) formula \( \varphi(i, x) \). For each such \( \varphi \), \( \text{LK}_\mathbb{R} \) contains the axiom
  \[ \emptyset \rightarrow \varphi(s, \bar{i}) \]
  for all tuples of index-valued terms \( s \) and ring-valued terms \( \bar{i} \) of appropriate arity.
- \( \text{LK}_\mathbb{R} \) contains every substitution of terms for variables in the integral domain axiom
  \[ xy = 0 \rightarrow x = 0, y = 0 \]
  and the equality schemes
  \[ \emptyset \rightarrow x = x \]
  \[ \emptyset \rightarrow i = i \]
  \[ \bar{x} = \bar{y}, \bar{i} = \bar{j} \rightarrow f(\bar{x}, \bar{i}) = f(\bar{y}, \bar{j}). \]
- \( \text{LK}_\mathbb{R} \) contains the \( \Phi_\mathbb{R} \)-induction rule
  \[
  \frac{\Gamma, \varphi(i) \rightarrow \varphi(i + 1), \Delta}{\Gamma, \varphi(0) \rightarrow \varphi(i), \Delta}
  \]
where \( i \) is any index-valued term, \( \varphi \in \Phi_\mathbb{R} \) may contain other parameters, and \( i \) is an index variable which does not occur in the bottom sequent.

**Lemma 30.** Let \( \varphi \) be any formula such that the universal closure of \( \varphi \) is provable in \( \text{TPC}_\mathbb{R} \). Then the sequent \( \emptyset \rightarrow \varphi \) is derivable in \( \text{LK}_\mathbb{R} \). If furthermore \( \varphi \) is a negation \( \neg \psi \), then the sequent \( \psi \rightarrow \emptyset \) is derivable in \( \text{LK}_\mathbb{R} \).

**Proof.** Since \( \text{LK}_\mathbb{R} \) is complete with respect to pure logic it is enough to check that, for every axiom \( \sigma \) of \( \text{TPC}_\mathbb{R} \), the sequent \( \emptyset \rightarrow \sigma \) is derivable in \( \text{LK}_\mathbb{R} \). This is standard. \( \square \)

B. Translation of \( \text{LK}_\mathbb{R} \) into \( \text{PC}_\mathbb{R,d}^{\text{rad}} \)

Consider a sequent \( \Gamma \rightarrow \Delta \). We treat cedents as multisets of formulas. We define
\[
\langle \Gamma \rangle_{\alpha}^L := \bigcup_{\varphi \in \Gamma} \langle \varphi \rangle_{\alpha}
\]
and
\[
\langle \Delta \rangle_{\alpha}^R := \prod_{\varphi \in \Delta} \langle \varphi \rangle_{\alpha}.
\]
The superscripts \( L \) and \( R \) stand for Left and Right, and in general we use the translation \( \langle \Gamma \rangle_{\alpha}^L \) if \( \Gamma \) is an antecedent, and \( \langle \Delta \rangle_{\alpha}^R \) if \( \Delta \) is a succedent. Notice that \( \langle \Gamma \rangle_{\alpha}^L = \langle \bigwedge_{\varphi \in \Gamma} \varphi \rangle_{\alpha} \) and \( \langle \Delta \rangle_{\alpha}^R = \langle \bigvee_{\varphi \in \Delta} \varphi \rangle_{\alpha} \).

**Theorem 31.** Let \( \Pi \) be a \( \text{LK}_\mathbb{R} \) derivation of the sequent \( \Gamma \rightarrow \Delta \) in which all formulas are in \( \Phi_\mathbb{R} \) and such that all formulas in \( \Gamma \) and \( \Delta \) have free-index variables \( i \) and free ring-variables \( \bar{x} \). Then there exists \( d \in N \) such that for every assignment \( \alpha \) for \( \bar{x} \) and \( i \) there exists a \( \text{PC}_\mathbb{R,d}^{\text{rad}} \) derivation
\[
\langle \Gamma \rangle_{\alpha}^L \models \langle \Delta \rangle_{\alpha}^R.
\]
This 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 [6]. The main differences are that we do not need to deal with existential quantifiers, and that we are using multiplication instead of disjunction \( \lor \), so need to use the radical rule to deal with contraction.

Now we are able to prove Theorem 29, the translation of \( \text{TPC}_\mathbb{R} \) into \( \text{PC}_\mathbb{R,d}^{\text{rad}} \).

