2014 IEEE Annual Symposium on Foundations of Computer Science

Circuit Complexity, Proof Complexity and Polynomial Identity Testing

(Extended abstract)

Joshua A. Grochow
Santa Fe Institute
Santa Fe, NM, USA
Email: jgrochow@santafe.edu

Toniann Pitassi
Depts. of Computer Science and Mathematics
University of Toronto
Toronto, Canada
Email: toni@cs.toronto.edu

***Abstract*—We introduce a new and natural algebraic proof system, which has tight connections to (algebraic) circuit complexity. In particular, we show that any super-polynomial lower bound on any Boolean tautology in our proof system implies that the permanent does not have polynomial-size algebraic circuits ($\mathsf{VNP} \neq \mathsf{VP}$).**

As a corollary, super-polynomial lower bounds on the number of lines in Polynomial Calculus proofs (as opposed to the usual measure of number of monomials) imply the Permanent versus Determinant Conjecture.

Note that, prior to our work, there was no proof system for which lower bounds on an arbitrary tautology implied *any* computational lower bound.

Our proof system helps clarify the relationships between previous algebraic proof systems, and begins to shed light on why proof complexity lower bounds for various proof systems have been so much harder than lower bounds on the corresponding circuit classes. In doing so, we highlight the importance of polynomial identity testing (PIT) for understanding proof complexity.

***Keywords*-AC0[p]-Frege; algebraic circuit complexity; Grobner bases; lower bounds; polynomial identity testing; proof complexity; syzygies**

All proofs are present in the freely available draft of the full version [1].

I. Introduction

NP versus coNP is the very natural question of whether, for every graph that doesn't have a Hamiltonian path, there is a short proof of this fact. One of the arguments for the utility of proof complexity is that by proving lower bounds against stronger and stronger proof systems, we "make progress" towards proving $\mathsf{NP} \neq \mathsf{coNP}$. However, until now this argument has been more the expression of a philosophy or hope, as there is no known proof system for which lower bounds imply computational complexity lower bounds of any kind, let alone $\mathsf{NP} \neq \mathsf{coNP}$.

We remedy this situation by introducing a very natural algebraic proof system, which has tight connections to (algebraic) circuit complexity. We show that any super-polynomial lower bound on any Boolean tautology in our proof system implies that the permanent does not have polynomial-size algebraic circuits ($\mathsf{VNP} \neq \mathsf{VP}$). Note that, prior to our work, essentially all implications went the opposite direction: a circuit complexity lower bound implying a proof complexity lower bound. We use this result to begin to explain why several long-open lower bound questions in proof complexity—lower bounds on Extended Frege, on $\mathsf{AC}^0[p]$-Frege, and on number-of-lines in Polynomial Calculus-style proofs—have been so apparently difficult.

A. Background and Motivation

Algebraic Circuit Complexity.: The most natural way to compute a polynomial function $f(x_1, \ldots, x_n)$ is with a sequence of instructions $g_1, \ldots, g_m = f$—called an algebraic circuit or a straight-line program—starting from the inputs $x_1, \ldots, x_n$, and where each instruction g_i is of the form $g_j \circ g_k$ for some $j, k < i$, where $\circ$ is either a linear combination or multiplication. The goal of algebraic complexity is to understand the optimal asymptotic complexity of computing a given polynomial family $(f_n(x_1, \ldots, x_{\mathrm{poly}(n)})_{n=1}^{\infty}$, typically in terms of size and depth of algebraic circuits. In addition to the intrinsic interest in these questions, since Valiant's work [2] algebraic complexity has become more and more important for Boolean computational complexity. Valiant argued that understanding algebraic complexity could give new intuitions that may lead to better understanding of other models of computation; several direct connections have been found between algebraic and Boolean complexity [3], [4], [5]; and the Geometric Complexity Theory Program (see, e. g., the overview [6] and references therein) suggests how algebraic techniques might be used to resolve major Boolean complexity conjectures.

Two central functions in this area are the determinant and permanent polynomials, which are fundamental both because of their prominent role in many areas of mathematics and because they are complete for various natural complexity classes. In particular, the permanent of $\{0, 1\}$-matrices is $\#\mathsf{P}$-complete, and the permanent of arbitrary matrices is VNP-complete. Valiant's Permanent versus Determinant Conjecture [2] states that the permanent of an $n \times n$ matrix, as a polynomial in n^2 variables, cannot be written as the determinant of any polynomially larger matrix all of whose entries are variables or constants.

0272-5428/14 $31.00 © 2014 IEEE
DOI 10.1109/FOCS.2014.20

Unlike in Boolean circuit complexity, (slightly) non-trivial lower bounds for the size of algebraic circuits are known [7], [8]. However, their techniques only give lower bounds up to $\Omega(n \log n)$. Moreover, their methods do not give lower bounds for polynomials of constant degree. Recent exciting work [9], [10], [11] has shown that polynomial-size algebraic circuits computing functions of polynomial degree can in fact be computed by subexponential-size depth 4 algebraic circuits. Thus, strong enough lower bounds for depth 4 algebraic circuits for the permanent would already prove $\mathsf{VP} \neq \mathsf{VNP}$.

Proof Complexity.: Despite considerable progress obtaining super-polynomial lower bounds for many weak proof systems (resolution, cutting planes, bounded-depth Frege systems), there has been essentially no progress in the last 25 years for stronger proof systems such as Extended Frege systems or Frege systems. More surprisingly, no nontrivial lower bounds are known for the seemingly weak $\mathsf{AC}^0[p]$-Frege system. In contrast, the analogous result in circuit complexity was resolved by Smolensky over 25 years ago [12].

To date, there has been no satisfactory explanation for this state of affairs. In proof complexity, there are no known formal barriers such as relativization [13], Razborov–Rudich-natural proofs [14], or algebrization [15] that exist in Boolean function complexity. Moreover, there has not even been progress by way of conditional lower bounds. That is, trivially $\mathsf{NP} \neq \mathsf{coNP}$ implies superpolynomial lower bounds for $\mathsf{AC}^0[p]$-Frege, but we know of no weaker complexity assumption that implies such lower bounds. The only formal implication in this direction shows that certain circuit lower bounds imply lower bounds for proof systems that admit feasible interpolation, but unfortunately even very weak proof systems such as Frege and AC^0-Frege don't have this property, under standard complexity-theoretic assumptions [16], [17]. In the converse direction, there are essentially no implications at all. For example, we do not know if $\mathsf{AC}^0[p]$-Frege lower bounds—nor even Frege nor Extended Frege lower bounds—imply any nontrivial circuit lower bounds.

B. Our Results

In this paper, we define a simple and natural proof system that we call the Ideal Proof System (IPS) based on Hilbert's Nullstellensatz. Our system is similar in spirit to related algebraic proof systems that have been studied previously, but is different in a crucial way that we explain below.

