The Proof Complexity of Polynomial Identities

Pavel Hrubeš*
School of Mathematics
Institute for Advanced Study
Princeton, NJ, USA
pahrubes@centrum.cz

Iddo Tzameret†
Mathematical Institute
Academy of Sciences of the Czech Rep.
Prague, Czech Rep.
tzameret@math.cas.cz

Abstract

Devising an efficient deterministic – or even a non-deterministic sub-exponential time – algorithm for testing polynomial identities is a fundamental problem in algebraic complexity and complexity at large. Motivated by this problem, as well as by results from proof complexity, we investigate the complexity of proving *polynomial identities. To this end, we study a class of equational proof systems, of varying strength, operating with polynomial identities written as arithmetic formulas over a given ring. A proof in these systems establishes that two arithmetic formulas compute the same polynomial, and consists of a sequence of equations between polynomials, written as arithmetic formulas, where each equation in the sequence is derived from previous equations by means of* the polynomial-ring axioms*. We establish the first non-trivial upper and lower bounds on the size of equational proofs of polynomial identities, as follows:*

1) *Polynomial-size upper bounds on equational proofs of identities involving symmetric polynomials and interpolation-based identities. In particular, we show that basic properties of the elementary symmetric polynomials are efficiently provable already in equational proofs operating with depth-4 formulas, over infinite fields. This also yields polynomial-size depth-4 proofs of the Newton identities, providing a positive answer to a question posed by Grigoriev and Hirsch [6].*
2) *Exponential-size lower bounds on (full, unrestricted) equational proofs of identities over certain specific rings.*
3) *Exponential-size lower bounds on analytic proofs operating with depth-3 formulas, under a certain regularity condition. The "analytic" requirement is, roughly, a condition that forbids introducing arbitrary formulas in a proof and the regularity condition is an additional structural restriction.*
4) *Exponential-size lower bounds on one-way proofs (of unrestricted depth) over infinite fields. Here,* one-way proofs *are analytic proofs, in which one is also not allowed to introduce arbitrary constants.*

Furthermore, we determine basic structural characterizations of equational proofs, and consider relations with polynomial identity testing procedures. Specifically, we show that equational proofs efficiently simulate the polynomial identity testing algorithm provided by Dvir and Shpilka [4].

1. Introduction

Let $\mathbb{F}$ be a field (say, the complex numbers) and let Φ be an arithmetic formula in the input variables $x_1, \ldots, x_n$, computing a polynomial in the ring of polynomials $\mathbb{F}[x_1, \ldots, x_n]$. An *elementary operation* is any transformation of a subformula in Φ into another subformula, by means of the standard polynomial-ring axioms (expressing associativity and commutativity of addition and multiplication, distributivity of multiplication over addition, field element equalities and the laws for the 0 and 1 elements in the field). This paper is centered around the following question:

> WHAT IS THE MINIMAL NUMBER OF ELEMENTARY OPERATIONS ONE NEEDS TO PERFORM ON Φ IN ORDER TO VALIDATE THAT Φ COMPUTES THE ZERO POLYNOMIAL?

To deal with this and related problems, we introduce a family of *equational proof systems*, which are proof systems operating with equations between arithmetic formulas over rings (and fields). Specifically, assume that the arithmetic formulas Φ_1, Φ_2 compute the same polynomial in $\mathbb{F}[x_1, \ldots, x_n]$. An *equational proof* of $\Phi_1 = \Phi_2$ is a sequence of equations, terminating with the equation $\Phi_1 = \Phi_2$, starting from polynomial-ring axioms, and identities like $\varphi = \varphi$, and such that every other identity in the sequence is derived from previous ones by simple rules, expressing basic (logical) properties of equalities.

The purpose of this paper is, first, to argue that the study of the complexity of proofs establishing polynomial identities deserves deep attention and is an issue relevant to both algebraic complexity and proof complexity; second, to

*Supported by NSF grant CCF 0832797.
†*Supported by The Eduard Čech Center for Algebra and Geometry and The John Templeton Foundation.*

lay the basics of such investigation by introducing a class of equational proof systems establishing polynomial identities, as well as determining their basic structural properties; and third, to prove non-trivial upper and lower bounds on the size-complexity of proofs in these systems, with a special focus on equational proofs of (depth-3) identities involving symmetric formulas and interpolation-based identities.

1.1. Background and Motivation

The problem of deciding whether a given arithmetic circuit (or formula) over some field computes the zero polynomial – namely, the *polynomial identity testing* problem (PIT, for short) – is of great importance in algebraic complexity theory, and complexity theory in general. It is known that there is an efficient *probabilistic* procedure[1] for testing whether an arithmetic circuit computes the zero polynomial (cf. [13], [17]). However, not much is known about the complexity of *deterministic* algorithms for this problem. Devising an efficient deterministic algorithm, or even a non-deterministic sub-exponential one, for PIT is an open problem.

The difficulty of finding an efficient deterministic procedure for PIT led researchers to several different directions. On the one hand, there is a growing body of work dedicated to establishing efficient deterministic procedures for PIT when arithmetic circuits are replaced by more restrictive models for computing polynomials (cf. [4], [8], [9], [11], [14]). On the other hand, in a somewhat more logical vein, evidence or justifications for the empirical difficulty of finding efficient deterministic algorithms for PIT were discovered in [7] (see also, [5]).

In this paper we propose a different direction of research, relevant both to the polynomial identity testing problem as well as to proof complexity (the field that studies the sizes of symbolic proofs – mainly propositional proofs). Instead of studying algorithms for PIT, we concentrate on *proofs*, and further restrict our study to *symbolic* proofs of polynomial identities, that is, proof sequences that manipulate algebraic formulas. Abstractly, one can think of these proof systems as non-deterministic algorithms for PIT. On the one hand, non-determinism makes the proof system potentially stronger than a deterministic algorithm. On the other hand, proofs are restricted to syntactic manipulations of arithmetic formulas, which limits the power of the system.

If it turns out that every polynomial identity has a polynomial-size proof (consisting of only manipulations of algebraic formulas), then we would have an efficient non-deterministic algorithm for PIT. Conversely, showing that there are identities that do not have polynomial-size proofs, would imply that any (deterministic or non-deterministic) algorithm for PIT must use more sophisticated techniques than merely algebraic manipulations of formulas. In this respect, the study of the complexity of proofs of polynomial identities aims at better understanding of the polynomial identity testing problem: understanding the strengthes and weaknesses of symbolic proofs of polynomial identities would at least partially delimit possible form and strength of PIT algorithms.

This paper is a first, somewhat modest, step towards this goal. We introduce the notion of equational proofs of polynomial identities, and we prove several non-trivial lower and upper bounds on sizes of proofs. In accordance with recent research made on PIT algorithms and related problems, we devote special attention to depth-3 arithmetic formulas. We also discuss connections with polynomial identity testing procedures, and we show that equational proofs can efficiently formalize the Dvir-Shpilka PIT algorithm for depth-3 circuits of constant top fan-in [4].

The second motivation for the study of symbolic proofs of polynomial identities comes from the field of proof complexity, which is predominantly concerned with complexity of propositional proofs. The basic propositional proof system considered is the so called *Frege system*, and very little is known about the complexity of propositional Frege proofs. The Frege proof system for propositional logic can be viewed as a straightforward extension of the equational proof system considered in this paper, when taken over the field $\mathbb{F}_2$. Thus, a progress in understanding the latter system can potentially help in better understanding of the structure of propositional Frege proofs.