**Proof of Theorem 29.** Let \( \varphi(i) \) be a \( \Phi_\mathbb{R} \) formula with free index variables \( i \) and no free ring variables. Suppose \( \text{TPC}_\mathbb{R} \models \forall i \neg \varphi(i) \).

By Lemma 30 there is an \( \text{LK}_\mathbb{R} \)-derivation of the sequent \( \varphi(i) \rightarrow \emptyset \). By the two-sorted version of the free-cut elimination theorem (see [9]), we may assume that this derivation contains no free cuts. All formulas in the non-logical axioms and the induction rule of \( \text{LK}_\mathbb{R} \) are \( \Phi_\mathbb{R} \). Therefore, by the subformula property of free-cut free proofs, every formula in this derivation is \( \Phi_\mathbb{R} \). Hence we can apply Theorem 31 and conclude that there is a \( d \in \mathbb{N} \) such that for every tuple \( \bar{n} \in \mathbb{N} \), we have a \( \text{PC}_\mathbb{R,d}^{\text{rad}} \) refutation of \( \langle \varphi \rangle_{\bar{n} \rightarrow \bar{a}} \). \( \square \)

VII. FORMALIZING \( \text{PC}_\mathbb{R,d}^{\text{rad}} \) IN \( \text{TPC}_\mathbb{R} \)

We claim that everything refutable in \( \text{PC}_\mathbb{R} \) in constant degree is also refutable in \( \text{TPC}_\mathbb{R} \), in the sense of the following theorem. The formula \( \varphi \) in the statement should be understood as expressing something about the oracle sequence \( X \), using a size parameter \( i \).

**Theorem 32.** Let \( \varphi(i) \) be any \( \Phi_\mathbb{R} \) 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 $\langle \varphi \rangle_{[n \to n]}$ is refutable in $\text{PC}_R^{\text{rad}}$ by some refutation $\pi_n$ of degree $d$. Then $\text{TPC}_R \vdash \forall i \neg \varphi(i)$.

This result does not require any assumptions on the uniformity of the refutations $\pi_n$ because we have included all functions $F_{\text{ind}}$ and $F_{\text{ring}}$ 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 $\text{TPC}_R$ proves the soundness of constant depth $\text{PC}_R^{\text{rad}}$. 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, and the details are omitted here.

VIII. TRANSLATIONS TO AND FROM CONSTANT DEGREE $\text{SoS}$

Recall that the theory $\text{TSoS}$ is in the same language as $\text{TPC}_R$ – in particular, we do not add any ordering symbol for the ring sort. $\text{TSoS}$ extends $\text{TPC}_R$ by adding the Boolean axiom and the sum-of-squares axiom scheme defined in Section III, 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 $\text{TSoS}$ and constant degree $\text{SoS} + \text{Bool}$ as we showed between $\text{TPC}_R$ and $\text{PC}_R^{\text{rad}}$.

Theorem 33. Let $\varphi(i)$ be any $\Phi^R$ formula with no ring quantifiers and with index variable $i$ as its only free variable. Define $S_n$ to be the set of equations $\langle \varphi \rangle_{[n \to n]}$. Then every set $S_n$ is refutable in $\text{SoS} + \text{Bool}$ in some fixed constant degree if and only if $\text{TSoS} \vdash \forall i \neg \varphi(i)$.

Proof. Suppose $\text{TSoS} \vdash \forall i \neg \varphi(i)$. We extend the proof of Theorem 29 to deal with the the sum-of-squares scheme and the Boolean axiom. For the sum-of-squares scheme, we extend the sequent calculus $\text{LK}_R$ by adding the sequents

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

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 $\alpha$ there is a depth $d$ $\text{SoS}$ 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 $\sum_{i<n} t(i)^2 = 0 \vdash \langle t(m) \rangle_\alpha = 0$ 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 $\text{LK}_R$ by adding the sequent

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

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 $\text{PC}$ soundness in the theory by showing that $\text{TSoS}$ can prove the soundness of the sum-of-squares rule and the propositional Boolean axioms. This is straightforward.