Given a set of polynomials $F_1, \ldots, F_m$ in n variables $x_1, \ldots, x_n$ over a field $\mathbb{F}$ without a common zero over the algebraic closure of $\mathbb{F}$, Hilbert's Nullstellensatz says that there exist polynomials $G_1, \ldots, G_m \in \mathbb{F}[x_1, \ldots, x_n]$ such that $\sum F_i G_i = 1$, i. e., that 1 is in the ideal generated by the F_i. In the Ideal Proof System, we introduce new variables y_i which serve as placeholders into which the original polynomials F_i will eventually be substituted:

Definition 1 (Ideal Proof System)**.** An *IPS certificate* that a system of $\mathbb{F}$-polynomial equations $F_1(\vec{x}) = F_2(\vec{x}) = \cdots = F_m(\vec{x}) = 0$ is unsatisfiable over $\overline{\mathbb{F}}$ is a $\mathbb{F}$-polynomial $C(\vec{x}, \vec{y})$ in the variables $x_1, \ldots, x_n$ and $y_1, \ldots, y_m$ such that

1) $C(x_1, \ldots, x_n, \vec{0}) = 0$, and
2) $C(x_1, \ldots, x_n, F_1(\vec{x}), \ldots, F_m(\vec{x})) = 1$.

The first condition is equivalent to C being in the ideal generated by $y_1, \ldots, y_m$, and the two conditions together therefore imply that 1 is in the ideal generated by the F_i, and hence that $F_1(\vec{x}) = \cdots = F_m(\vec{x}) = 0$ is unsatisfiable.

An *IPS proof* of the unsatisfiability of the polynomials F_i is an $\mathbb{F}$-algebraic circuit on inputs $x_1, \ldots, x_n, y_1, \ldots, y_m$ computing some IPS certificate of unsatisfiability.

For any class $\mathcal{C}$ of polynomial families, we may speak of $\mathcal{C}$-IPS proofs of a family of systems of equations $(\mathcal{F}_n)$ where $\mathcal{F}_n$ is $F_{n,1}(\vec{x}) = \cdots = F_{n,\mathrm{poly}(n)}(\vec{x}) = 0$. When we refer to IPS without further qualification, we mean VP-IPS, i. e., the family of IPS proofs should be computed by circuits of polynomial size *and polynomial degree*.

The Ideal Proof System is easily shown to be sound; its completeness (without size bounds) follows from the Nullstellensatz.

We typically consider IPS as a propositional proof system by translating a CNF tautology φ into a system of equations in the following standard way. We translate a clause κ of φ into a single algebraic equation $F(\vec{x})$ using $x \mapsto 1 - x$, $x \vee y \mapsto xy$. A $\{0,1\}$-assignment thus satisfies κ if and only if it satisfies the equation $F = 0$. We add to this system of equations the equations $x_i^2 - x_i = 0$, which forces any solutions over $\overline{\mathbb{F}}$ to be $\{0,1\}$-valued.

Like previously defined algebraic systems [18], [19], [20], [21], proofs in our system can be checked in randomized polynomial time. The key difference between our system and previously studied ones is that those systems are axiomatic in the sense that they require that *every* sub-computation (derived polynomial) be in the ideal generated by the original polynomial equations F_i, and thus be a sound consequence of the equations $F_1 = \cdots = F_m = 0$.

In contrast our system has no such requirement; an IPS proof can compute potentially unsound sub-computations (whose vanishing does not follow from $F_1 = \cdots = F_m = 0$), as long as the *final polynomial* is in the ideal generated by the equations. This key difference allows IPS proofs to be *ordinary algebraic circuits*, and thus nearly all results in algebraic circuit complexity apply directly to the Ideal Proof System. To quote the tagline of a common US food chain, IPS is a "No rules, just right" proof system.

Our first main theorem shows one of the advantages of this close connection with algebraic circuits. To the best of our knowledge, this is the first implication showing that a proof complexity lower bound implies any sort of computational complexity lower bound.

Theorem 1. *Super-polynomial lower bounds for the Ideal Proof System imply that the permanent does not have polynomial-size algebraic circuits, that is,* $\mathsf{VNP} \neq \mathsf{VP}$.

The preceding theorem is somewhat unsurprising—though not completely immediate—given the definition of IPS, because of the close connection between the definition of IPS proofs and algebraic circuits. However, the following result is significantly more surprising—showing a relation between a standard rule-based algebraic proof system and algebraic circuit lower bounds—and we believe we would not have come to this result had we not first considered the rule-less Ideal Proof System.

Corollary 1.1. *Super-polynomial lower bounds on the number of lines in Polynomial Calculus proofs imply the Permanent versus Determinant Conjecture.*[1]

Under a reasonable assumption on polynomial identity testing (PIT) we show that Extended Frege is equivalent to the Ideal Proof System (§V). Extended Frege (EF) is the strongest natural deduction-style propositional proof system that has been proposed.

Theorem 2. *Let K be a family of polynomial-size Boolean circuits for PIT such that the PIT axioms for K (see Def. 2) have polynomial-size EF proofs. Then EF p-simulates IPS, and hence EF and IPS are p-equivalent.*

Under this assumption about PIT, Thms. 1 and 2 in combination suggest a precise reason that proving lower bounds on Extended Frege is so difficult, namely, that doing so implies $\mathsf{VP} \neq \mathsf{VNP}$. Thm. 2 also suggests that to make progress toward proving lower bounds in proof complexity, it may be necessary to prove lower bounds for the Ideal Proof System, which we feel is more natural, and creates the possibility of harnessing tools from algebra, representation theory, and algebraic circuit complexity. We give a specific suggestion of how to apply these tools towards proof complexity lower bounds in §VI.

Remark 1. Given that $\mathrm{PIT} \in \mathsf{P}$ is known to imply lower bounds, one may wonder if the combination of the above two theorems really gives any explanation at all for the difficulty of proving lower bounds on Extended Frege. There are at least two reasons that it does.

First, the best lower bound known to follow from $\mathrm{PIT} \in \mathsf{P}$ is an algebraic circuit-size lower bound on an integer polynomial that can be evaluated in $\mathsf{NEXP} \cap \mathsf{coNEXP}$ [5] (via personal communication we have learned that Impagliazzo and Williams have also proved similar results), whereas our conclusion is a lower bound on algebraic circuit-size for an integer polynomial computable in $\#\mathsf{P} \subseteq \mathsf{PSPACE}$.

[1]Although Corollary 1.1 may seem to be saying that lower bounds on PC imply a circuit lower bound, this is not precisely the case, because size complexity in PC is typically measured not by the number of lines, but rather by the total number of monomials appearing in a PC proof.

Second, the hypothesis that our PIT axioms can be proven efficiently in Extended Frege seems to be somewhat orthogonal to, and may be no stronger than, the widely-believed hypothesis that $\mathrm{PIT} \in \mathsf{P}$. As Extended Frege is a nonuniform proof system, efficient Extended Frege proofs of our PIT axioms are unlikely to have any implications about the uniform complexity of PIT (and given that we already know unconditionally that $\mathrm{PIT} \in \mathsf{P/poly}$, uniformity is what the entire question of derandomizing PIT is about). In the opposite direction, it's a well-known observation in proof complexity that nearly all natural uniform polynomial-time algorithms have feasible (Extended Frege) correctness proofs. If this phenomenon doesn't apply to PIT, it would be interesting for both proof complexity and circuit complexity, as it indicates the difficulty of proving that $\mathrm{PIT} \in \mathsf{P}$. $\lhd$

Although PIT has long been a central problem of study in computational complexity—both because of its importance in many algorithms, as well as its strong connection to circuit lower bounds—our theorems highlight the importance of PIT in proof complexity. Next we prove that Thm. 2 can be scaled down to obtain similar results for weaker Frege systems, and discuss some of its more striking consequences.