There is a close connection between proofs of polynomial identities and so called *algebraic propositional proof systems*, which are propositional proof systems that operate with multivariate polynomials over a field (although there are also significant differences; see Comment 2). In this setting, a propositional tautology is viewed as a (multivariate) arithmetic formula Φ over some fixed field, such that $\Phi = 0$ holds for all $0, 1$ inputs (in contrast to our framework, where $\Phi = 0$ intends to mean that Φ defines the constant polynomial 0). This viewpoint of propositional logic is well studied in the proof complexity literature. Algebraic propositional proof systems include relatively weak proof systems such as *Nullstellensatz* [1] and the *Polynomial Calculus* [3], but also systems as strong as Frege. Such strong algebraic systems were considered (among other systems) in both [2] and [6], and both of these works are close to the proof systems presented here (since all of these systems incorporate the polynomial-ring axioms in them).

1.2. The Basic Model: Equational Proofs of Polynomial Identities

We now introduce the basic proof system for proving polynomial identities.

1. More precisely, PIT is in coRP .

Note: The definition of equational proof systems below (Definition 1.2) is a general one. This means that by adding different set of axioms, one can obtain many proof systems establishing all sorts of languages, e.g., *propositional* proof systems (that is, proof systems for *Boolean* tautologies) as strong as Frege systems, and also proof systems for other languages. We shall discuss mainly proofs of polynomial identities (as in Definition 1.3).

We consider *arithmetic formulas* (*formulas*, for short) as labeled trees, where internal nodes have fan-in two and are labeled with product ($\times$) and plus ($+$) gates, and leaves are labeled either with ring elements or with input variables, and such that edges are directed from leaves toward the root. An arithmetic formula (whose leaves are labeled with elements from a ring $\mathcal{R}$) *computes a polynomial* over $\mathcal{R}$ in the natural way, that is, leaves compute the ring element or variable that labels them, and plus and product gates compute the sum (respectively, product) of the polynomials computed by the nodes that have incoming edges to them. The *size* of a formula is the number of nodes in it. For two formulas f, g, an *equation* is an expression $f = g$.

Definition 1.1 (Derivation rule)**.** *A derivation rule (or just a* rule*, for short) is a $k+1$-tuple of equations $e_0, \ldots, e_k$, for $k \geq 1$, written as*

$$\frac{e_1, \ldots, e_k}{e_0}.$$

Given the equations $e_1, \ldots, e_k$ we can derive the equation e_0, in which case we say that e_0 was derived from *$e_1, \ldots, e_k$ by* applying the derivation rule *above.*

Definition 1.2 (Equational proof system)**.** An equational proof system $\mathscr{E}$ *is described by a set of equations $\mathscr{A}$ that are said to be the* proper axioms of $\mathscr{E}$*. The* axioms of $\mathscr{E}$ *are the elements of $\mathscr{A}$ together with all equations of the form:*

$$f = f\,.$$

The derivation rules of an equational proof system $\mathscr{E}$ are the following:

$$(1)\ \frac{f = g}{g = f} \qquad (2)\ \frac{f = g \qquad g = h}{f = h}$$

$$(3)\ \frac{f_1 = g_1 \qquad f_2 = g_2}{f_1 + f_2 = g_1 + g_2} \qquad (4)\ \frac{f_1 = g_1 \qquad f_2 = g_2}{f_1 \times f_2 = g_1 \times g_2}$$

A proof in $\mathscr{E}$ of an equation $f = g$ *(also called an* equational proof *[in $\mathscr{E}$]) is a sequence of equations that terminates with the equation $f = g$, and such that every equation is either an axiom or has been derived from previous equations by one of the above four rules. In case there is an $\mathscr{E}$-proof of $f = g$ we write $\mathscr{E} \vdash f = g$. The* ***size*** *of an equational proof is the total size of all formulas in all proof-lines. The* number of steps *respectively,* number of lines *in an equational proof is the total number of equations in it.*

Comment 1. *Note that in the definition of a size of a formula, and hence of a proof, we count only the number of symbols in the formula. In particular, a constant symbol is understood to have size one regardless of the ring element it denotes. (In an extreme case, the constant may represent a superexponentially large integer or even a transcendent real number.)*

Next, we introduce a particular equational proof system intended to prove polynomial identities over a ring. The first five sets of axioms describe general properties of polynomials, the *Ring identities* reflect the structure of the particular ring $\mathcal{R}$. The system resembles the system of *equational logic* introduced in [2] (see Comment 2). Note also that **all rings in this paper are assumed to be commutative.**

Definition 1.3. *(*The system $\mathbb{P}(\mathcal{R})$: proofs of polynomial-identities over $\mathcal{R}$*): Let $\mathcal{R}$ be a (commutative) ring. $\mathbb{P}(\mathcal{R})$ is the equational proof system whose set of proper axioms $\mathscr{A}$ consists of the following equations:*

Commutativity	$f + g = g + f$	$f \cdot g = g \cdot f$
Associativity	$f + (g + h) = (f + g) + h$	
	$f \cdot (g \cdot h) = (f \cdot g) \cdot h$	
Distributivity	$f \cdot (g + h) = f \cdot g + f \cdot h$	
Zero element	$f + 0 = f$	$f \cdot 0 = 0$
Unit element	$f \cdot 1 = f$	
Ring identities	$c = a + b$	$d = a' \cdot b'$,

(where in the Ring identities *$a, a', b, b', c, d \in \mathcal{R}$ are such that the equations $c = a + b$ and $d = a' \cdot b'$ hold in $\mathcal{R}$).*

Convention: 1. When speaking about *equational proofs over some ring $\mathcal{R}$* we refer to the systems $\mathbb{P}(\mathcal{R})$.

2. Associativity of addition allows us to identify $(a+b)+c$ with $a+(b+c)$, or simply $a+b+c$. We can also abbreviate $a_1+\cdots+a_n$ with $\sum_{i=1}^{n} a_i$, and similarly for multiplication.

Theorem 1.1 (Soundness & Completeness)**.** *Let $\mathcal{R}$ be a ring. Then $\mathbb{P}(\mathcal{R}) \vdash f = g$ iff f and g compute the same polynomial.*

Proof: The implication ($\Rightarrow$) is a straightforward induction on the number of lines in a proof. The opposite implication follows from the fact that by the means of the rules and axioms in $\mathbb{P}(\mathcal{R})$, one can express any formula f in normal form, that is, as a sum of monomials. More exactly, there exists a formula $f^\star$ which has the form $\sum_j c_j \prod_i x_i$, such that, $\mathbb{P}(R) \vdash f = f^\star$. If f and g define the same polynomial, they have the same normal form, up to associativity and commutativity of addition and multiplication. Hence $\mathbb{P}(\mathcal{R})$ proves $f = f^\star$, $g = g^\star$ and $f^\star = g^\star$. Hence also $\mathbb{P}(\mathcal{R}) \vdash f = g$. ■

Comment 2. *(i) The main difference between $\mathbb{P}(\mathcal{R})$ and*

algebraic propositional proof systems is the following. The system $\mathbb{P}(\mathcal{R})$ establishes that two arithmetic formulas compute the same formal polynomial over $\mathcal{R}$ (that is, the two polynomials have the same vector of coefficients for their monomials), or, equivalently, that an arithmetic formula computes the identically zero polynomial over $\mathcal{R}$. On the other hand, propositional algebraic proof systems usually prove that a set of polynomial equations does not have a $0,1$ solution, or that a certain polynomial equation outputs 0 for every $0,1$ input. Over the two element field $\mathbb{F}_2$, $\mathbb{P}(\mathbb{F}_2)$ proves $\Phi = 0$ iff Φ defines the zero polynomial, whereas in an algebraic propositional proof system, $\Phi = 0$ would mean that Φ computes the identically zero function. (Note that $x^2 + x$ defines the zero function over $\mathbb{F}_2$ but it is not a zero polynomial.) $\mathbb{P}(\mathbb{F}_2)$ defines a coRP *language, whereas the set of all formulas computing the zero function is* coNP.