IX. THEORIES THAT REASON DIRECTLY ABOUT INEQUALITIES

We have developed a first-order theory, $\text{TSoS}$, with the property that the sentences about $X$ (of a suitable form) which are refutable in $\text{TSoS}$ are precisely the principles that are refutable in constant depth $\text{SoS}$. This gives us a new way of constructing $\text{TSoS}$ refutations. But this theory has the disadvantage of being somewhat unnatural, as intuitively a natural theory for $\text{SoS}$ would allow us to reason directly about inequalities on the ring sort. This is something $\text{TSoS}$ 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 IV-B, and in this sense we have not gained much from working in $\text{SoS}$.

In this section we sketch some approaches for getting a more “usable” theory than $\text{TSoS}$. Our goal is to construct a theory $T$ which extends $\text{TSoS}$ 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 $\text{TSoS}$ that every sentence refutable in $T$ (of a suitable form) translates into a principle with constant degree $\text{SoS} + \text{Bool}$ refutations.

We do not take this approach here, but a natural way to achieve this would be for $T$ to be conservative over $\text{TSoS}$, that is, for every relevant sentence in the language of $\text{TSoS}$ that is provable in $T$ to be already provable in $\text{TSoS}$. 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.

A. $\text{TSoS}_\geq$ - unrestricted use of ordering

We first consider what happens if we introduce ordering in a naive way. We define a language $\mathcal{L}_\geq$ by taking $\mathcal{L}_R^{\geq}$ and adding a binary relation symbol $\geq$ for an partial order on the ring sort. We define $\Phi^R_\geq$ in the same way as $\Phi^R_=$ except that we also allow the $\geq$ symbol in all places that $\Phi^R_=$ allows the ring equality symbol $\equiv_{\text{ring}}$. In particular, formulas made from atomic formulas of the form $s \geq t$, for ring terms $s, t$, and closed under $\land, \lor$ and $\forall$ are $\Phi^R_\geq$ formulas.
The theory $\text{TSoS}_2$ is $\text{TSoS}$ 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. $x \geq 0 \land y \geq 0 \supset x \cdot y \geq 0$
  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 $\Phi_2$ (with other parameters allowed).

The next proposition shows that $\text{TSoS}_2$ 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 $S$ is any constant-degree set of polynomial equations that are unsatisfiable over 0/1 assignments, then $\text{TSoS}_2$ proves that $S$ is not satisfied by $X$. Hence if a version of our translation theorem for $\text{TSoS}$, Theorem 33, held for $\text{TSoS}_2$, it would imply that $S$ has a constant-degree refutation in $\text{SoS} + \text{Bool}$, which is not in general true.

This theory seems rather to correspond to the fully dynamic version of constant-degree $\text{SoS}$, which is a very strong system. For example, the (complete) Lovasz-Schrijver proof system is the degree 2 fragment of it [16].

**Proposition 34.** 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 $F_{\text{ind}}$ which take $n$ as a parameter). Then $\text{TSoS}$ 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 $F_{\text{ind}}$, we can construct a ring-valued term

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

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 $\Phi_2$, as we can handle bounded index quantifiers the same way as we did in Section IV-A. 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 $1 \neq 0$.

**B. Other theories**

In this section we discuss some ongoing work on how to weaken a theory like $\text{TSoS}_2$ described above, into something which (a) still allows robust reasoning about orderings; (b) still proves the soundness of $\text{SoS}$; but (c) admits a translation into constant degree $\text{SoS}$, similar to Theorem 33.

A first observation is that the integral domain axiom plays a big role in the proof of Proposition 34, 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 VII. Furthermore the integral domain axiom is the only place in which a disjunction explicitly appears in our sequent calculus (it is implicitly allowed in $\Phi_2^B$ 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 34 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 $x \geq_d y \supset x \geq_{>d} y$ for each $e > d$
ii. $x \geq_d y \supset x + z \geq_d y + z$
iii. $x \geq_d 0 \land y \geq_d 0 \supset x \cdot y \geq_{d+e} 0$
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 $(s - t) - U = 0$, 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 34 still goes through if we replace $\geq$ there with $\geq_d$.

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 $\varphi \lor \psi$ at most one of $\varphi$ and $\psi$ can contain an inequality (in fact we may need the stronger condition that at most one of $\varphi$ and $\psi$ can mention ring variables or the oracle $X$).

We believe that weakening $\text{TSoS}_2$ along these lines gives a theory with (b) and (c) (that is, with the strength of constant-degree $\text{SoS}$). 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 $\lor$ and $\neg$ connectives (but so far still requiring the “levelled” orderings $\geq_\alpha$).