Theorem 3. *Let $\mathcal{C} \in \{\mathsf{AC}^k, \mathsf{AC}^k[p], \mathsf{ACC}^k, \mathsf{TC}^k, \mathsf{NC}^k | k \geq 0\}$. Let K be a family of polynomial-size Boolean circuits for PIT (not necessarily in $\mathcal{C}$) such that the PIT axioms for K have polynomial-size $\mathcal{C}$-Frege proofs. Then $\mathcal{C}$-Frege is p-equivalent to IPS, and thus to Extended Frege as well.*

Thm. 3 also highlights the importance of our PIT axioms for $\mathsf{AC}^0[p]$-Frege lower bounds, which have been open for nearly thirty years. (For even weaker systems, Thm. 3 in combination with known results yields an unconditional lower bound on AC^0-Frege proofs of the PIT axioms.) In particular, we are in the following win-win scenario:

Corollary 3.1. *For any d, either:*

- *There are polynomial-size $\mathsf{AC}^0[p]$-Frege proofs of the depth-d PIT axioms, in which case* any superpolynomial lower bounds on $\mathsf{AC}^0[p]$-Frege imply $\mathsf{VNP}_{\mathbb{F}_p}$ does not have polynomial-size depth-d algebraic circuits*, thus explaining the difficulty of obtaining such lower bounds, or*
- *There are no polynomial-size $\mathsf{AC}^0[p]$-Frege proofs of the depth-d PIT axioms, in which case we've gotten $\mathsf{AC}^0[p]$-Frege lower bounds.*

Finally, in §VI we suggest a new framework for proving lower bounds for the Ideal Proof System which we feel has promise. Along the way, we make precise the difference in difficulty between proof complexity lower bounds (on IPS, which may also apply to Extended Frege via Thm. 2) and algebraic circuit lower bounds. In particular, the set of *all IPS-certificates* for a given unsatisfiable system of equations is, in a certain precise sense, "finitely generated."

We suggest how one might take advantage of this finite generation to transfer techniques from algebraic circuit complexity to prove lower bounds on IPS, and consequently on Extended Frege (since IPS p-simulates Extended Frege unconditionally), giving hope for the long-sought length-of-proof lower bounds on an algebraic proof system. We hope to pursue this approach in future work.

C. Related Work

We will see in §III-C that many previously studied proof systems can be p-simulated by IPS, and furthermore can be viewed simply as different complexity measures on IPS proofs, or as $\mathcal{C}$-IPS for certain classes $\mathcal{C}$.

Raz and Tzameret [22] introduced various multilinear algebraic proof systems. Although their systems are not so easily defined in terms of IPS, the Ideal Proof System nonetheless p-simulates all of their systems. Amongst other results, they show that a super-polynomial separation between two variants of their system—one representing lines by multilinear circuits, and one representing lines by general algebraic circuits—would imply a super-polynomial separation between general and multilinear circuits computing multilinear polynomials. However, they only get implications to lower bounds on multilinear circuits rather than general circuits, and they do not prove a statement analogous to our Thm. 1, that lower bounds on a single system imply algebraic circuit lower bounds.

D. Outline

In §III we discuss the relationship between IPS and previously studied proof systems. We also highlight several consequences of results on algebraic circuits for IPS, such as division elimination and the chasms at depth 3 and 4. In §IV, we outline the proof that lower bounds on IPS imply algebraic circuit lower bounds (Thm. 1). We also show how this result gives as a corollary a new, simpler proof that $\mathsf{NP} \not\subseteq \mathsf{coMA} \Rightarrow \mathsf{VNP}^0 \neq \mathsf{VP}^0$. In §V we introduce our PIT axioms and outline the proof of Thms. 2 and 3. We also discuss many variants of Thm. 3 and their consequences, as briefly mentioned above. In §VI we suggest a new framework for transferring techniques from algebraic circuit complexity to (algebraic) proof complexity lower bounds. Finally, in §VII we gather some open questions raised by our work, many of which we believe may be quite approachable (the full version [1] contains many more open questions). In appendices to the full version [1], we introduce two variants of the Ideal Proof System—one of which allows certificates to be rational functions and not only polynomials, and one of which has a more geometric flavor—and discuss their relationship to IPS. These systems further suggest that tools from geometry and algebra could potentially be useful for understanding the complexity of various propositional tautologies and more generally the complexity of individual instances of NP-complete problems.

II. A few preliminaries

A. Algebraic Complexity

Over a ring R, VP_R is the class of families $f = (f_n)_{n=1}^{\infty}$ of formal polynomials—i. e., considered as symbolic polynomials, rather than as functions—f_n such that f_n has $\mathrm{poly}(n)$ input variables, is of $\mathrm{poly}(n)$ degree, and can be computed by algebraic circuits over R of $\mathrm{poly}(n)$ size. VNP_R is the class of families g of polynomials g_n such that g_n has $\mathrm{poly}(n)$ input variables and is of $\mathrm{poly}(n)$ degree, and can be written as

$$g_n(x_1, \ldots, x_{\mathrm{poly}(n)}) = \sum_{\vec{e} \in \{0,1\}^{\mathrm{poly}(n)}} f_n(\vec{e}, \vec{x})$$

for some family $(f_n) \in \mathsf{VP}_R$.

A family of algebraic circuits is said to be *constant-free* if the only constants used in the circuit are $\{0, 1, -1\}$. Other constants can only be used by constructing them using algebraic operations, which count towards the size of the circuit. Over a fixed finite field $\mathbb{F}_q$, $\mathsf{VP}^0_{\mathbb{F}_q} = \mathsf{VP}_{\mathbb{F}_q}$ and $\mathsf{VNP}^0_{\mathbb{F}_q} = \mathsf{VNP}_{\mathbb{F}_q}$, since there are only finitely many possible constants. $\mathsf{VP}^0_{\mathbb{Z}}$ coincides with those families in $\mathsf{VP}_{\mathbb{Z}}$ that are computable by algebraic circuits of polynomial total *bit-size* (use the binary expansion of an integer). Similarly, over the algebraic closure $\overline{\mathbb{F}}_p$ of a finite field, $\mathsf{VP}^0_{\overline{\mathbb{F}}_p}$ coincides with those families in $\mathsf{VP}_{\overline{\mathbb{F}}_p}$ that are computable by algebraic circuits of polynomial total bit-size, or equivalently where the constants they use lie in subfields of $\overline{\mathbb{F}}_p$ of total size bounded by $2^{n^{O(1)}}$.

B. Proof Complexity

A *proof system* for a language $L \in \mathsf{coNP}$ is a nondeterministic algorithm for L, or equivalently a deterministic polynomial-time verifier P such that $x \in L \Leftrightarrow (\exists y)[P(x, y) = 1]$, and we refer to any such y as a P-proof that $x \in L$. We say that P is *p-bounded* if for every $x \in L$ there is a P-proof of length polynomially bounded in $|x|$: $|y| \leq \mathrm{poly}(|x|)$. We will generally be considering proof systems for the coNP-complete language TAUT consisting of all propositional tautologies; there is a p-bounded proof system for TAUT if and only if $\mathsf{NP} = \mathsf{coNP}$. Given two proof systems P_1 and P_2 for the same language $L \in \mathsf{coNP}$, we say that P_1 *p-simulates* P_2 if there is a polynomial-time function f such that $P_1(x, y) = 1 \Leftrightarrow P_2(x, f(y)) = 1$. We say that P_1 and P_2 are *p-equivalent* if each p-simulates the other. There are a variety of standard, well-studied propositional proof systems. In this paper, we consider Extended Frege, Frege, AC^0-Frege, and $\mathsf{AC}^0[p]$-Frege systems.