(ii) $\mathbb{P}(\mathcal{R})$ is essentially the system of equational logic *mentioned in [2]. However, they focus on the case where $\mathcal{R}$ is a finite field (of some characteristic p), with additional axioms of the form $x^p - x = 0$. This means that $f = g$ is understood as equivalence of functions rather than of polynomials (this is a different example of the general equational proof system $\mathscr{E}$, and is an extension of $\mathbb{P}(\mathbb{F}_p)$). Their system in [2] is intended to prove propositional tautologies, and the question of the complexity of proofs of polynomial identities is not addressed there.*

(iii) In propositional proof complexity one usually requires a proof system to be polynomially verifiable, in the sense that there exists a polynomial-time algorithm that decides whether a string of symbols is a correct proof in the system. This is true about $\mathbb{P}(\mathcal{R})$, if the underlying ring is finite. In general, however, the system $\mathbb{P}(\mathcal{R})$ does not have this property. One reason is that we do not consider the structure of constant symbols in the notion of size of a formula and a proof; however, if the ring $\mathcal{R}$ is efficiently presented, this problem can be avoided by accommodating the notion of size (of a formula or a proof) to measure also the size of constant symbols. Another reason, is that the ring $\mathcal{R}$ itself may have large computational complexity, in the sense that we cannot efficiently test whether $a + b = c$ holds for $a, b, c \in \mathcal{R}$. On the other hand, we may think of $\mathcal{R}$ as a kind of an oracle, in which case proofs of $\mathbb{P}(\mathcal{R})$ will be polynomially verifiable with respect to the oracle.

1.3. Summary of Results

We present three kinds of results regarding equational proofs of polynomial identities:

Structural results. The first kind of results are basic structural results concerning equational proofs. We introduce an alternative formulation of the general proof system $\mathscr{E}$ (Definition 1.2), namely, *straight-line proofs*, and prove that this formulation is essentially equivalent to the original one (namely, that it is polynomially equivalent with respect to the number of proof-lines with tree-like $\mathscr{E}$ proofs). Furthermore, we introduce several fragments of the system $\mathbb{P}(\mathcal{R})$ (Definition 1.3), each obtained by imposing certain restrictions on the structure of proofs.

Upper bounds. The second kind of results concern *polynomial upper bounds* on sizes of equational proofs of certain polynomial identities in $\mathbb{P}(\mathcal{R})$. We focus on identities based on depth-3 symmetric polynomials and interpolation-based formulas. One reason to study these identities is that – as suggested in [6] – they seem to be hard candidates for equational proofs. Our results refute this suggestion already for equational proofs operating with bounded-depth formulas, over infinite fields: *we show that the properties of the symmetric polynomials are provable with depth-4 equational proofs.*

Additional evidence of the strength of equational proof systems is provided by observing that equational proofs can simulate the Dvir-Shpilka [4] polynomial identity testing algorithm for depth-3 formulas of constant top fan-in.

Lower bounds. The third kind of results are *exponential lower bounds* on equational proofs.

First, we prove an exponential lower bound on the number of $\mathbb{P}(\mathcal{R})$ proof-lines, for a certain specific ring $\mathcal{R}$. This result is an unconditional one (that is, there are no restrictions made on the proofs or their structure). The ring $\mathcal{R}$ is specifically tailored for the purpose of the lower bound.

Second, we prove exponential lower bounds for two fragments of $\mathbb{P}(\mathcal{R})$, namely *analytic depth-3 proofs* under a certain regularity condition and *one-way proofs* (defined in Section 2.2).

Analytic proofs are proofs where one is not allowed to introduce arbitrary formulas in a proof. This requirement is akin to the analytic (or cut-free) requirement in propositional proofs. We consider analytic proofs operating with formulas of depth 3 under a certain regularity condition on the structure of proofs.

One-way proofs are obtained by further restricting analytic proofs, in the sense that we are not allowed to introduce even new constants in a proof. Here we prove an exponential-lower bound on *unrestricted-depth* proofs. The hard identities are considerably simple, and so this gives evidence that one-way proof systems are quite weak.

The first and third lower bounds have the merit of exploiting the possibility of working over an infinite underlying ring $\mathcal{R}$. Hence, the proof methods differ substantially from the standard techniques used in proof complexity.[2]

1.4. Organization of the Paper

In Section 2 we give basic structural results on equational proof systems and introduce several fragments. Section 3 is

2. It might be worth mentioning that *we do not use the interpolation technique* from proof complexity. The term *interpolation* in this paper stands for the algebraic notion of *polynomial interpolation*.

devoted to prove upper bounds as well as to connections with PIT algorithms. Section 4 presents our lower bounds. Some proofs are omitted from the text. They will appear in the full version of this paper.

2. Basic Properties and Fragments of Equational Proofs

We now introduce an alternative formalization of equational proofs, which we call *straight-line proofs*. We use this formulation to define fragments of the system $\mathbb{P}(\mathcal{R})$.

2.1. Straight-line Proofs

The idea of a straight-line proof is that if we prove $f = g$ then we should be able to transform f into g, by means of the axioms of the proof system.

Let $\mathscr{E}$ be an arbitrary equational proof system. *An elementary operation* is an ordered pair $\langle f, g\rangle$, such that $f = g$ or $g = f$ is a proper axiom of $\mathscr{E}$. An elementary operation will be written as $f \to g$. Hence, an axiom $f = g$ defines two elementary operations, $f \to g$ and $g \to f$. *An application of* $f \to g$ *to* h is the result of replacing *at most one* occurrence of f in h by g (that is, substituting a subformula f inside h by the formula g).

Definition 2.1 (Straight-line proof in $\mathscr{E}$)**.** *An* $\mathscr{E}$-straight-line proof of the equation $f = g$*, is a sequence of formulas* $f_1, \ldots, f_m$ *such that* f_1 *is* f *and* f_m *is* g *and* f_{i+1} *(for* $i \in [m-1]$*) was obtained from* f_i *by an application of one of the elementary operations corresponding to an axioms of the equational proof system* $\mathscr{E}$*.*[3]

We say that an equational proof in $\mathscr{E}$ is a *tree-like* proof if every proof-line is used at most once in a derivation rule application in the proof. Otherwise, the proof is called *dag-like* (when we do not state explicitly whether the proof is tree-like or dag-like, we mean dag-like). It is easy to show that any straight-line proof of size s can be converted to a tree-like $\mathscr{E}$-proof of size $O(s)$. The converse is slightly more intricate:

Proposition 2.1. *Let* $\mathscr{E}$ *be an equational proof system, and assume that* $\mathscr{E}$ *proves* $f = g$*. Then, there exists an* $\mathscr{E}$ *straight-line proof of* $f = g$*. Moreover:*

1) *If* $f = g$ *has a tree-like proof with* m *proof-lines and size* s*, then it has a straight-line proof with* $O(m)$ *proof-lines, and size polynomial in* s*.*
2) *If* $f = g$ *has a dag-like proof with* m *proof-lines, then it has a straight-line proof with* $O(m)$ *applications of distinct elementary operations.*

The following shows that in the case of the particular system $\mathbb{P}(\mathcal{R})$, general and tree-like equational proofs are polynomially equivalent, as far as the *number of steps* is concerned. (The proposition is analogous to the result in [10] concerning propositional proofs.)

Proposition 2.2. *Assume that the identity* $f = g$ *has a* $\mathbb{P}(\mathcal{R})$ *proof with* m *proof-lines. Then,* $f = g$ *has a tree-like* $\mathbb{P}(\mathcal{R})$ *proof with* $O(m^2)$ *proof-lines.*

2.2. Fragments

We now define several fragments of the system $\mathbb{P}(\mathcal{R})$. The restrictions are of two kinds: one is the restriction on the *depth* of formulas, and it applies to both general equational proofs and straight-line proofs. The other kind is obtained by restricting the operations used in straight-line proofs.