Let us call this formula-class $\Phi^\land_\land$ and the theory $TS\text{oS}^\land_\land$. The translations of $\Phi^\land_\land$ formulas and $TS\text{oS}^\land_\land$ 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 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 $\omega$. The translation theorem for $TS\text{oS}^\land_\land$ proofs then says that, for example, if there is a $TS\text{oS}^\land_\land$ proof of $\varphi_1 \supset \varphi_2$, where $\varphi_1, \varphi_2$ are $\Phi^\land_\land$ formulas not containing $\lor$, then for every $\alpha$ and $\omega$ there exists $\omega_2$ and a 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 $\langle \varphi_1 \supset \varphi_2 \rangle \supset (\varphi_2 \supset \varphi_1)$. 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.

ACKNOWLEDGMENT

The authors would like to thank Leszek Kołodziejczyk for helpful discussion 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] Boaz Barak. Sum of squares upper bounds, lower bounds, and open questions. Lecture notes, 2014. I, I
[3] 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. (document), I, II-B
[4] Boaz Barak and David Steurer. Sum-of-squares proofs and the quest toward optimal algorithms. Electronic Colloquium on Computational Complexity (ECCC), 21:59, 2014. (document)
[5] 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. I, A1, II-A
[6] Arnold Beckmann, Pavel Pudlák, and Neil Thapen. Parity games and propositional proofs. ACM Transactions on Computational Logic, 1, I-B, VI-B
[7] 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. (document)
[8] Samuel R. Buss. Bounded Arithmetic, volume 3 of Studies in Proof Theory. Bibliopolis, 1986. I
[9] 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. VI-A, VI-B
[10] Samuel R. Buss, Leszek Aleksander Kołodziejczyk, and Konrad Zdanowski. Collapsing modular counting in bounded arithmetic and constant depth propositional proofs. Transactions of the AMS, (367):7517–7563, 2015. I, I-B
[11] 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. I
[12] Stephen Cook and Phuong Nguyen. Logical Foundations of Proof Complexity. ASL Perspectives in Logic. Cambridge University Press, 2010. I
[13] Noah Fleming, Pravesh Kothari, and Toniann Pitassi. Semialgebraic proofs and efficient algorithm design. Found. Trends Theor. Comput. Sci., 14(1-2):1–221, 2019. I
[14] D. Grigoriev. Complexity of Positivstellensatz proofs for the knapsack. Comput. Complexity, 10(2):139–154, 2001. I-A3
[15] 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 (Creteil, 2001). 2, II-A
[16] Dima Grigoriev, Edward A. Hirsch, and Dmitrii V. Pasechnik. Complexity of semialgebraic proofs. Mosc. Math. J., 2(4):647–679, 2002. I, IX-A
[17] Dima Grigoriev and Nicolai Vorobjov. Complexity of Null- and Positivstellensatz proofs. Ann. Pure Appl. Logic, 113(1-3):153–160, 2002. I
[18] 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). II-B
[19] P. Hájek and P. Pudlák. Metamathematics of First-order Arithmetric. Perspectives in Mathematical Logic. Springer-Verlag, Berlin, 1993. I
[20] 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. I-A3, II-C
[21] Jan Krajíček. Lower bounds to the size of constant-depth propositional proofs. The Journal of Symbolic Logic, 59(1):73–86, 1994. I-B
[22] Jan Krajíček. Bounded arithmetic, propositional logic, and complexity theory, volume 60 of Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge, 1995. I
[23] 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. I-B
[24] Jan Krajíček. On the weak pigeonhole principle. Fund. Math., 170(1-2):123–140, 2001. I-B
[25] László Lovász. Stable sets and polynomials. Discrete Mathematics, 124:137–153, 1994. I
[26] L. Lovász and A. Schrijver. Cones of matrices and set-functions and 0–1 optimization. SIAM Journal on Optimization, 1:166–190, 1991. I
[27] 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. I-B
[28] Ryan O’Donnell. SOS is not obviously automatizable, even approximately. Electron. Colloquium Comput. Complex., 23:141, 2016. I
[29] 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. I
[30] J. Paris and A. 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. I, I-B
[31] 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. I
[32] Michael Soltys and Stephen Cook. The proof complexity of linear algebra. Ann. Pure Appl. Logic, 130(1-3):277–323, 2004. I, I-B
[33] Neil Thapen and Michael Soltys. Weak theories of linear algebra. Arch. Math. Log., 44(2):195–208, 2005. I, I-B