III. Foundational results

A. Relation with coMA

Proposition 4. *For any field $\mathbb{F}$, if every propositional tautology has a polynomial-size constant-free IPS$_{\mathbb{F}}$-proof, then*

$\mathsf{NP} \subseteq \mathsf{coMA}$*, and hence the polynomial hierarchy collapses to its second level.*

If we wish to drop the restriction of "constant-free" (which, recall, is no restriction at all over a finite field), we may do so either by using the Blum–Shub–Smale analogs of NP and coMA using the same proof, or in characteristic zero using the Generalized Riemann Hypothesis [1].

Proof: Merlin nondeterministically guesses the polynomial-size constant-free IPS proof, and then Arthur must check conditions (1) and (2) of Def. 1. (We need constant-free so that the algebraic proof has polynomial bit-size and thus can in fact be guessed by a Boolean Merlin.) Both conditions of Def. 1 are instances of PIT, which can be solved by the standard Schwarz–Zippel–DeMillo–Lipton coRP algorithm. ■

B. Chasms, depth reduction, and other circuit transformations

Since an IPS proof is just a circuit, algebraic circuit depth reductions apply equally well to IPS proof size. We note that it wasn't clear to us how to adapt the proofs of these results to the type of circuits used in the Polynomial Calculus or other previous algebraic systems [21], and indeed this was part of the motivation to move to our more general notion of IPS proof.

Observation 1 (Depth chasms for IPS proofs)**.** If a system of $n^{O(1)}$ polynomial equations in n variables has an IPS proof of unsatisfiability of size s and (semantic) degree d, then it also has:

1) A $O(\log d(\log s + \log d))$-depth IPS proof of size $poly(ds)$ (follows from [23]);
2) A depth 4 IPS formula proof of size $n^{O(\sqrt{d})}$ (follows from [10]) or a depth 4 IPS proof of size $2^{O(\sqrt{d \log(ds) \log n})}$ (follows from [11]).
3) (In characteristic zero) A depth 3 IPS proof of size $2^{O(\sqrt{d \log d \log n \log s})}$ (follows from [24]) or even $2^{O(\sqrt{d \log n \log s})}$ (follows from [11]). ◁

This observation helps explain why size lower bounds for algebraic proofs for the stronger notion of size—number of lines, used here and in Pitassi [20], rather than number of monomials—have been difficult to obtain. This also suggests that size lower bounds for IPS proofs in restricted circuit classes would be interesting, even for restricted kinds of depth 3 circuits.

Similarly, since IPS proofs are just circuits, any IPS certificate family of polynomially bounded degree that is computed by a polynomial-size family of algebraic circuits with divisions can also be computed by a polynomial-size family of algebraic circuits without divisions (follows from Strassen [25]). We note, however, that one could in principle consider IPS certificates that were not merely polynomials, but even rational functions, under suitable conditions; divisions for computing these cannot always be eliminated. We discuss this "Rational Ideal Proof System," the exact conditions needed, and when such divisions can be effectively eliminated in the full version [1].

C. Simulations and definitions of other algebraic proof systems in terms of IPS

Previously studied algebraic proof systems can be viewed as particular complexity measures on the Ideal Proof System, including the Polynomial Calculus (or Gröbner) proof system (PC) [19], Polynomial Calculus with Resolution (PCR) [26], the Nullstellensatz proof system [18], and Pitassi's algebraic systems [20], [21], as we explain below.

Before explaining these, we note that although the Nullstellensatz says that if $F_1(\vec{x}) = \cdots = F_m(\vec{x}) = 0$ is unsatisfiable then there always exists a certificate that is linear in the y_i—that is, of the form $\sum y_i G_i(\vec{x})$—our definition of IPS certificate does not enforce $\vec{y}$-linearity. The definition of IPS certificate allows certificates with $\vec{y}$-monomials of higher degree, and it is conceivable that one could achieve a savings in size by considering such certificates rather than only considering $\vec{y}$-linear ones. As the linear form is closer to the original way Hilbert expressed the Nullstellensatz, we refer to certificates of the form $\sum y_i G_i(\vec{x})$ as *Hilbert-like IPS certificates*.

Using multivariate polynomial interpolation we are able to show:

Proposition 5. *Let $F_1 = \cdots = F_m = 0$ be a polynomial system of equations in n variables $x_1, \ldots, x_n$ and let $C(\vec{x}, \vec{y})$ be an IPS-certificate of the unsatisfiability of this system. Let $D = \max_i \deg_{y_i} C$ and let t be the number of terms of C, when viewed as a polynomial in the y_i with coefficients in $\mathbb{F}[\vec{x}]$. Suppose C and each F_i can be computed by a circuit of size $\leq s$. Then a Hilbert-like IPS-certificate for this system can be computed by a circuit of size $poly(D, t, n, s)$.*[2]

We note that all known multivariate interpolation algorithms only give limited control on the *depth* of the resulting Hilbert-like IPS-certificate (as a function of the depth of the original IPS-certificate f), because they all involve solving linear systems of equations, which is not known to be computable efficiently in constant depth.

All of the previous algebraic proof systems are rule-based systems, in that they syntactically enforce the condition that every line of the proof is a polynomial in the ideal of the original polynomials $F_1(\vec{x}), \ldots, F_m(\vec{x})$. Typically they do this by allowing two derivation rules: 1) from G and H, derive $\alpha G + \beta H$ for α, β constants, and 2) from G, derive Gx_i for any variable x_i. By "rule-based circuits" we mean circuits with inputs $y_1, \ldots, y_m$ having linear combination

[2]If the base field $\mathbb{F}$ has size less than $T = Dt\binom{n}{2}$, and the original circuit had multiplication gates of fan-in bounded by k, then the size of the resulting Hilbert-like certificate should be multiplied by $(\log T)^k$.

gates and, for each $i = 1, \ldots, n$, gates that multiply their input by x_i. In particular, rule-based circuits necessarily produce Hilbert-like certificates.

Now we define previous algebraic proof systems in terms of complexity measures on the Ideal Proof System:

- Degree in the Nullstellensatz proof system is simply the minimal degree of any Hilbert-like certificate.
- Polynomial Calculus (PC) size is the sum of the (semantic) number of monomials at each gate in $C(\vec{x}, \vec{F}(\vec{x}))$, where C ranges over rule-based circuits.
- PC degree is the minimum over rule-based circuits $C(\vec{x}, \vec{y})$ of the maximum semantic degree at any gate in $C(\vec{x}, \vec{F}(\vec{x}))$.
- Pitassi's 1998 algebraic proof system [21] is essentially PC, except where size is measured by number of lines of the proof (rather than total number of monomials appearing). This corresponds exactly to the smallest size of any rule-based circuit $C(\vec{x}, \vec{y})$ computing any Hilbert-like IPS certificate.
- Polynomial Calculus with Resolution (PCR) [26] also allows variables $\overline{x}_i$ and adds the equations $\overline{x}_i = 1 - x_i$ and $x_i\overline{x}_i = 0$. This is easily accommodated into the Ideal Proof System: add the $\overline{x}_i$ as new variables, with the same restrictions as are placed on the x_i's in a rule-based circuit, and add the polynomials $\overline{x}_i - 1 + x_i$ and $x_i\overline{x}_i$ to the list of equations F_i. Note that while this may have an effect on the PC size as it can decrease the total number of monomials needed, it has essentially no effect on the number of lines of the proof.