Constant-depth proofs. We define constant-depth formulas. Since the equational proofs as defined above work with formulas of fan-in two, it is convenient to define the depth of formulas as the maximal number of *alternations* between different gate-labels in a path in the formula. We write, for instance, $\Sigma\Pi\Sigma$ to denote the class of formulas of depth-3, where the gate at the root is a plus gate (and similarly, for other classes of constant-depth formulas).

Comment 3. *When considering depth-*3 *formulas we refer to* $\Sigma\Pi\Sigma$ *formulas and we assume that coefficients multiplying variables* do not increase the depth of formulas*. Hence a linear form* $\sum_{i=1}^{n} \alpha_i x_i$ *is assumed to be a* (Σ) *depth-*1 *formula (and not* $\Sigma\Pi$ *depth-*2 *formula). This conforms to the standard definition of depth-*3 *arithmetic formulas as sums of products of linear forms.*

Definition 2.2 (Depth-d equational proof)**.** *A* depth-d equational proof *is an equational proof in which each formula occurring in the proof is of depth at most* d*. (The same terminology applies for all other variants [and fragments] of equational proof systems [that is, straight-line proofs, analytic proofs and one-way proofs defined in the sequel].)*

Analytic Proofs. We introduce analytic proofs as straight-line proofs where one cannot introduce arbitrary formulas along proofs. This resembles the so-called subformula property in standard (propositional or predicate sequent calculus) proofs.

Definition 2.3 (Analytic straight-line proofs)**.** *A* $\mathbb{P}(\mathcal{R})$ *straight-line proof is called* analytic *if it contains* no *applications of the rule* $0 \to f \cdot 0$*. (The converse rule* $f \cdot 0 \to 0$ *is allowed.)*

The analytic criterion implies, for instance, that one

3. Specifically, the elementary operations of straight-line proofs of polynomial identities over $\mathcal{R}$ are: $f+g \leftrightarrow g+f$, $f \cdot g \leftrightarrow g \cdot f$, $f+(g+h) \leftrightarrow (f+g)+h$, $f \cdot (g \cdot h) \leftrightarrow (f \cdot g) \cdot h$, $f \cdot (g+h) \leftrightarrow f \cdot g + f \cdot h$, $f+0 \leftrightarrow f$, $f \cdot 0 \leftrightarrow 0$, $f \cdot 1 \leftrightarrow f$, and $c \leftrightarrow a+b$, $d \leftrightarrow a' \cdot b'$, where $a, a', b, b', c, d \in \mathcal{R}$, such that $c = a+b$, $d = a' \cdot b'$, are true in $\mathcal{R}$. (We write $f \leftrightarrow g$ to denote the two operations $f \to g$ and $g \to f$.)

cannot derive the formula $f + x - x$ from the formula f, if x does not occur in f.

One-Way Straight-Line Proofs. A one-way proof is an analytic straight-line proof, where one is also forbidden to introduce new (arbitrary) constant symbols via the elementary operations $a \to b+c$ and $a \to b' \cdot c'$ (even when $a = b+c$ and $a = b' \cdot c'$ are true in the underlying ring).

Definition 2.4 (One-way straight-line proofs)**.** *An analytic straight-line proof is called* one-way *if it contains* no *applications of the rules $a \to b+c$ and $a \to b' \cdot c'$ (for a, b, b', c, c' constants symbols). (We do allow the converse operations, that is, $b + c \to a$ and $b' \cdot c' \to a$.)*

Comment 4. *Note that both analytic and one-way proofs are* complete *for the set of equations $f = 0$. However, both of these proof systems are not complete for the set of equations $f = g$. In other words, there exist formulas f, g defining the same polynomial, but there is no analytic proof of $f = g$. For example $y - y = z - z$ has no analytic proofs. Also note that there may exist f, g such that there is an analytic proof of $f = g$ but not of $g = f$, and if both proofs do exist, they may have different sizes.*

3. Upper Bounds

In this section we illustrate the power of equational proofs by presenting efficient proofs for several polynomial identities.

3.1. Symmetric Polynomials and Interpolation over Fields

We consider identities connected to counting and interpolation. We show that they have polynomial-size bounded-depth proofs over large enough fields. We start with the *elementary symmetric polynomials*. For $k \geq 0$, let $\mathbb{S}_n^k(x_1, \ldots, x_n)$ denote the elementary symmetric polynomial of degree k, that is:

$$\mathbb{S}_n^k(x_1, \ldots, x_n) := \sum_{\substack{I \subseteq [n] \\ |I|=k}} \prod_{i \in I} x_i \,.$$

We set $\mathbb{S}_n^0(x_1, \ldots, x_n) := 1$ and $\mathbb{S}_n^k(x_1, \ldots, x_n) := 0$, for $k > n$.

It is known that over large enough fields there are polynomial-size (in n, the number of variables) arithmetic formulas of depth-3 for the symmetric polynomials. Our results show that basic properties of such formulas are already *provable with depth-4 equational proofs*, in the sense of the following theorem ("polynomial-size" means polynomial-size with respect to the number of variables n):

Theorem 3.1. *Let $\mathbb{F}$ be an infinite field. For $k, n \geq 0$, there exist-polynomial size depth-3 formulas $\mathbf{S}_n^k(x_1, \ldots x_n)$, computing $\mathbb{S}_n^k$, such that the following identities have polynomial-size depth-4 equational proofs:*

1) $\mathbf{S}_n^0(X_n) = 1,\ \mathbf{S}_n^k(X_n) = 0,\ k > n$;
2) $\mathbf{S}_n^k(X_n) = x_n \otimes \mathbf{S}_{n-1}^{k-1}(X_{n-1}) + \mathbf{S}_{n-1}^k(X_{n-1})\, 0 < k \leq n$;
3) $\prod_{i=1}^{n}(x_i + y) = \sum_{k=0}^{n} \left(y^{n-k} \otimes \mathbf{S}_n^k(X_n)\right)$ *with y a variable.*

In the theorem, we denote

$$X_n := \{x_1, \ldots, x_n\}$$

and we use the following abbreviation: for a (depth-3) $\Sigma\Pi\Sigma$ formula f and a $\Pi\Sigma$ formula g, denote by $g \otimes f$ the $\Sigma\Pi\Sigma$ formula obtained by distributing g over the plus gates of f. That is, if $f = \sum_i A_i$ then $g \otimes f = \sum_i (g \cdot A_i)$.

The following theorem is due to M. Ben-Or (cf. Theorem 5.1 in [15]). We give the proof of this theorem since it is relevant to the construction of the small equational proofs below, and also to Section 3.3.

Theorem 3.2 (Ben-Or)**.** *Let $\mathbb{F}$ be a field, let X be a set of n variables $\{x_1, \ldots, x_n\}$, where $n < |\mathbb{F}|$, and let $r_0, \ldots, r_n$ be any sequence of distinct field elements. For every elementary (multilinear) symmetric polynomial over X (over the field $\mathbb{F}$) there is a polynomial-size (in n) depth-3 formula computing it, of the following form:*

$$\sum_{j=0,\ldots,n} c_j \cdot \prod_{i=1,\ldots,n} (x_i + r_j)\,, \tag{1}$$

where the c_j's are field elements.

