The Proof Complexity of Polynomial Identities

Pavel Hrubeš* Iddo Tzameret†

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. 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 [GH03].
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 straight-line 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 [DS06].

Contents

*Institute for Advanced Study, Princeton, NJ. Supported by NSF grant CCF 0832797 pahrubes@centrum.cz.

†Mathematical Institute, Academy of Sciences of the Czech Republic, Zitná 25, Prague, CZ-11567, tzameret@math.cas.cz. Supported by The Eduard Čech Center for Algebra and Geometry and The John Templeton Foundation.

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 basic 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. 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 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 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. [Sch80, Zip79]). 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. [RS05, DS06, KS07b, KS07a, SV08]). 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 [KI04] (see also, [DSY08]).

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 see a proof system as a non-deterministic algorithm 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.

[1] More precisely, PIT is in coRP.

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) 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 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 [DS06].

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 is in fact 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.

Moreover, propositional proof systems that operate with multivariate polynomials over a field have a central role in propositional proof complexity theory. In this setting, one usually starts from a direct translation of a propositional formula into a multivariate polynomial equation over a given fixed field. This polynomial equation defines, over $0, 1$ values, the original propositional formula (that is, the polynomial equation is true iff the formula is true, under the given assignment). This viewpoint of propositional logic, under the name *algebraic propositional proof systems*, is well studied in the proof complexity literature. When writing polynomials inside proofs as arithmetic formulas, the natural choice in formulating such systems is to enable the proof systems (among other things) to manipulate the arithmetic formulas according to the polynomial-ring axioms. This is done in order for the proofs to be efficiently recognizable (that is, we can verify efficiently that a polynomial formula was derived correctly according to the algebraic deduction rules). These kinds of algebraic propositional proof systems were considered in both [BIK$^+$97] and [GH03]. Understanding symbolic proof systems for polynomial identities is, in that sense, an essential part of the theory of algebraic proof systems.

1.2 The Basic Model: Equational Proofs of Polynomial Identities

We now introduce the basic proof system for proving polynomial identities.
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 a host of 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 form 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. For two formulas f, g, an *equation* is an expression $f = g$. The *size* of a formula is the number of nodes in it.

We write $h \equiv g$ if h and g are two (syntactically) equal formulas (equal as labeled trees; not to be confused with equality between polynomials or with proof-lines occurring in equational proofs).

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 [BIK$^+$97]. The system in [BIK$^+$97] concerns finite fields and contains additional axioms of the form $x^p - x = 0$, for all variables, which 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 $\mathbb{P}(\mathbb{F}_p)$. 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 $a,a',b,b',c,d\in\mathcal{R}$, *such that the equations hold in $\mathcal{R}$.*

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

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 define 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 *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 [GH03] – 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 [DS06] 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. 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]

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 $f_1 \equiv f$, $f_m \equiv g$ and f_{i+1} (for $i \in [m-1]$) was obtained*

[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.*

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 (see the appendix, Section B for a proof):

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 [Kraj94] 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). (See the appendix, Definition A.1.1.)

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.*

[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 $g \to f$.)

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 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 $a = b' \cdot c'$ 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 $y - y = z - z$. Also note that there may exist an analytic proof of $f = g$ but not of $g = f$, and if both 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 $k \leq n$, 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 $\mathbb{S}_n^k(x_1, \ldots, x_n) := 0$, if $k > n$. 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 (cf. [SW01] and Section C.1 in the appendix for more details). Our

results show that basic properties of such formulas are already *provable with depth-4 equational proofs*, in the sense of the following theorem (the phrase "polynomial-size" means polynomial-size with respect to n, the number of variables):

Theorem 3.1 *Let $\mathbb{F}$ be a field. For $n < |\mathbb{F}|$, 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 have polynomial-size depth-4 equational proofs:*

1. $\mathbf{S}_n^0(x_1, \ldots x_n) = 1$, $\mathbf{S}_n^k(x_1, \ldots x_n) = 0$, $k > n$;
2. $\mathbf{S}_n^k(x_1, \ldots, x_n) = x_n \otimes \mathbf{S}_{n-1}^{k-1}(x_1, \ldots x_{n-1}) + \mathbf{S}_{n-1}^k(x_1, \ldots x_{n-1})$;
3. $\prod_{i=1,\ldots,n}(x_i + y) = \sum_{k=0,\ldots,n} \left(y^{n-k} \otimes \mathbf{S}_n^k(x_1, \ldots x_n)\right)$, *for any variable y.*

In the theorem, 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 proof of Theorem 3.1 is not straightforward, since the induction should be done carefully due to the depth-4 restriction.