The following proposition allows us to extend the connection with algebraic circuit complexity lower bounds from IPS to the number of lines in Polynomial Calculus proofs.

Theorem 6. *Pitassi's 1996 algebraic proof system [20] is p-equivalent to Hilbert-like IPS.*

Pitassi's 1998 algebraic proof system [21]—equivalent to the number-of-lines measure on PC proofs—is p-equivalent to Hilbert-like $\det$*-IPS or* VP_{ws}*-IPS.*

Combining Thm. 6 with the techniques used in Thm. 1 shows that super-polynomial lower bounds on the number of lines in PC proofs would positively resolve the Permanent Versus Determinant Conjecture (Cor. 1.1), explaining the difficulty of such proof complexity lower bounds.

In light of this proposition, we henceforth refer to the systems from [20] and [21] as Hilbert-like IPS and Hilbert-like $\det$-IPS, respectively. Pitassi [20, Theorem 1] showed that Hilbert-like IPS p-simulates Polynomial Calculus and Frege. Essentially the same proof shows that Hilbert-like IPS p-simulates Extended Frege as well.

Unfortunately, the proof of the simulation in [20] does not seem to generalize to a depth-preserving simulation, which we show is nonetheless possible:

Theorem 7. *For any $d(n)$, depth-$(d+2)$ $\mathrm{IPS}_{\mathbb{F}_p}$ p-simulates depth-d Frege proofs with unbounded fan-in $\vee, \wedge, MOD_p$ connectives (for $d = O(1)$, this is $\mathsf{AC}^0_d[p]$-Frege).*

IV. IPS lower bounds imply circuit lower bounds

Theorem 1. *A super-polynomial lower bound on [constant-free] Hilbert-like IPS_R proofs of any family of tautologies implies $\mathsf{VNP}_R \neq \mathsf{VP}_R$ [respectively, $\mathsf{VNP}^0_R \neq \mathsf{VP}^0_R$], for any ring R.*

A super-polynomial lower bound on the number of lines in Polynomial Calculus proofs implies the Permanent versus Determinant Conjecture ($\mathsf{VNP} \neq \mathsf{VP}_{ws}$*).*

Together with Prop. 4, this immediately gives an alternative, and we believe simpler, proof of the following:

Corollary 1.2. *If* $\mathsf{NP} \not\subseteq \mathsf{coMA}$*, then* $\mathsf{VNP}^0_R \neq \mathsf{VP}^0_R$*, for any ring R.*

The previous proofs we are aware of all depend crucially on the random self-reducibility of the permanent or of some function complete for $\mathsf{Mod}_p\mathsf{P}/\mathsf{poly}$ In contrast, our proof is quite different, in that it avoids random self-reduciblity altogether: indeed, we do not even know if there exist tautologies and a choice of ordering of the clauses such that the VNP-IPS certificates of Lem. 1.1 are random self-reducible.

The following lemma is the key to Thm. 1. (Thm. 6 is needed for the second part.)

Lemma 1.1. *Every family of CNF tautologies (φ_n) has a Hilbert-like family of IPS certificates (C_n) in* VNP^0_R*.*

V. PIT as a bridge between circuit complexity and proof complexity

In this section we state our PIT axioms and give an outline of the proof of Thms. 2 and 3, which say that Extended Frege (EF) (resp., AC^0- or $\mathsf{AC}^0[p]$-Frege) is p-equivalent to the IPS if there are polynomial-size circuits for PIT whose correctness—suitably formulated—can be efficiently proved in EF (resp., AC^0- or $\mathsf{AC}^0[p]$-Frege).

More precisely, we identify a small set of natural axioms for PIT and show that if these axioms can be proven efficiently in EF, then EF is p-equivalent to IPS. Thm. 3 begins to explain why $\mathsf{AC}^0[p]$-Frege lower bounds have been so difficult to obtain, and highlights the importance of our PIT axioms for $\mathsf{AC}^0[p]$-Frege lower bounds. We begin by describing and discussing these axioms.

Fix some standard Boolean encoding of constant-free algebraic circuits, so that the encoding of any size-m constant-free algebraic circuit has size $\mathrm{poly}(m)$. We use "$[C]$" to denote the encoding of the algebraic circuit C. Let $K = \{K_{m,n}\}$ denote a family of Boolean circuits solving PIT: $K_{m,n}$ is a Boolean function that takes as input the encoding of a size-m constant-free algebraic circuit, C, over variables $x_1, \ldots, x_n$, and if C has polynomial degree, then K outputs 1 if and only if the polynomial computed by C is the 0 polynomial.

Notational convention: We underline parts of a statement that involve propositional variables. For example, if in a propositional statement we write "$[C]$", this refers to a fixed Boolean string that is encoding the (fixed) algebraic circuit C. In contrast, if we write $\underline{[C]}$, this denotes a Boolean string *of propositional variables*, which is to be interpreted as a description of an as-yet-unspecified algebraic circuit C; any setting of the propositional variables corresponds to a particular algebraic circuit C. Throughout, we use $\vec{p}$ and $\vec{q}$ to denote propositional variables (which we do not bother underlining except when needed for emphasis), and $\vec{x}, \vec{y}, \vec{z}, \ldots$ to denote the algebraic variables that are the inputs to algebraic circuits. Thus, $C(\vec{x})$ is an algebraic circuit with inputs $\vec{x}$, $[C(\vec{x})]$ is a fixed Boolean string encoding some particular algebraic circuit C, $\underline{[C(\vec{x})]}$ is a string of propositional variables encoding an unspecified algebraic circuit C, and $[C(\vec{p})]$ denotes a Boolean string together with propositional variables $\vec{p}$ that describes a fixed algebraic circuit C whose inputs have been set to the propositional variables $\vec{p}$.

Definition 2. Our PIT axioms for a Boolean circuit K are as follows.

1) The first axiom states that if C is a circuit computing the identically 0 polynomial, then the polynomial evaluates to 0 on all Boolean inputs.
$$K(\underline{[C(\vec{x})]}) \to K(\underline{[C(\vec{p})]})$$
2) The second axiom states that if C is a circuit computing the zero polynomial, then the circuit $1 - C$ does not compute the zero polynomial.
$$K(\underline{[C(\vec{x})]}) \to \neg K(\underline{[1 - C(\vec{x})]})$$
3) The third axiom states that PIT circuits respect certain substitutions. More specifically, if the polynomial computed by circuit G is 0, then G can be substituted for the constant 0.
$$K(\underline{[G(\vec{x})]}) \wedge K(\underline{[C(\vec{x}, 0)]}) \to K(\underline{[C(\vec{x}, G(\vec{x}))]})$$
4) The last axiom states that PIT is closed under permutations of the (algebraic) variables.
$$K(\underline{[C(\vec{x})]}) \to K(\underline{[C(\pi(\vec{x}))]})$$

We can now state and discuss two of our main theorems.