Proof of Theorem 3.2: Observe that for all $j = 0, \ldots, n$:

$$\prod_{i=1,\ldots,n} (x_i + r_j) = \sum_{k=0,\ldots,n} \mathbb{S}_n^k(x_1, \ldots, x_n) \cdot r_j^{n-k}\,.$$

Thus, we obtain

$$\left(\mathbb{S}_n^n(X_n), \mathbb{S}_n^{n-1}(X_n), \ldots, \mathbb{S}_n^0(X_n)\right) \cdot \mathbf{V} = \left(\prod_{i=1}^{n}(x_i + r_0), \prod_{i=1}^{n}(x_i + r_1), \ldots, \prod_{i=1}^{n}(x_i + r_n)\right),$$

where $\mathbf{V}$ is the Vandermonde matrix

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ r_0 & r_1 & \ldots & r_n \\ r_0^2 & r_1^2 & \ldots & r_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ r_0^n & r_1^n & \ldots & r_n^n \end{pmatrix}$$

Since $\mathbf{V}$ is a Vandermonde matrix it is invertible, and the formulas $\mathbf{S}_n^n(X_n), \mathbf{S}_n^{n-1}(X_n), \ldots, \mathbf{S}_n^0(X_n)$ can be defined

as

$$\left(\mathbf{S}_n^n(X_n), \mathbf{S}_n^{n-1}(X_n), \ldots, \mathbf{S}_n^0(X_n)\right) := \left(\prod_{i=1}^{n}(x_i + r_0), \prod_{i=1}^{n}(x_i + r_1), \ldots, \prod_{i=1}^{n}(x_i + r_n)\right) \cdot \mathbf{V}^{-1}\,.$$

The formulas are of depth-3 and size $O(n^2)$. ■

We now consider proofs operating with depth-4 formulas. By *depth-4 formulas* we specifically refer to formulas with a product gate at the top (that is, $\Pi\Sigma\Pi\Sigma$ formulas).

Proof of Theorem 3.1: Let $r_0, r_1, \ldots$ be an infinite sequence of distinct elements of $\mathbb{F}$. We set $\mathbf{S}_n^k(x_1, \ldots, x_n) := 0$ whenever $k > 0$ and $\mathbf{S}_0^0 := 1$. Otherwise, the formulas $\mathbf{S}_n^k(x_1, \ldots x_n)$, for $k \leq n$, are defined to be of the form

$$\sum_{j=0,\ldots,n} c_{j,n}^{(k)} \cdot \prod_{i=1,\ldots,n} (x_i + r_j)\,, \tag{2}$$

where $c_{j,n}^{(k)}$ are constants from $\mathbb{F}$, such that every $\mathbf{S}_n^k(x_1, \ldots, x_n)$ computes the symmetric polynomial $\mathbb{S}_n^k(x_1, \ldots, x_n)$, according to Theorem 3.2.

For $n \geq 0$, let A_n^0 denote the equation

$$\mathbf{S}_n^0(X_n) = 1\,,$$

and A_n^k, for $k = 1, \ldots, n$, denotes the equation

$$\mathbf{S}_n^k(X_n) = x_n \otimes \mathbf{S}_{n-1}^{k-1}(X_{n-1}) + \mathbf{S}_{n-1}^k(X_{n-1})\,.$$

Let $B_n(y)$ be the equation

$$\prod_{i=1}^{n}(x_i + y) = \sum_{k=0}^{n} \left(y^{n-k} \otimes \mathbf{S}_n^k(X_n)\right)\,.$$

The proofs of $A_n^k, B_n(y)$ will be constructed inductively, using the two following claims:

Claim 3.3. *There exists a polynomial p such that for every n, $B_n(y)$ has a depth-4 proof of size $p(n)$ from the set of equations A_m^k, $m = 0, \ldots, n$, $k = 0, \ldots, m$ (that is, a proof where the equations can be used as axioms).*

Proof of claim: We construct the proofs by induction on the number of variables n.

Base case: $n = 0$. $B_0(y)$ is a true identity of constant size and hence it has a constant size proof.

Induction step:

$$\prod_{i=1}^{n}(x_i + y) = (x_n + y) \cdot \prod_{i=1}^{n-1}(x_i + y) \overset{\text{by induction hypothesis}}{\overset{\downarrow}{=}}$$

$$(x_n + y) \cdot \sum_{k=0}^{n-1} \left(y^{n-1-k} \otimes \mathbf{S}_{n-1}^k(X_{n-1})\right) =$$

$$\sum_{k=0}^{n-1} \left((y^{n-1-k} \cdot x_n) \otimes \mathbf{S}_{n-1}^k(X_{n-1})\right) + \sum_{k=0}^{n-1} \left(y^{n-k} \otimes \mathbf{S}_{n-1}^k(X_{n-1})\right) \overset{\text{by rearranging}}{\overset{\downarrow}{=}}$$

$$y^n \cdot \mathbf{S}_{n-1}^0(X_{n-1}) + \sum_{k=1}^{n-1} y^{n-k} \cdot \left(x_n \otimes \mathbf{S}_{n-1}^{k-1}(X_{n-1}) + \mathbf{S}_{n-1}^k(X_{n-1})\right) + x_n \otimes \mathbf{S}_{n-1}^{n-1}(X_{n-1})\,. \tag{3}$$

A_n^0 and A_{n-1}^0 gives $\mathbf{S}_{n-1}^0(X_{n-1}) = 1 = \mathbf{S}_n^0(X_n)$, A_n^n and A_{n-1}^{n-1} gives $x_n \cdot \mathbf{S}_{n-1}^{n-1}(X_{n-1}) = \mathbf{S}_n^n(X_n)$. $A_n^k, 0 < k < n$ gives $x_n \otimes \mathbf{S}_{n-1}^{k-1}(X_{n-1}) + \mathbf{S}_{n-1}^k(X_{n-1}) = \mathbf{S}_n^k(X_n)$ and we can derive that the last sum in (3) equals

$$\sum_{k=0}^{n}(y^{n-k} \otimes \mathbf{S}_n^k(x_1, \ldots, x_n))\,.$$

Overall, the constructed proof is of depth-4 and has polynomial size. ■Claim

Claim 3.4. *There exists a polynomial q s.t. for every n and $k = 0, \ldots n$, A_n^k has depth-4 proof of size $q(n)$ from the set of equations $B_{n-1}(r_j)$, $j = 0, \ldots n$.*

Proof of claim: Let us construct the proof of A_n^k , for some $1 \leq k \leq n$ ($k = 0$ is analogous), i.e., of the equation

$$\mathbf{S}_n^k(X_n) = x_n \otimes \mathbf{S}_{n-1}^{k-1}(X_{n-1}) + \mathbf{S}_{n-1}^k(X_{n-1}).$$

We need to prove:

$$\sum_{j=0}^{n} c_{j,n}^{(k)} \cdot \prod_{i=1}^{n}(x_i + r_j) = x_n \otimes \mathbf{S}_{n-1}^{k-1}(X_{n-1}) + \mathbf{S}_{n-1}^k(X_{n-1})\,. \tag{4}$$

Consider the left hand side of (4):

$$\sum_{j=0}^{n} \left((x_n + r_j) \cdot c_{j,n}^{(k)} \cdot \prod_{i=1}^{n-1}(x_i + r_j)\right)\,. \tag{5}$$

$B_{n-1}(r_j)$ gives

$$\prod_{i=1}^{n-1}(x_i + r_j) = \sum_{k=0}^{n-1} \left(r_j^{n-1-k} \otimes \mathbf{S}_{n-1}^k(X_{n-1})\right)\,.$$

and hence

$$(x_n + r_j) \cdot c_{j,n}^{(k)} \cdot \prod_{i=1}^{n-1}(x_i + r_j) = \tag{6}$$

$$(x_n + r_j) \cdot c_{j,n}^{(k)} \cdot \sum_{k=0}^{n} \left(r_j^{n-k} \otimes \mathbf{S}_n^k(X_n)\right) =$$

$$c_{j,n}^{(k)} \cdot \sum_{k=0}^{n} \left(\left((x_n + r_j) \cdot r_j^{n-k}\right) \otimes \mathbf{S}_n^k(X_n)\right) .$$

Hence (5) is equal to

$$\sum_{j=0}^{n}\sum_{i=0}^{n-1} \left(\left((x_n + r_j) \cdot c_{j,n}^{(k)} \cdot r_j^{n-i-1}\right) \otimes \mathbf{S}_{n-1}^i(X_{n-1})\right) . \tag{7}$$