We apply the proofs of the symmetric polynomials in order 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 symmetric polynomials denoted (as in the previous). The following are the Newton identities:

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

As written in (1), the identities are depth-5 formulas. By appropriate opening of brackets in (1), we can write them as polynomial-size depth-3 formula.

The fact that the Newton identities are true identities can be shown by observing that each summand in (Newton_n) can in fact be expanded into two different summands, so that when this expansion is applied on every summand in (Newton_n) we get a telescopic sum (see the appendix, Section C.1.1 for more details).

Theorem 3.2 *Over a field $\mathbb{F}$, such that $n < |\mathbb{F}|$, 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 [GH03] 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 [GH03] 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. In Section 4 we show that there are no subexponential-size analytic straight-line proofs operating with depth-3 formulas for these identities (over any ring).

Given a set Z of $n+1$ variables $\{z_0, \ldots, z_n\}$ we define

$$\mathbf{V}_n[Z] := \prod_{0 \le i < k \le n} (z_k - z_i)\,.$$

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

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ z_0 & z_1 & \ldots & z_n \\ z_0^2 & z_1^2 & \ldots & z_n^2 \\ \vdots & & \ddots & \vdots \\ z_0^n & z_1^n & \ldots & z_n^n \end{pmatrix}$$

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:

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

That (Van_n) is an identity can be proved using Cramer's rule (see the appendix Section C.1.2). We show that, in fact, the identities (Van_n) can be efficiently proved with equational proofs of depth-4 over large enough fields.

Theorem 3.3 *The identities* (Van_n) *have polynomial-size (in* n*) depth-*4 *proofs over fields* $\mathbb{F}$*, such that* $n < |\mathbb{F}|$*.*

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 [DS06] designed a quasipolynomial deterministic PIT algorithm for $\Sigma\Pi\Sigma$ with a constant top fan-in. Subsequently, Kayal and Saxena [KS07b] gave a polynomial algorithm for the same class of formulas. We show that the PIT algorithm of Dvir and Shpilka can be simulated by equational proof systems, which implies the following theorem:

Theorem 3.4 *For all identically zero depth-*3 *formulas over a ring* $\mathcal{R}$ *with a constant top fan-in there are quasipolynomial-size* $\mathbb{P}(\mathcal{R})$ *proofs. (The proofs have bounded depth.)*

For the algorithm of Kayal and Saxena the problem is open (see discussion in the appendix, Section C.3). 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 [KS07b] 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 $\mathcal{R}$ be an arbitrary ring. Consider the equation

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

where $x_i, i = 1, \ldots, n$ are variables and $a_i, b_i, i = 1, \ldots, n$ are elements of $\mathcal{R}$. For $X \subseteq [n]$, let Γ_X be the formula $\prod_{i \in X} a_i \cdot \prod_{i \in [n] \setminus X} b_i$. Then (E) is an identity in $\mathcal{R}$ iff

$$\Gamma_X = 0$$

for every $X \subseteq [n]$. This follows from the fact that (E) can be written as

$$\sum_{X \subseteq [n]} \left(\Gamma_X \cdot \prod_{i \in X} x_i \right) = 0. \tag{2}$$

Let $\mathcal{R}^\star$ be the ring of polynomials in variables $a_i, b_i, i \in [n]$ over $\mathcal{R}$. Let $I \subseteq \mathcal{R}^\star$ be the ideal generated by the polynomials $\Gamma_X, X \subseteq [n]$. Finally, let $\mathcal{S} := \mathcal{R}^\star / I$.

Theorem 4.1 *Consider the equation (E) as an equation over $\mathcal{S}$, where the constants a_i, b_i are identified with the respective polynomials a_i, b_i in $\mathcal{S}$. Then, (E) is an identity. Moreover, every equational proof of (E) over $\mathcal{S}$ contains at least 2^n lines.*

Proof Idea. That (E) is an identity follows from the fact that $\Gamma_X \in I$. In the lower bound, we count the number of constant axioms used in the proof, that is, axioms of the form $a = b + c$, $a = b \cdot c$, where $a, b, c \in \mathcal{S}$. We show that if there exists a proof of (E) with m constant axioms then there exists $H \subseteq I$ such that $|H| \leq m$ and H generates the ideal I. We then show that every such H has size at least 2^n.

Comment 5

(i) The "catch" in the theorem is that the underlying ring $\mathcal{S}$ itself has a high computational complexity. It is not know whether $\mathcal{S}$ can be presented in such way that we can decide in polynomial time whether $a + b = c$, respectively $a \cdot b = c$ for $a, b, c \in \mathcal{S}$.