Theorem 2. *If there is a family K of polynomial-size Boolean circuits that correctly compute PIT, such that the PIT axioms for K have polynomial-size EF proofs, then EF is polynomially equivalent to IPS.*

Note that the issue is not the existence of small circuits for PIT since we would be happy with nonuniform polynomial-size PIT circuits, which do exist. Unfortunately the known constructions are highly nonuniform—they involve picking uniformly random points—and we do not see how to prove the above axioms for these constructions. Nonetheless, it seems very plausible to us that there exists a polynomial-size family of PIT circuits where the above axioms are efficiently provable in EF, especially in light of Remark 1.

Our next main result shows that the previous result can be scaled down to much weaker proof systems than EF.

Theorem 3. *Let $\mathcal{C}$ be any class of circuits closed under AC^0 circuit reductions. If there is a family K of polynomial-size Boolean circuits computing PIT such that the PIT axioms for K have polynomial-size $\mathcal{C}$-Frege proofs, then $\mathcal{C}$-Frege is polynomially equivalent to IPS, and consequently polynomially equivalent to Extended Frege.*

Note that here we *do not* need to restrict the circuit family K to be in the class $\mathcal{C}$. This requires one more (standard) technical device compared to the proof of Thm. 2, namely the use of auxiliary variables for the gates of K. Here we discuss some corollaries of Thm. 3; the proof of Thm. 3 is given in the full version [1].

As AC^0 is known unconditionally to be strictly weaker than Extended Frege, we immediately get that AC^0-Frege cannot efficiently prove the PIT axioms for any Boolean circuit family K correctly computing PIT.

Using essentially the same proof as Thm. 3, we also get the following result. By "depth-d PIT axioms" we mean a variant where the algebraic circuits C (encoded as $[C]$ in the statement of the axioms) have depth at most d. Note that, even over finite fields, super-polynomial lower bounds on depth-d algebraic circuits are notoriously open problems even for d as small as 4 or 5.[3]

Corollary 3.1. *For any d, if there is a family of tautologies with no polynomial-size $\mathsf{AC}^0[p]$-Frege proof, and $\mathsf{AC}^0[p]$-Frege has polynomial-size proofs of the [depth-d] PIT axioms for some K, then $\mathsf{VNP}_{\mathbb{F}_p}$ does not have polynomial-size [depth-d] algebraic circuits.*

This corollary makes the following question of central importance in getting lower bounds on $\mathsf{AC}^0[p]$-Frege:

Open Question 1. For some $d \geq 4$, is there some K computing depth-d PIT, for which the depth-d PIT axioms have $\mathsf{AC}^0[p]$-Frege proofs of polynomial size?

This question has the virtue that answering it either way is highly interesting:

- If $\mathsf{AC}^0[p]$-Frege does not have polynomial-size proofs of the [depth-d] PIT axioms for any K, then we have super-polynomial size lower bounds on $\mathsf{AC}^0[p]$-Frege, answering a major open question.

[3]Lower bounds of $2^{\Omega(\sqrt{n}\log n)}$ on *homogeneous* depth 4 circuits are known [27], [28]—and furthermore *any* asymptotic improvement to these lower bounds implies $\mathsf{VP} \neq \mathsf{VNP}$ [11]—but for unrestricted depth 4 algebraic circuits nothing better than Strassen's degree bound of $\Omega(n \log n)$ is known [7]. The only lower bounds for depth 5 circuits, beyond Strassen's degree bound, are for a very restricted class of circuits, namely, homogeneous depth 5 circuits of bottom fan-in bounded by N^{δ} with $\delta < 1$ [29].

- Otherwise, super-polynomial size lower bounds on $\mathsf{AC}^0[p]$-Frege imply that the permanent does not have polynomial-size algebraic circuits [of depth d] over any finite field of characteristic p. This would then explain why getting superpolynomial lower bounds on $\mathsf{AC}^0[p]$-Frege has been so difficult.

This dichotomy is in some sense like a "completeness result for $\mathsf{AC}^0[p]$-Frege, modulo proving strong algebraic circuit lower bounds on VNP": if one hopes to prove $\mathsf{AC}^0[p]$-Frege lower bounds *without proving* strong lower bounds on VNP, then one must prove $\mathsf{AC}^0[p]$-Frege lower bounds on the PIT axioms. For example, if you believe that proving $\mathsf{VP} \neq \mathsf{VNP}$ [or that proving VNP does not have bounded-depth polynomial-size circuits] is very difficult, and that proving $\mathsf{AC}^0[p]$-Frege lower bounds is comparatively easy, then to be consistent you must also believe that proving $\mathsf{AC}^0[p]$-Frege lower bounds *on the [bounded-depth] PIT axioms* is easy.

Similarly, along with Thm. 7, we get the following:

Corollary 3.2. *If for every constant d, there is a constant d' such that the depth-d PIT axioms have polynomial-size depth-d' $\mathsf{AC}^0_{d'}[p]$-Frege proofs, then $\mathsf{AC}^0[p]$-Frege is p-equivalent to constant-depth IPS$_{\mathbb{F}_p}$.*

Using the chasms at depth 3 and 4 for algebraic circuits [9], [10], [11] (see Observation 1 above), we can also help explain why sufficiently strong exponential lower bounds for AC^0-Frege—that is, lower bounds that don't depend on the depth, or don't depend so badly on the depth, which have also been open for nearly thirty years—have been difficult to obtain:

Corollary 3.3. *Let $\mathbb{F}$ be any field, and let c be a sufficiently large constant. If there is a family of tautologies (φ_n) such that any AC^0-Frege proof of φ_n has size at least $2^{c\sqrt{n}\log n}$, and AC^0-Frege has polynomial-size proofs of the depth-4 PIT$_{\mathbb{F}}$ axioms for some K, then $\mathsf{VP}^0_{\mathbb{F}} \neq \mathsf{VNP}^0_{\mathbb{F}}$.*

If $\mathbb{F}$ has characteristic zero, we may replace "depth 4" above with "depth 3."

As with Corollary 3.1, we conclude a similar dichotomy: either AC^0-Frege can efficiently prove the depth 4 PIT axioms (depth 3 in characteristic zero), or proving $2^{\omega(\sqrt{n}\log n)}$ lower bounds on AC^0-Frege implies $\mathsf{VP}^0 \neq \mathsf{VNP}^0$.

VI. Towards lower bounds

Thm. 1 shows that proving lower bounds on (Hilbert-like) IPS, or on the number of lines in Polynomial Calculus proofs, is at least as hard as proving algebraic circuit lower bounds. In this section we begin to make the difference between proof complexity lower bounds and circuit lower bounds more precise, and use this precision to suggest a direction for proving new proof complexity lower bounds, aimed at proving the long-sought length-of-proof lower bounds on an algebraic proof system.

The key fact we use is embodied in Lem. 1, which says that the set of (Hilbert-like) certificates for a given unsatisfiable system of equations is, in a precise sense, "finitely generated." The basic idea is then to leverage this finite generation to extend lower bound techniques from individual polynomials to entire "finitely generated" sets of polynomials.

Because Hilbert-like certificates are somewhat simpler to deal with, we focus on those here, but note that all our key conclusions about Hilbert-like certificates will also apply to general IPS certificates [1].