Line (7) is a depth-3 formula that can be easily proved equal (with a depth-3 proof) to the following term:

$$x_n \otimes \left(\sum_{i=0}^{n-1} \epsilon_i \otimes \mathbf{S}_{n-1}^i(X_{n-1})\right) + \sum_{i=0}^{n-1} \delta_i \otimes \mathbf{S}_{n-1}^i(X_{n-1}) , \tag{8}$$

where ϵ_i, δ_i are some constants. By the soundness of the proof system, (8) is equal to $x_n \otimes \mathbf{S}_{n-1}^{k-1}(x_1, \ldots x_{n-1}) + \mathbf{S}_{n-1}^k(x_1, \ldots x_{n-1})$. Since x_n occurs only in the left term in (8), this left term equals $x_n \otimes \mathbf{S}_{n-1}^{k-1}(x_1, \ldots x_{n-1})$ and the right term in (8) equals $\mathbf{S}_{n-1}^k(x_1, \ldots x_{n-1})$. Since for every $0 \leq i \leq n-1$, $\mathbf{S}_{n-1}^i(x_1, \ldots x_{n-1})$ computes a homogeneous polynomial of degree i, we have $\epsilon_k = 1$ and for all $i \neq k$, $\epsilon_i = 0$; similarly, $\delta_k = 1$ and for all $i \neq k$, $\delta_i = 0$. Hence, we can prove (using the zero element axioms) that (8) equals $x_n \otimes \mathbf{S}_{n-1}^{k-1}(x_1, \ldots x_{n-1}) + \mathbf{S}_{n-1}^k(x_1, \ldots x_{n-1})$. ■Claim

Claims 3.3 and 3.4 imply that for every n and $k = 0, \ldots, n$ A_n^k has depth-4 proofs from the set of equations $\{A_m^k; m < n,\ k = 0, \ldots, m\}$, the proof being of size $\leq (n+1) \cdot p(n) + q(n)$. Hence, we may conclude that A_n^k has polynomial size depth-4 size proofs. ■

Corollary 3.5. *Over an infinite field $\mathbb{F}$, any true identity of the form*

$$\sum_{j=0}^{n} c_j \cdot \prod_{i=1}^{n}(x_i + r_j) = c , \tag{9}$$

c_j's, r_j's and c being field elements, has polynomial-size depth-4 equational proofs.

We apply the short equation proofs of the properties of the symmetric polynomials to prove related algebraic identities, as shown in the next section.

3.2. Newton's Identities

In this section we establish polynomial-size depth-4 equational proofs of the Newton identities over large enough fields.

Let $\mathbf{S}_n^k(x_1, \ldots, x_n)$ be the depth-3 formulas for the elementary symmetric polynomials (as in the previous subsection). The following are the Newton identities:

$$(\mathsf{Newton}_n) \quad \sum_{i=0}^{n} \left((-1)^i \cdot \mathbf{S}_n^i(x_1, \ldots x_n) \cdot \sum_{j=1}^{n} x_j^{n-i}\right) = 0 . \tag{10}$$

As written in (10), the identities are depth-5 formulas. By appropriate opening of brackets in (10), we can write them as polynomial-size depth-3 formulas.

The fact that the Newton identities are true identities can be easily proved using the properties of elementary symmetric polynomials.

Theorem 3.6. *Over an infinite field $\mathbb{F}$, there are polynomial-size (in n) depth-4 equational proofs of* Newton_n.

This provides a positive answer to a question posed by Grigoriev and Hirsch [6] on whether there exist short proofs of the Newton identities using only elementary transformation of arithmetic formulas. (Our equational proof systems for polynomial identities are certainly of the type considered by Grigoriev and Hirsch; in fact the [implicit] proof system for polynomial identities considered in [6] is the same as our definition of straight-line proofs.)

3.3. Interpolation over General Points and Determinants of Vandermonde Matrices

Here we deal with identities that involve determinants of Vandermonde matrices. We construct polynomial-size depth-4 equational proofs for these identities.

Given a set X of $n+1$ variables $\{x_0, \ldots, x_n\}$ we define

$$\mathbf{V}_n[X] := \prod_{0 \leq i < k \leq n} (x_k - x_i) .$$

Thus, $\mathbf{V}_n[X]$ is just the determinant of the following $n+1 \times n+1$ Vandermonde matrix:

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ x_0 & x_1 & \ldots & x_n \\ x_0^2 & x_1^2 & \ldots & x_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_0^n & x_1^n & \ldots & x_n^n \end{pmatrix}$$

Let $X := \{x_0, \ldots, x_{n+1}\}$ and let $Y := \{y_1, \ldots, y_n\}$. We consider the following depth-3 identities, denoted (Van_n) in both the X and Y variables:

$$(\mathsf{Van}_n) \quad \sum_{i=0}^{n+1} \left((-1)^i \cdot \mathbf{V}_n\left[X \setminus \{x_i\}\right] \cdot \prod_{j=1}^{n}(y_j + x_i)\right) = 0 .$$

That (Van_n) is a true identity can be proved using Cramer's rule. We show that the identities (Van_n) can be efficiently

proved with equational proofs of depth-4 over large enough fields.

Theorem 3.7. *The identities* (Van_n) *have polynomial-size (in* n*) depth-*4 *proofs over an infinite fields* $\mathbb{F}$.

The theorem entails that identities expressing basic properties of determinants of Vandermonde matrices have efficient depth-4 proofs.

3.4. Connections with Polynomial Identity Testing Algorithms

As noted in the introduction, an efficient deterministic algorithm for polynomial identity testing (PIT) is not known. Even for depth-3 $\Sigma\Pi\Sigma$ formulas, no polynomial-time deterministic algorithm is known. However, feasible PIT algorithms were designed for $\Sigma\Pi\Sigma$ formulas, where the fan-in of the top plus gate is a *constant*. First, Dvir and Shpilka [4] designed a quasipolynomial deterministic PIT algorithm for $\Sigma\Pi\Sigma$ with a constant top fan-in. Subsequently, Kayal and Saxena [9] gave a polynomial algorithm for the same class of formulas (see also [12]). In what follows we show that the PIT algorithm of Dvir and Shpilka can be simulated by equational proof systems.

Let f be a $\Sigma\Pi\Sigma$ formula (over some base ring) of the form

$$\sum_{i=1}^{k} A_i$$

such that f is identically zero. The formula f is *minimal*, if the sum of any proper subset of $A_1, \ldots, A_k$ is not identically zero; f is *simple*, if there is no linear form occurring in every $A_1, \ldots, A_k$ (up to a scalar multiple). The *rank of* f, $\mathrm{rank}(f)$, is the rank of the set of linear forms computed by all the bottom plus gates in f (where a linear form is identified with the vector of its coefficients). The core of the PIT algorithm in [4] is the following:

Theorem 3.8 ([4])**.** *Let* $\mathbb{F}$ *be a field. Let* f *be a minimal and simple* $\Sigma\Pi\Sigma$ *formula which is identically zero. Let* f *have degree* $d \geq 2$*, and assume that the fan-in of the top plus gate in* f *is* $k \geq 3$*. Then,* $\mathrm{rank}(f) \leq 2^{O(k^2)}(\log d)^{k-2}$.

Whether a formula f of size m, degree d and rank r is identically equal to zero, can be tested in time $\mathrm{poly}(m, (d+r)^r)$, for we may first express f as a formula in r variables, and then expand the modified formula as a sum of monomials. If k is constant, by Theorem 3.8, this can be done in quasipolynomial time.

We observe that a similar reasoning applies to equational proofs. Assume that f has degree d, rank r and size m, and that f is identically zero. Then there exists an equational-proof of the polynomial identity $f = 0$ of size $\mathrm{poly}(m, (d+r)^r)$. For let f contain the variables $x_1, \ldots, x_n$. Then we can find a polynomial-size formula $f^\star$ in variables $y_1, \ldots, y_r$ and degree d, and linear functions $g_1(\overline{x}), \ldots, g_r(\overline{x})$, such that:

1) $f^\star(y_1, \ldots, y_r)$ is identically zero, and
2) the identity $f(\overline{x}) = f^\star\left(y_1/g_1(\overline{x}), \ldots, y_r/g_r(\overline{x})\right)$ has a polynomial-size proof.