(ii) Theorem 4.1 gives one identity (E), whereas in fact we want an infinite sequence of identities (E_n). This would be achieved by constructing (E_n) and I_n with disjoint variables as in the Theorem 4.1, and defining I as the ideal generated by $\bigcup I_n$.

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 4.2 *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 integers 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 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 $A \times B + A \times C$, in no way the two formulas $A \times B$ and $A \times C$, as well as any other two formulas that originate (among others) from $A \times B$ and $A \times C$, be united together again into a product formula by means of the distributivity rule. For instance, in our case, after $A \times (B + C)$ was broken into the two sums $A \times B + A \times C$, these two sums ($A \times B$ and $A \times C$) cannot be united together again into a product formula by means of the 'backward' distributivity rule (that is, factoring), to yield $A \times (B + C)$, once more.

With this additional assumption, however, much simpler 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 4.3 *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.

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

[BIK+97] 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. *Computational Complexity*, 6(3):256–298, 1996/97. 1.1, 1.2

[DS06] 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. (document), 1.1, 1.3, 3.4, C.14

[DSY08] 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. 1.1

[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. An error in our proof was spotted by Emil Jeřábek to whom we are grateful.

[GH03] 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). 1, 1.1, 1.3, 3.2, C.1.1

[KI04] Valentine Kabanets and Russell Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *Computational Complexity*, 13(1-2):1–46, 2004. 1.1

[KS07a] 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. 1.1

[KS07b] Neeraj Kayal and Nitin Saxena. Polynomial identity testing for depth 3 circuits. *Computational Complexity*, 16(2):115–138, 2007. 1.1, 3.4, 3.4, C.3

[Kraj94] Jan Krajíček. Lower bounds on constant-depth propositional proofs. *Journal of Symbolic Logic*, 59(1):73-86, 1994. 2.1

[RS05] Ran Raz and Amir Shpilka. Deterministic polynomial identity testing in non commutative models. *Comput. Complexity*, 14(1):1–19, 2005. 1.1

[Sch80] Jacob T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27(4):701–717, 1980. 1.1

[SV08] 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. 1.1

[SW01] Amir Shpilka and Avi Wigderson. Depth-3 arithmetic circuits over fields of characteristic zero. *Comput. Complexity*, 10:1–27, 2001. 3.1, C.1

[Zip79] Richard Zippel. Probabilistic algorithms for sparse polynomials. In *Proceedings of the International Symposiumon on Symbolic and Algebraic Computation*. Springer-Verlag, 1979. 1.1

Appendix

A Preliminaries

For a natural number m, we use $[m]$ to denote $\{1, \ldots, m\}$.

A.1 Arithmetic Formulas

Definition A.1 (Arithmetic formula) *Fix a ring $\mathcal{R}$. An* arithmetic formula *is a labeled tree, with edges directed from the leaves to the root, and with fan-in at most two. Every leaf of the tree (namely, a node of fan-in 0) is labeled with either an input variable or a field element. Every other node of the tree is labeled with either $+$ or $\times$ (in the first case the node is a* plus gate *and in the second case a* product gate*). We assume that there is only one node of out-degree zero, called the* root*. The* size *of an arithmetic formula is the total number of nodes in its tree. An arithmetic formula computes a polynomial in the ring of polynomials $\mathcal{R}[x_1, \ldots, x_n]$ in the following way. A leaf just computes the input variable or field element that labels it. A plus gate computes the sum of polynomials computed by its incoming nodes. A product gate computes the product of the polynomials computed by its incoming nodes. (Subtraction is obtained using the constant -1.) The output of the formula is the polynomial computed by the root. The* depth *of a formula is the maximal* number of alternations[5] between plus and product gates *in a path from a leaf to the root.*

Notational conventions. In this paper we deal mainly with arithmetic formulas, and so we will use the term "formulas" to mean arithmetic formulas. We sometimes write $\cdot$ instead of $\times$ in formulas. We will use parenthesis to designate the structure of formulas. Associativity of addition allows us to identify $(a + b) + c$ with $a + (b + c)$, or simply $a + b + c$. multiplication. Also, we sometime identify arithmetic formulas with the polynomials they compute, and vice versa.

We write $h \equiv g$ if h and g are two (syntactically) equal formulas (equal as labeled trees; not to be confused with equality between polynomials or with proof-lines occurring in equational proofs).