The algebraic circuit size of a Hilbert-like certificate $C = \sum_i G_i(\vec{x})y_i$ is equivalent to the algebraic circuit size of computing the entire tuple $(G_1(\vec{x}), \ldots, G_m(\vec{x}))$. A circuit computing the tuple can be converted to a circuit computing C by adding m times gates and a single plus gate. Conversely, for each i we can recover $G_i(\vec{x})$ from $C(\vec{x}, \vec{y})$ by plugging in 0 for all y_j with $j \neq i$ and 1 for y_i. So from the point of view of lower bounds, we may consider Hilbert-like certificates, and their representation as tuples, essentially without loss of generality. This holds even in the setting of Hilbert-like depth 3 IPS-proofs.

Hilbert-like IPS-certificates are thus in bijective correspondence with $R[\vec{x}]$ solutions to the following $R[\vec{x}]$-linear equation in the new variables g_i:

$$\begin{pmatrix} F_1(\vec{x}) & \cdots & F_m(\vec{x}) \end{pmatrix} \begin{pmatrix} g_1 & \cdots & g_m \end{pmatrix}^T = 1$$

Just as in linear algebra over a field, the set of such solutions can be described by taking one solution and adding to it all solutions to the associated homogeneous equation:

$$\begin{pmatrix} F_1(\vec{x}) & \cdots & F_m(\vec{x}) \end{pmatrix} \begin{pmatrix} g_1 & \cdots & g_m \end{pmatrix}^T = 0 \quad (1)$$

(To see why: given two solutions of the inhomogeneous equation, consider their difference.) Solutions to the latter equation are commonly called "syzygies" amongst the F_i. Syzygies and their properties are well-studied—though not always well-understood—in commutative algebra and algebraic geometry, so lower and upper bounds on Hilbert-like IPS-proofs may benefit from known results in algebra and geometry.

Lemma 1. *Given unsatisfiable polynomial equations $F_1(\vec{x}) = \cdots = F_m(\vec{x}) = 0$ over a Noetherian ring R (such as a field or $\mathbb{Z}$), the set of Hilbert-like IPS-certificates is a coset of a finitely generated submodule of $R[\vec{x}]^m$.*

Proof: The discussion above shows that the set of Hilbert-like certificates is a coset of a $R[\vec{x}]$-submodule of $R[\vec{x}]^m$, namely the solutions to (1). As R is a Noetherian ring, so is $R[\vec{x}]$ (by Hilbert's Basis Theorem). Thus $R[\vec{x}]^m$ is a Noetherian $R[\vec{x}]$-module, and hence every submodule of it is finitely generated. ∎

Lem. 1 seems such an important idea that it's worth restating:

The set of all Hilbert-like IPS-certificates for a given system of equations can be described by a single Hilbert-like IPS-certificate and a finite generating set for the syzygies.

Its importance is underscored by contrasting the preceding statement with the structure (if any?) of the set of all proofs in other proof systems, particularly non-algebraic ones.

Note that a finite generating set for the syzygies (even a Gröbner basis) can be found in the process of computing a Gröbner basis for the $R[\vec{x}]$-ideal $\langle F_1(\vec{x}), \ldots, F_m(\vec{x})\rangle$. This process is to Buchberger's algorithm as the extended Euclidean algorithm is to the usual Euclidean algorithm.

Lem. 1 suggests that one might be able to prove size lower bounds on Hilbert-like-IPS along the following lines: 1) find a single family of Hilbert-like IPS-certificates $(G_n)_{n=1}^{\infty}$, $G_n = \sum_{i=1}^{\mathrm{poly}(n)} y_i G_i(\vec{x})$ (one for each input size n), 2) use your favorite algebraic circuit lower bound technique to prove a lower bound on the polynomial family G, 3) find a (hopefully nice) generating set for the syzygies, and 4) show that when adding to G any $R[\vec{x}]$-linear combinations of the generators of the syzygies, whatever useful property was used in the lower bound on G still holds. Although this indeed seems significantly more difficult than proving a single algebraic circuit complexity lower bound, it at least suggests a recipe for proving lower bounds on Hilbert-like IPS (and its subsystems such as homogeneous depth 3, depth 4, multilinear, etc.), which should be contrasted with the difficulty of transferring lower bounds for a circuit class to lower bounds on previous related proof systems.

This entire discussion also applies to general IPS-certificates, with only slight modifications [1].

VII. Summary and open questions

The Ideal Proof System raises many new questions, not only about itself, but also about PIT, new examples of VNP functions coming from propositional tautologies, and the complexity of ideals or modules of polynomials. In particular, it motivates the following general question:

General Question 2. Given a family of cosets of ideals $f_n^{(0)} + I_n$ (or more generally modules) of polynomials, with $I_n \subseteq R[x_1, \ldots, x_{\mathrm{poly}(n)}]$, consider the function families $(f_n) \in (f_n^{(0)} + I_n)$ (meaning that $f_n \in f_n^{(0)} + I_n$ for all n) under any computational reducibility $\leq$ such as p-projections. What can the $\leq$ structure look like? When, if ever, is there such a unique $\leq$-minimum (even a single nontrivial example would be interesting)? Can there be infinitely many incomparable $\leq$-minima?

Say a $\leq$-degree $\mathbf{d}$ is "saturated" in $(f_n^{(0)} + I_n)$ if every degree $\mathbf{d}' \geq \mathbf{d}$ has some representative in $f^{(0)} + I$. Must saturated degrees always exist? We suspect yes, given that one may multiply any element of I by arbitrarily complex polynomials. What can the set of saturated degrees look like for a given $(f_n^{(0)} + I_n)$? Must every $\leq$-degree in $f^{(0)} + I$ be *below* some saturated degree? What can the $\leq$-structure of $f^{(0)} + I$ look like below a saturated degree?

Question 2 is of interest even when $f^{(0)} = 0$, i. e., for ideals and modules of functions rather than their nontrivial cosets.

The complexity of Gröbner basis computations obviously depends on the degrees and the number of polynomials that one starts with. From this point of view, Mayr and Meyer [30] showed that the doubly-exponential upper bound on the degree of a Gröbner basis could not be improved in general. However, in practice many Gröbner basis computations seem to work much more efficiently, and even theoretically many classes of instances—such as proving that 1 is in a given ideal—can be shown to have only a singly-exponential degree upper bound. These points of view are reconciled by the more refined measure of the (Castelnuovo–Mumford) *regularity* of an ideal or module [31]. Given that the syzygy module or ideal of zero-certificates are so crucial to the complexity of IPS-certificates, and the tight connection between these modules/ideals and the computation of the Gröbner basis of the ideal one started with, we ask:

General Question 3. Is there a formal connection between the proof complexity of individual instances of TAUT (in, say, the Ideal Proof System), and the Castelnuovo–Mumford regularity of the corresponding syzygy module or ideal of zero-certificates?

Prior to our work, much work was done on bounds for the Ideal Membership Problem. The viewpoint afforded by the Ideal Proof Systems raises new questions about potential strengthening of these results. In particular, the following is a natural extension of Def. 1.

Definition 3. An *IPS certificate* that a polynomial $G(\vec{x}) \in \mathbb{F}[\vec{x}]$ is in the ideal [respectively, radical of the ideal] generated by $F_1(\vec{x}), \ldots, F_m(\vec{x})$ is a polynomial $C(\vec{x}, \vec{y})$ such that

1) $C(\vec{x}, \vec{0}) = 0$, and
2) $C(\vec{x}, F_1(\vec{x}), \ldots, F_m(\vec{x})) = G(\vec{x})$ [respectively, $G(\vec{x})^k$ for any $k > 0$].