$f^\star$ can be expressed as a sum of $\binom{d+r-1}{r-1} \leq (d+r)^r$ monomials, and hence $f^\star = 0$ has a proof of size $\mathrm{poly}(m, (d+r)^r)$. Hence also $f^\star(y_1/g_1(\overline{x}), \ldots y_k/g_k(\overline{x})) = 0$ and $f = 0$ have proofs of size $\mathrm{poly}(m, (d+r)^r)$.

Finally, when *proving* $f = 0$, we can assume without loss of generality that f is simple and minimal (if f is not minimal, we can prove each of the partial sums that equals 0 separately; and if f is not simple we can factor out the common linear forms). Thus, Theorem 3.8 gives quasipolynomial size proofs of $f = 0$, for a fixed k.

Thus, we obtain the following theorem:

Theorem 3.9. *For all identically zero depth-*3 *formulas over a field* $\mathbb{F}$ *with a constant top fan-in there are quasipolynomial-size* $\mathbb{P}(\mathbb{F})$ *proofs. (The proofs have bounded depth.)*

For the PIT algorithm of Kayal and Saxena the problem of simulation by equational proofs is open. The algorithm of Kayal and Saxena is an example of an elegant algorithm that cannot be *prima facie* formalized as an equational proof. Moreover, it can be noted that the identities (Van_n) (discussed in Section 3.3) can be easily recognized as identities by the [9] heuristics, whereas their equational proofs are quite cumbersome.

4. Lower Bounds

4.1. Full Equational Proofs over a Specific Ring

We now construct a ring $\mathcal{S}$ and give an example of a polynomial-size identity over $\mathcal{S}$, such that every equational proof of the identity has exponential size. Basically, the lower bound is a trick that exploits the high complexity of the underlying ring. We believe that the construction is interesting, for it shows that unconditional lower bounds can be obtained at least for some rings. Moreover, it is not impossible that similar arguments might work for more natural rings or fields.

Let $\mathbb{F}$ be a field. Let $\mathcal{R} := \mathbb{F}[u_1, \ldots, u_n, v_1, \ldots, v_n]$, that is, $\mathcal{R}$ is the ring of polynomials over $\mathbb{F}$ in the variables $u_1, \ldots, u_n, v_1, \ldots, v_n$. For any $X \subseteq [n]$, define the following polynomial (in $\mathcal{R}$):

$$\Gamma_X := \prod_{i \in X} u_i \cdot \prod_{i \in [n] \setminus X} v_i \,.$$

Let $I \subseteq \mathcal{R}$ be the ideal generated by the polynomials Γ_X, for all $X \subseteq [n]$. That is, $I := \mathrm{ideal}\langle \Gamma_X \ : \ X \subseteq [n] \rangle$. Finally,

let $\mathcal{S} := \mathcal{R}/I$, that is, $\mathcal{S}$ is the quotient ring of $\mathcal{R}$ by I. Consider the following identity in the ring of polynomials over $\mathcal{S}$ with variables $x_1, \ldots, x_n$ (that is, $\mathcal{S}[x_1, \ldots, x_n]$):

$$(E) \qquad \prod_{i=1,\ldots,n} (u_i \cdot x_i + v_i) = 0\,.$$

We will show that any $\mathbb{P}(\mathcal{S})$-proof of (E) has exponential in n number of lines.

Claim 4.1. *(E) is a true identity over $\mathcal{S}$. Moreover, for every ideal $J \subseteq \mathcal{R}$, (E) is an identity in $\mathcal{R}/J$ iff $I \subseteq J$.*

Proof of claim: It suffices to prove the second statement. We can rewrite (E) as

$$\sum_{X\subseteq[n]} \left(\prod_{i\in X} u_i \cdot x_i \cdot \prod_{i\in[n]\setminus X} v_i \right) = \sum_{X\subseteq[n]} \Gamma_X \cdot \prod_{i\in X} x_i = 0\,. \tag{11}$$

Thus, for every $X \subseteq [n]$ the coefficient of the monomial $\prod_{i\in X} x_i$ in (E) is Γ_X. Therefore, (E) is an identity over $\mathcal{R}/J$ iff for all $X \subseteq [n]$, Γ_X is the zero element in $\mathcal{R}/J$. The latter happens iff $I \subseteq J$. ■Claim

In order to prove the lower bound (Theorem 4.3 below), we first prove the following lemma:

Lemma 4.2. *Let $H \subseteq \mathcal{R}$. If $\mathrm{ideal}\langle H\rangle = I$, then $|H| \geq 2^n$.*

Proof: For a polynomial h, let $h^{(k)}$ denote its kth homogeneous part. The ideal I is generated by monomials of degree n, and hence for every $g \in I$ and $k < n$, $g^{(k)} = 0$. Thus, for every $h \in H$ it holds that $h^{(k)} = 0$ for all $k < n$ (as otherwise $\mathrm{ideal}\langle H\rangle \neq I$). Therefore, if $\Gamma_X = \sum_{h\in H} h \cdot g_h$ then $\Gamma_X = \sum_{h\in H} h^{(n)} \cdot g_h^{(0)}$. Hence, we can assume without loss of generality that for all $h \in H$ and all $k > n$, it holds that $h^{(k)} = 0$. In other words, every $h \in H$ is a homogeneous polynomial of degree n. If H consists of homogeneous polynomials of degree n such that $\Gamma_X \in \mathrm{ideal}\langle H\rangle$, then Γ_X is a linear combination (with coefficients in $\mathbb{F}$) of the polynomials in H. Hence the size of H is at least the dimension of the vector space $\{\Gamma_X : X \subseteq [n]\}$, where a polynomial is identified with the vector of its coefficients. The set $\{\Gamma_X : X \subseteq [n]\}$ is linearly independent, and is of size 2^n, and hence $|H| \geq 2^n$. ■

Theorem 4.3. *Every equational proof of (E) over $\mathcal{S}$ contains at least 2^n lines.*

Proof: Let P be a $\mathbb{P}(\mathcal{S})$ proof of (E) with m lines. Let us concentrate on the constant symbols and rules occurring in P (that is, the ring $\mathcal{S}$ identities). We can assume that the constant symbols in P are presented as elements of the polynomial ring $\mathcal{R}$, in such a way that different elements of $\mathcal{R}$ represent different elements of $\mathcal{S}$. Let us define the set $H \subseteq \mathcal{R}$ as follows: if P contains the constant axioms (that is, the $\mathcal{S}$ ring identities) $g_3 = g_1 + g_2$ respectively $g_3 = g_1 \cdot g_2$, we add to H the corresponding polynomials $g_3 - (g_1 + g_2)$ respectively $g_3 - (g_1 \cdot g_2)$. Then $|H| \leq m$. Since P is a proof in $\mathbb{P}(\mathcal{S})$, we have $H \subseteq I$ and hence $\mathrm{ideal}\langle H\rangle \subseteq I$. Now, P is also a proof in $\mathcal{R}/\mathrm{ideal}\langle H\rangle$, since every line of P is satisfied in this ring. Therefore (E) is an identity in $\mathcal{R}/\mathrm{ideal}\langle H\rangle$. Hence, by Claim 4.1, $I \subseteq \mathrm{ideal}\langle H\rangle$, and finally $\mathrm{ideal}\langle H\rangle = I$. By the previous lemma $|H| \geq 2^n$, and therefore $m \geq 2^n$. ■