A.1.1 Constant-depth formulas

We shall consider bounded-depth formulas. This means that there is an a priori constant d that bounds the number of alternations between plus and product gates in every path in the formula-graph. A formula Φ is said to be a $\Sigma\Pi\Sigma\ldots$ *formula* (where $\Sigma\Pi\Sigma\ldots$ has $d \geq 1$ symbols) if every path in Φ starting at the root and ending in the immediate ancestor of a leaf in the formula-graph of Φ is labeled with a block of (zero or more) consecutive plus gates followed by a block of (zero or more) consecutive product gates and so forth (d times).

When considering constant depth-formulas, and specifically depth-3 formulas we slightly change the definition of depth in order to conform to the standard definition of depth-3 arithmetic formulas, as sums of products of linear forms. Specifically, we assume that coefficients multiplying variables *do not increase the depth of formulas*:

[5] Given a path p from the root to a leaf, the number of alternations between plus and product gates is the number of alternations between consecutive blocks of the same gate-labels.

Definition A.2 (Depth-3 formulas ($\Sigma\Pi\Sigma$)) *A depth-3 ($\Sigma\Pi\Sigma$) formula Φ (in the variables $x_1, \ldots, x_n$) over the ring $\mathcal{R}$ is a formula having the following form:*

$$\Phi \equiv \sum_{i=1}^{m} \prod_{j=1}^{d_i} L_{ij} \,, \tag{3}$$

where the L_{ij}'s are linear forms $a_{0,i} + a_{1,i} \cdot x_1 + \ldots + a_{n,i} \cdot x_n$, for the $a_{k,j}$'s being constant ring symbols.

Thus, under the above definition, a linear form $\sum_{i=1}^{n} \alpha_i \cdot x_i$ is assumed to be a (Σ) depth-1 formula (and not a $\Sigma\Pi$ depth-2 formula).

Factoring in depth-3. In accordance with the way we define depth-3 formulas, we also accommodate appropriately the axioms of the $\mathbb{P}(\mathcal{R})$ proof systems, *to allow for the addition of two linear forms in side depth-3 formulas, without increasing the depth of the formula.*

Definition A.3 (Addition of linear forms axiom) *When considering depth-d $\mathbb{P}(\mathcal{R})$ proofs, for a constant d, we add the following axiom to the set of proper axioms of $\mathbb{P}(\mathcal{R})$ (which also carries over to the definition of straight-line proofs and all other fragments):*

	$b \cdot x_i + c \cdot x_i = a \cdot x_i$
Addition of linear forms:	*(where, a, b, c in $\mathcal{R}$ and $b + c = a$ is true in $\mathcal{R}$).*

As a corollary, we can factor $\Pi\Sigma$ formulas with (short) depth-3 equational proofs, in the following sense:

Corollary A.1 *There is (a linear-size in the size of the formulas) depth-3 $\mathbb{P}(\mathcal{R})$-proof of:*

$$\prod_{i=2}^{d} L_i \cdot L_0 + \prod_{i=2}^{d} L_i \cdot L_1 = \prod_{i=2}^{d} L_i \cdot (\widehat{L_0 + L_1}) \,, \tag{4}$$

where the L_i's are linear forms $a_{0,i} + a_{1,i}x_1 + \ldots + a_{n,i}x_n$, and $\widehat{L_0 + L_1}$ is $b_0 + b_1x_1 + \ldots + b_nx_n$, where $b_j = a_{j,0} + a_{j,1}$, for every $0 \leq j \leq n$, holds in $\mathcal{R}$.

Definition A.3 is justified by the fact that we can efficiently simulate the *Addition of linear forms* axiom inside depth-3 $\mathbb{P}(\mathcal{R})$ proofs without increasing the depth, as the following claim shows:[6]

Claim A.2 *There is polynomial-size (in n and d) depth-3 $\mathbb{P}(\mathcal{R})$-proof of Identity (4), without using* Addition of linear forms *axioms.*

Proof of claim: From the right hand side of (4) we apply factoring to arrive at $\prod_{i=2}^{d} L_i \cdot (L_0 + L_1)$. Since $L_0 + L_1$ is a linear form (we ignore the order and associativity of terms):

$$a_{0,0} + a_{0,1} + a_{1,0}x_1 + a_{1,1}x_1 + \ldots + a_{n,0}x_n + a_{n,1}x_n \,,$$

[6]The reason we add a special axiom, instead of using the simulation, is that we will consider in the sequel (Section D.3.2) a restriction on the structure of proofs called *regularity*; the simulation of the new axiom cannot be done in regular proofs.