An *IPS derivation* of G from $F_1, \ldots, F_m$ is a circuit computing some IPS certificate that $G \in \langle F_1, \ldots, F_m\rangle$.

For the Ideal Membership Problem, known EXPSPACE lower bounds [30] imply a subexponential-size lower bound on constant-free circuits computing IPS-certificates of ideal membership (or non-constant-free circuits in characteristic zero, assuming GRH, see the full version [1]). However, under special circumstances, one may be able to achieve better upper bounds; for the effective Nullstellensatz and its arithmetic variant, we leave the following open:

Open Question 4. For any $G, F_1, \ldots, F_m$ on $x_1, \ldots, x_n$, is there always an IPS-certificate of subexponential size that G is in the *radical* of $\langle F_1, \ldots, F_m\rangle$ (see Def. 3)? Similarly,

if $G, F_1, \ldots, F_m \in \mathbb{Z}[x_1, \ldots, x_n]$ is there a constant-free $\mathrm{IPS}_{\mathbb{Z}}$-certificate of subexponential size that $aG(\vec{x})$ is in the *radical* of the ideal $\langle F_1, \ldots, F_m \rangle$ for some integer a?

ACKNOWLEDGMENT

We are grateful to the following people for many interesting discussions, questions and comments: Eric Allender, Andy Drucker, Pascal Koiran, David Liu and Iddo Tzameret.

REFERENCES

[1] J. A. Grochow and T. Pitassi, "Circuit complexity, proof complexity and polynomial identity testing," ECCC Tech. Report TR14-052 and arXiv:1404.3820 [cs.CC], 2014.

[2] L. G. Valiant, "Completeness classes in algebra," in *STOC '79*. ACM, 1979, pp. 249–261.

[3] V. Kabanets and R. Impagliazzo, "Derandomizing polynomial identity tests means proving circuit lower bounds," *Comput. Complexity*, vol. 13, no. 1-2, pp. 1–46, 2004.

[4] P. Bürgisser, "Cook's versus Valiant's hypothesis," *Theoret. Comput. Sci.*, vol. 235, no. 1, pp. 71–88, 2000.

[5] M. Jansen and R. Santhanam, "Stronger lower bounds and randomness-hardness trade-offs using associated algebraic complexity classes," in *STACS '12*. Schloss Dagstuhl., 2012, vol. 14, pp. 519–530.

[6] K. D. Mulmuley, "The GCT program toward the P vs. NP problem," *CACM*, vol. 55, no. 6, pp. 98–107, Jun. 2012.

[7] V. Strassen, "Die Berechnungskomplexität von elementarsymmetrischen Funktionen und von Interpolationskoeffizienten," *Numer. Math.*, vol. 20, pp. 238–251, 1972/73.

[8] W. Baur and V. Strassen, "The complexity of partial derivatives," *Theoret. Comput. Sci.*, vol. 22, no. 3, pp. 317–330, 1983.

[9] M. Agrawal and V. Vinay, "Arithmetic circuits: A chasm at depth four," in *FOCS '08*. IEEE, 2008, pp. 67–75.

[10] P. Koiran, "Arithmetic circuits: the chasm at depth four gets wider," *Theoret. Comput. Sci.*, vol. 448, pp. 56–65, 2012.

[11] S. Tavenas, "Improved bounds for reduction to depth 4 and depth 3," in *MFCS '13*, ser. Springer LNCS, 2013, vol. 8087, pp. 813–824.

[12] R. Smolensky, "Algebraic methods in the theory of lower bounds for Boolean circuit complexity," in *STOC '87*. ACM, 1987, pp. 77–82.

[13] T. Baker, J. Gill, and R. Solovay, "Relativizations of the P =? NP question," *SIAM J. Comput*, vol. 4, pp. 431–442, 1975.

[14] A. A. Razborov and S. Rudich, "Natural proofs," *J. Comput. System Sci.*, vol. 55, no. 1, part 1, pp. 24–35, 1997.

[15] S. Aaronson and A. Wigderson, "Algebrization: a new barrier in complexity theory," in *STOC '08*. ACM, 2008, pp. 731–740.

[16] M. L. Bonet, T. Pitassi, and R. Raz, "On interpolation and automatization for Frege systems," *SIAM J. Comput*, vol. 29, no. 6, pp. 1939–1967, 2000.

[17] M. L. Bonet, C. Domingo, R. Gavaldà, A. Maciel, and T. Pitassi, "Non-automatizability of bounded-depth Frege proofs," *Comput. Complexity*, vol. 13, no. 1-2, pp. 47–68, 2004.

[18] P. Beame, R. Impagliazzo, J. Krajíček, T. Pitassi, and P. Pudlák, "Lower bounds on Hilbert's Nullstellensatz and propositional proofs," *Proc. LMS (3)*, vol. 73, no. 1, pp. 1–26, 1996.

[19] M. Clegg, J. Edmonds, and R. Impagliazzo, "Using the Groebner basis algorithm to find proofs of unsatisfiability," in *STOC '96*. ACM, 1996, pp. 174–183.

[20] T. Pitassi, "Algebraic propositional proof systems," ser. DIMACS series in Discrete Math and TCS, vol. 31. AMS, 1996, pp. 215–244.

[21] ——, "Propositional proof complexity and unsolvability of polynomial equations," in *Proc. ICM. Vol. III.*, 1998, pp. 215–244.

[22] R. Raz and I. Tzameret, "The strength of multilinear proofs," *Comput. Complexity*, vol. 17, no. 3, pp. 407–457, 2008.

[23] L. G. Valiant, S. Skyum, S. Berkowitz, and C. Rackoff, "Fast parallel computation of polynomials using few processors," *SIAM J. Comput*, vol. 12, no. 4, pp. 641–644, 1983.

[24] A. Gupta, P. Kamath, N. Kayal, and R. Saptharishi, "Arithmetic circuits: A chasm at depth three," in *FOCS '13*, 2013.

[25] V. Strassen, "Vermeidung von Divisionen," *J. Reine Angew. Math.*, vol. 264, pp. 184–202, 1973.

[26] M. Alekhnovich, E. Ben-Sasson, A. A. Razborov, and A. Wigderson, "Space complexity in propositional calculus," *SIAM J. Comput*, vol. 31, no. 4, pp. 1184–1211, 2002.

[27] M. Kumar and S. Saraf, "On the power of homogeneous depth 4 arithmetic circuits," in *FOCS '14*, 2014, arXiv:1404.1950 [cs.CC] and ECCC TR14-045.

[28] N. Kayal, N. Limaye, C. Saha, and S. Srinivasan, "An exponential lower bound for homogeneous depth four arithmetic formulas," in *FOCS '14*, 2014, ECCC TR14-005.

[29] N. Kayal and C. Saha, "Lower bounds for depth three arithmetic circuits with small bottom fanin," ECCC Tech. Report TR14-089, 2014.

[30] E. W. Mayr and A. R. Meyer, "The complexity of the word problems for commutative semigroups and polynomial ideals," *Adv. in Math.*, vol. 46, no. 3, pp. 305–329, 1982.

[31] D. Bayer and D. Mumford, "What can be computed in algebraic geometry?" in *Computational algebraic geometry and commutative algebra (Cortona, 1991)*, ser. Sympos. Math., XXXIV. Cambridge Univ. Press, Cambridge, 1993, pp. 1–48, preprint available as arXiv:alg-geom/9304003.