Comment 5. *(i) The "catch" in the theorem seems to be the fact that the underlying ring $\mathcal{S}$ itself has a high computational complexity. (It is not known whether $\mathcal{S}$ can be presented in such way that one can decide in polynomial time whether $a+b=c$, respectively $a\cdot b = c$ for $a, b, c \in \mathcal{S}$.) However, the real issue is that $\mathcal{S}$ is not a field. It would be of great interest to prove a lower bound for $\mathbb{P}(\mathbb{F})$ for some field $\mathbb{F}$, no matter how complicated and artificial the field would be.*

(ii) Theorem 4.3 gives one identity (E), whereas in fact we want an infinite sequence of identities (E_n) (all over the same *ring). This could be achieved by constructing (E_n) and I_n with disjoint variables as in Theorem 4.3, and defining I as the ideal generated by $\bigcup_{n\in\mathbb{N}} I_n$.*

4.2. One-Way Proofs

We present a lower bound on one-way straight-line proofs over an infinite field. Let us consider the equation

$$(D) \qquad \prod_{i=1,\ldots n} (a_i \cdot x_i + b_i) + \prod_{i=1,\ldots n} (c_i \cdot x_i + d_i) = 0,$$

where $x_i, i = 1, \ldots, n$ are variables and $a_i, b_i, c_i, d_i \in \mathbb{Z}, i = 1, \ldots, n$. We show that the parameters in (D) can be chosen in such a way that (D) is an identity, but every one-way proof of (D) has an exponential-size:

Theorem 4.4. *Let $\mathbb{F}$ be an infinite field. Then there exist field elements $a_i, b_i, c_i, d_i, i \in [n]$ such that (D) is an identity, and every one-way proof of (D) must have at least 2^n proof-lines. If $\mathbb{F}$ contains rational numbers, the coefficients can be chosen as $\frac{p}{q}$, where p, q are integers with $|p|, |q| \leq 2^{O(n^2)}$.*

Comment 6. *Recall that we ignore the magnitude of coefficients in the definition of formula size, and hence (D) has polynomial size in our setting. However, this would be the case even if we assumed the integers to be written in binary notation, and included the length of the binary representations in the size of (D).*

Proof idea. We choose the coefficients in (D) to be sufficiently independent, in the sense that every constant (different from 0 and 1) occurring in any possible one-way proof of (D) can be uniquely expressed from the coefficients $a_i, b_i, c_i, d_i, i = 1, \ldots, n$. The existence of such elements is proved non-constructively (this is not necessary). We then

look at monomials in the variables $x_1, \ldots, x_n$ in a proof of (D). (D) has the form $D_1 + D_2 = 0$, where D_1 defines a polynomial of the form

$$\sum_{X \subseteq [n]} r_X \cdot \prod_{i \in X} x_i,$$

where $r_X \in \mathbb{Z}$, and D_2 defines the polynomial

$$\sum_{X \subseteq [n]} s_X \cdot \prod_{i \in X} x_i \,.$$

If $D_1 + D_2 = 0$ then $s_X = -r_X$. In other words, D_1 contains 2^n monomials, and D_2 contains the same monomials with opposite signs. In a proof of (D), every monomial from D_1 will, at some point, cancel with a monomial from D_2. The independence of the coefficients allows us to control the movement of monomials in a proof. In particular we get that in given line, at most one monomial can be canceled.

4.3. Depth-3 Analytic Regular Proofs

Notice that the polynomial size proof of the basic properties of the symmetric polynomials $\mathbb{S}_n^k$, given in section 3.1, and of related identities like (Van_n), is, first, of depth-4 and second, non-analytic. In fact, the best analytic upper bound (in an unrestricted-depth) we know for those identities is of quasipolynomial size. We are convinced that proving a lower bound – even in a very restricted model such as analytic depth-3 proofs – is quite difficult.[4] Nevertheless, we can prove the result under an additional restriction, that the depth-3 analytic proof is also *regular*.

The regularity condition guarantees the following: once a proof-line $A \times (B + C)$ is transformed into the proof-line $A \times B + A \times C$, the two formulas $A \times B$ and $A \times C$, as well as any other formulas that originate from $A \times B$ and $A \times C$, cannot be again united into a product formula by means of the distributivity rule. For instance, after $A \times (B + C)$ was expanded into $A \times B + A \times C$, the formulas $A \times B$ and $A \times C$ cannot be again factorised to yield $A \times (B + C)$.

With this additional assumption simple identities do not have polynomial-size proofs, such as the identity

$$(\mathrm{Bin}_n) \qquad (x+y)^n + \sum_{i=0}^{n} a_i \cdot x^i y^{n-i} = 0\,,$$

where the a_i's are constants with values $-\binom{n}{i}$.

Theorem 4.5. *Every regular depth-3 analytic straight-line proof of (Bin_n) must have $2^{\Omega(n)}$ number of lines.*

The identity $(\mathrm{Bin})_n$ contains only two variables, and it has a simple polynomial-size analytic depth-3 proof. Thus, this theorem stands as an observation on the weakness of regular proofs.

4. We attempted to prove a lower-bound on the size of proofs for those identities (e.g., (Van_n)) for analytic depth-3 proofs (and thus to exponentially separate this fragment from depth-4 equational proofs [by the upper bound in Section 3.3]). An error in our proof was spotted by Emil Jeřábek to whom we are grateful.

Acknowledgments

The second author wishes to thank Ran Raz for his encouragement and interest in this work and Nachum Dershowitz, Jan Krajíček, Pavel Pudlák and Neil Thapen for useful discussions on issues close to this paper. We also wish to thank Emil Jeřábek for pointing out an error in the preliminary version of this paper.

References

[1] 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.

[2] Samuel R. Buss, Russell Impagliazzo, Jan Krajíček, Pavel Pudlák, Alexander A. Razborov, and Jiří Sgall. Proof complexity in algebraic systems and bounded depth Frege systems with modular counting. *Comput. Complexity*, 6(3):256–298, 1996/97.

[3] 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.

[4] Zeev Dvir and Amir Shpilka. Locally decodable codes with 2 queries and polynomial identity testing for depth 3 circuits. *SIAM J. on Computing*, 36(5):1404–1434, 2006.

[5] Zeev Dvir, Amir Shpilka, and Amir Yehudayoff. Hardness-randomness tradeoffs for bounded depth circuits. In *Proceedings of the 40th ACM Symposium on the Theory of Computing*, pages 741–748, 2008.

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

[7] Valentine Kabanets and Russell Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *Comput. Complexity*, 13(1-2):1–46, 2004.

[8] Zohar Karnin and Amir Shpilka. Deterministic black box polynomial identity testing of depth-3 arithmetic circuits with bounded top fan-in. In *Proceedings of the 23th Annual IEEE Conference on Computational Complexity*, 280–291, 2008.

[9] Neeraj Kayal and Nitin Saxena. Polynomial identity testing for depth 3 circuits. *Comput. Complexity*, 16(2):115–138, 2007.

[10] Jan Krajíček. Lower bounds on constant-depth propositional proofs. *Journal of Symbolic Logic*, 59(1):73-86, 1994.

[11] Ran Raz and Amir Shpilka. Deterministic polynomial identity testing in non commutative models. *Comput. Complexity*, 14(1):1–19, 2005.

[12] Nitin Saxena and C. Seshadhri. An Almost Optimal Rank Bound for Depth-3 Identities. *This conference's proceedings.*

[13] Jacob T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27(4):701–717, 1980.

[14] Amir Shpilka and Ilya Volkovich. Read-once polynomial identity testing. In *Proceedings of the 40th Annual ACM Symposium on the Theory of Computing*, pages 507–516, 2008.

[15] Amir Shpilka and Avi Wigderson. Depth-3 arithmetic circuits over fields of characteristic zero. *Comput. Complexity*, 10:1–27, 2001.

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

[17] Richard Zippel. Probabilistic algorithms for sparse polynomials. In *Proceedings of the International Symposiumon on Symbolic and Algebraic Computation*. Springer-Verlag, 1979.