the whole formula is still of depth-3. The first sum $a_{0,0} + a_{1,0}$ can turn (without increasing the depth) into b_0. Now we need to show how to factor each sum $a_{0,i}x_i + a_{1,i}x_i$ into $b_i x_i$. If we factorize inside the whole product

$$\prod_{i=2}^{d} L_i \cdot (b_0 + a_{1,0}x_1 + a_{1,1}x_1 + \ldots + a_{n,0}x_n + a_{n,1}x_n)$$

we would first need to transform the last linear form into a $\Sigma\Pi\Sigma$ formula $(b_0 + (a_{1,0} + a_{1,1}) \cdot x_1 + \ldots + a_{n,0}x_n + a_{n,1}x_n)$, and so the whole product would be a $\Sigma\Pi\Sigma\Pi\Sigma$ formula. To avoid this, we do the following:

$$\begin{aligned}
&\prod_{i=2}^{d} L_i \cdot (b_0 + a_{1,0}x_1 + a_{1,1}x_1 + \ldots + a_{n,0}x_n + a_{n,1}x_n) = \\
&\prod_{i=2}^{d} L_i \cdot (a_{1,0}x_1) + \prod_{i=2}^{d} L_i \cdot (a_{1,1}x_1) \\
&\qquad + \prod_{i=2}^{d} L_i \cdot (b_0 + a_{2,0}x_2 + a_{2,1}x_2 + \ldots + a_{n,0}x_n + a_{n,1}x_n) = \\
&\prod_{i=2}^{d} L_i \cdot x_1 \cdot (a_{1,0} + a_{1,1}) \\
&\qquad + \prod_{i=2}^{d} L_i \cdot (b_0 + a_{2,0}x_2 + a_{2,1}x_2 + \ldots + a_{n,0}x_n + a_{n,1}x_n) = \\
&\prod_{i=2}^{d} L_i \cdot (b_1 x_1) + \prod_{i=2}^{d} L_i \cdot (b_0 + a_{2,0}x_2 + a_{2,1}x_2 + \ldots + a_{n,0}x_n + a_{n,1}x_n)\,.
\end{aligned}$$

We can now factorize the last line and reach:

$$\prod_{i=2}^{d} L_i \cdot (b_0 + b_1 x_1 + a_{2,0}x_2 + a_{2,1}x_2 + \ldots + a_{n,0}x_n + a_{n,1}x_n)\,.$$

Now, we proceed in the same manner for $a_{2,0}x_2 + a_{2,1}x_2$, $a_{3,0}x_3 + a_{3,1}x_3$, $\ldots$, $a_{n,0}x_n + a_{n,1}x_n$. ■Claim

Notation. For a (depth-3) $\Sigma\Pi\Sigma$ formula g and a $\Pi\Sigma$ formula f, denote by $f \otimes g$ the $\Sigma\Pi\Sigma$ formula obtained by distributing f over the plus gates of g.
Example: $x_1 \cdot x_2 \otimes ((2x_2 + 3) \cdot (3x_4 + x1) + (x_1 + 2x_2) \cdot (1 + x_3)) \equiv x_1 \cdot x_2 \cdot (2x_2 + 3) \cdot (3x_4 + x1) + x_1 \cdot x_2 \cdot (x_1 + 2x_2) \cdot (1 + x_3)$.

Distributivity in constant-depth proofs. When working with constant-depth formulas, we accommodate the distributivity axiom to work with unbounded-fan in formulas (formally we still work with fan-in two formulas). This is done in order to be able to distribute without artificially increasing the depth of formulas. For example, assume that the formula $f \cdot (g_1 + \ldots + g_n)$ is of depth d, and that the g_i's and f all have product gates at the root. If we distribute f over the

sum, we arrive first at $(f \cdot g_1 + f \cdot g_2) + f \cdot (g_3 + \ldots + g_n)$ of depth $d+1$. But if we distribute f over the sum "at once" we arrive at $f \cdot g_1 + \ldots + f \cdot g_n$ of depth d again.

Definition A.4 (Distributivity axiom (for constant depth proofs)) *When considering depth-d $\mathbb{P}(\mathcal{R})$ proofs, for a constant d, we replace the distributivity axiom from Definition 1.3 by the following axiom:*

Distributivity (for constant-depth formulas): $f \cdot (g_1 + \ldots + g_k) = f \cdot g_1 + \ldots + f \cdot g_k$.

Summary. We conclude our assumptions on formulas inside equational proofs. When speaking of constant-depth proofs we use constant-depth formulas, written as binary trees (where the depth is counted as the maximal number of alternations between different gates). We treat linear forms $a_0 + a_1x_1 + \ldots + a_nx_n$ as Σ (depth-1) formulas. Also, we allow for direct addition of linear forms by adding the axiom in Definition A.3, and we allow for distributivity of multiplication over addition done "at once", by replacing the original distributivity axiom by Definition A.3. When carrying out equational proofs, we use a less rigorous writing, by ignoring, for instance, associativity of formulas.

B Proofs and Definitions Omitted from Section 2

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 $O(m)$ many applications of distinct elementary operations.*

Proof: In (1), let us first consider the number of lines. It is by induction on m. For axioms the statement is immediate. Let us take the rule

$$\frac{f = g}{g = f}.$$

By the assumption, we have a straight-line proof of $f = g$, that is, $f_1, \ldots f_m$, where $f_1 = f, f_m = g$. But note that the elementary operations are invertible, that is, if f_{i+1} is obtained from f_i by an elementary operation, then so can f_i from f_{i+1}. Hence $f_m, \ldots f_1$ is a straight-line proof of $g = f$. The rule

$$\frac{f = g,\ g = h}{f = h}$$

corresponds to concatenation of straight-line proofs. The rule

$$\frac{f_1 = g_1,\ f_2 = g_2}{f_1 \circ f_2 = g_1 \circ g_2},$$

for $\circ \in \{+, \times\}$, can be replaced by a pair of rules of the form

$$\frac{f = g}{h[f/z] = h[g/z]}, \tag{5}$$

where z occurs exactly once in h, and $h[f/z]$ and $h[g/z]$ denote the formula h in which the variable z occurring h is replaced by the formula f, respectively, g. For a rule of the form (5) replace the straight-line proof $f_1, \ldots f_m$ of $f = g$ by the straight-line proof $h(f_1), \ldots h(f_m)$.

Now consider the size of the straight-line proof. Every line in the proof corresponds to an axiom in the original tree-like proof (recall that all derivation rules indeed correspond to some axiom [Definition 2.1]). Since every operation replaces at most one subformula at every line, the size of a formula in the straight-line proof can be at most $O(m \cdot m_0)$, where m_0 is the maximum size of a formula in the original proof. Hence the size of the straight-line proof is at most

$$O(m^2 \cdot m_0).$$

Part (2) is similar, except that we count the number of elementary operations corresponding to the axioms of the original proof.

■

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.*

Proof: Let S be a proof of $f = g$ with n lines. Let Λ be the set of formulas $u - v$, where $u = v$ is an axiom used in S. By induction, we can show that there exist formulas $h_\lambda, \lambda \in \Lambda$ such that

$$f = g + \sum_{\lambda \in \Lambda} (\lambda \cdot h_\lambda)$$

has a tree like proof with $O(n^2)$ lines. From the equations $\lambda = 0, \lambda \in \Lambda$, we obtain the tree like proof of $f = g$. ■

C Proofs Omitted from Section 3 – Upper Bounds

C.1 Symmetric Polynomials and Interpolation over Fields

Recall that the symmetric polynomials of degree k denoted $\mathbb{S}_n^k(x_1, \ldots, x_n)$ are defined to be the polynomials

$$\sum_{\substack{I \subseteq X \\ |I|=k}} \prod_{i \in I} x_i \,.$$

The following theorem is due to M. Ben-Or (cf. Theorem 5.1 in [SW01]):

Theorem C.1 (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 any symmetric polynomial over X (over the field $\mathbb{F}$) there is a polynomial-size (in n) depth-3 formula of the form:*

$$\sum_{j=0,\ldots,n} c_j \cdot \prod_{i=1,\ldots,n} (x_i + r_j)\,, \tag{6}$$

where the c_j's are all field elements.

Proof: To find the coefficients c_j, observe that

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

Taking $j = 0, \ldots, n$, we obtain

$$\left(\mathbb{S}_n^n(x_1, \ldots, x_n), \quad \mathbb{S}_n^{n-1}(x_1, \ldots, x_n), \quad \ldots \quad , \mathbb{S}_n^0(x_1, \ldots, x_n) \right) \cdot \mathbf{V} = \\ \left(\prod_{i=1,\ldots,n}(x_i + r_0), \quad \prod_{i=1,\ldots,n}(x_i + r_1), \quad \ldots \quad , \prod_{i=1,\ldots,n}(x_i + r_n) \right),$$

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

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

Since $\mathbf{V}$ is a Vandermonde matrix it is invertible, and the formulas $\mathbf{S}_n^k$, for $k = 0, \ldots, n$, can be defined as

$$\left(\mathbf{S}_n^n(x_1, \ldots, x_n), \quad \mathbf{S}_n^{n-1}(x_1, \ldots, x_n), \quad \ldots \quad , \mathbf{S}_n^0(x_1, \ldots, x_n) \right) := \\ \left(\prod_{i=1,\ldots,n}(x_i + r_0), \quad \prod_{i=1,\ldots,n}(x_i + r_1), \quad \ldots \quad , \prod_{i=1,\ldots,n}(x_i + r_n) \right) \cdot \mathbf{V}^{-1}.$$

Note that this way, the formulas for $\mathbf{S}_n^k(x_1, \ldots, x_n)$ are indeed of the required form. ∎

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). (Recall the notation $\otimes$ from Section A.1.1.)

Theorem C.2 *Let $\mathbb{F}$ be a field. For all $n < |\mathbb{F}|$ and all $k \geq 0$ there exist polynomial-size depth-3 formulas $\mathbf{S}_n^k(x_1, \ldots x_n)$, computing $\mathbb{S}_n^k(x_1, \ldots, x_n)$, such that the following identities have polynomial-size depth-4 equational proofs:*

(A) $\quad \mathbf{S}_n^0(x_1, \ldots, x_n) = 1, \quad \mathbf{S}_n^k(x_1, \ldots, x_n) = 0$, *when $k > n$;*

(B_n) $\quad \mathbf{S}_n^k(x_1, \ldots, x_n) = x_n \otimes \mathbf{S}_{n-1}^{k-1}(x_1, \ldots, x_{n-1}) + \mathbf{S}_{n-1}^k(x_1, \ldots, x_{n-1})$;

(C_n) $\quad \prod_{i=1}^{n}(x_i + y) = \sum_{k=0}^{n} \left(y^{n-k} \otimes \mathbf{S}_n^k(x_1, \ldots, x_n) \right)$, *for any variable y.*

Proof: Assume that $\mathbb{F}$ is infinite. The finite case is similar. 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 $k = -1$ 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

$$\sum_{j=0,\ldots,n} c_{j,n}^{(k)} \cdot \prod_{i=1,\ldots,n} (x_i + r_j), \tag{7}$$

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 C.1.

Note that one can easily substitute equals in formulas in the following sense:

Claim C.3 *Let f, f' and g be $\Sigma\Pi\Sigma$ formulas, and let h be a $\Pi\Sigma$ formula. Assume that $f = f'$ has size s depth-4 proof. Then, $g + h \cdot f = g + h \cdot f'$ has a size $O(s + t)$ depth-4 proof, where t is the size of the equation $g + h \cdot f = g + h \cdot f'$ (that is, the total size of its right and left hand sides).*

Proof of claim: Using $f = f'$ and the axiom $h = h$, derive $h \cdot f = h \cdot f'$. The left and right hand sides of the latter equation are $\Pi\Sigma\Pi\Sigma$ formulas. Using the distributivity axiom (for constant-depth formulas; see Definition A.4), we arrive at the depth-3 formula $h \otimes f = h \otimes f'$. Now, use the axiom $g = g$ to derive $g + h \otimes f = g + h \otimes f'$, of depth-3. $\blacksquare_{\text{Claim}}$

Claim C.4 *Assume that there is a polynomial p such that (for all n) there is a size $p(n)$ depth-4 proof that contains (B_n) (from Theorem C.2), for all choice of $0 \leq k \leq n$, as proof-lines. Then, there is a polynomial q such that (for all n) there is a size $p(n) + q(n)$ depth-4 proof of (C_n).*

Proof of claim: By induction on the number of variables n.
Base case: $n = 1$. In this case (C_1) is just $1 = y \cdot 1 + \mathbf{S}_1^1(x_1)$. By assumption, there is a depth-4 proof of $\mathbf{S}_1^1(x_1) = x_1$ of constant size, and so (C_1) has a depth-4 proof of constant size too.
Induction step:

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

$$(x_n + y) \cdot \sum_{k=0}^{n-1}\left(y^{n-1-k} \otimes \mathbf{S}_{n-1}^k(x_1, \ldots x_{n-1})\right) =$$

$$\sum_{k=0}^{n-1}\left((y^{n-1-k} \cdot x_n) \otimes \mathbf{S}_{n-1}^k(x_1, \ldots x_{n-1})\right) + \sum_{k=0}^{n-1}\left(y^{n-k} \otimes \mathbf{S}_{n-1}^k(x_1, \ldots x_{n-1})\right) = \qquad \text{(by rearranging)}$$

$$y^n \cdot 1 + y^{n-1} \cdot (x_n + \mathbf{S}_{n-1}^1(x_1, \ldots, x_{n-1})) + y^{n-2} \cdot (x_n \cdot \mathbf{S}_{n-1}^1(x_1, \ldots, x_{n-1}) + \mathbf{S}_{n-1}^2(x_1, \ldots, x_{n-1})) + \tag{8}$$

$$\ldots + y \cdot (x_n \cdot \mathbf{S}_{n-1}^{n-2}(x_1, \ldots, x_{n-1}) + \mathbf{S}_{n-1}^{n-1}(x_1, \ldots, x_{n-1})) + x_n \cdot \mathbf{S}_{n-1}^{n-1}(x_1, \ldots, x_{n-1})\,.$$

By induction hypothesis, in the second line above we used the depth-4 proof of (C_{n-1}) of size at most $q(n-1)$. By assumption, there is a depth-4 proof of size at most $p(n)$ containing all the (B_n)'s, for all $0 \leq k \leq n$. Thus, using Claim C.3 (for h in the claim being the empty formula), we can derive from the last sum (8):

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

Overall, the proof we demonstrated is of depth-4 and size at most $p(n) + q(n)$ (for an appropriate choice of $q(n)$). $\blacksquare_{\text{Claim}}$

By the above claim it is sufficient to show only polynomial-size depth-4 proofs of (B_n). The proof of (B_n) will be constructed inductively. We assume that for all $m < n$ and for all $0 \leq k \leq m$, there is a polynomial-size proof of (B_m), and that for all $0 \leq j \leq n$, we have a polynomial-size depth-4 proof of $(C_{n-1})[r_j/y]$, that is, $\prod_{i=1}^{n-1}(x_i + r_j) = \sum_{k=0}^{n-1}\left(r_j^{n-1-k} \otimes \mathbf{S}_{n-1}^k(x_1, \ldots x_{n-1})\right)$. (Note that in the induction step below, for every $0 \leq k \leq n$, (B_n) will use *the same* n proofs of $(C_{n-1})[r_0/y], \ldots, (C_{n-1})[r_n/y]$; and that each of $(C_{n-1})[r_0/y], \ldots, (C_{n-1})[r_n/y]$ will use *the same* n proofs of (B_{n-1}), for $0 \leq k \leq n-1$. Thus, we will indeed end up with a polynomial-size proof of (B_n).)

Base case: $n = 1$. We have $\mathbf{S}_1^0 \equiv 0$ by definition, and (by Theorem C.1) we can set the coefficients $c_{0,1}^{(1)}, c_{1,1}^{(1)}$ in $\mathbf{S}_1^1(x_1) \equiv c_{0,1}^{(1)} \cdot (x_1 + r_0) + c_{1,1}^{(1)} \cdot (x_1 + r_1)$ to be such that $\mathbf{S}_1^1(x_1)$ computes $\mathbb{S}_1^1(x_1) = x_1$.

Now, we need to prove with a depth-4 equational proof the identity (B_1), that is,

$$(B_1): \quad \mathbf{S}_1^k(x_1) = x_1 \cdot \mathbf{S}_0^{k-1}() + \mathbf{S}_0^k()\,,$$

for $k = 0, 1$. This already stems from definition: $\mathbf{S}_1^0(x_1) = x_1 \cdot \mathbf{S}_0^{-1}() + \mathbf{S}_0^0()$ where the right hand side equals 1, since by definition $\mathbf{S}_0^{-1}() = 0$ and $\mathbf{S}_0^0() = 1$; and $\mathbf{S}_1^1(x_1) = x_1 \cdot \mathbf{S}_0^0 + \mathbf{S}_0^1$, where the right hand side equals x_1, since by definition $\mathbf{S}_0^0 = 1$ and $\mathbf{S}_0^1 = 0$.

Induction step: Let us construct the proof of (B_n), for some $0 \leq k \leq n$:

$$\mathbf{S}_n^k(x_1, \ldots, x_n) = x_n \otimes \mathbf{S}_{n-1}^{k-1}(x_1, \ldots x_{n-1}) + \mathbf{S}_{n-1}^k(x_1, \ldots x_{n-1}).$$

We need to prove:

$$\sum_{j=0,\ldots,n} c_{j,n}^{(k)} \cdot \prod_{i=1,\ldots,n} (x_i + r_j) = x_n \times \mathbf{S}_{n-1}^{k-1}(x_1, \ldots x_{n-1}) + \mathbf{S}_{n-1}^k(x_1, \ldots x_{n-1})\,. \tag{9}$$

We consider the left hand side of (9):

$$\sum_{j=0,\ldots,n} \left((x_n + r_j) \cdot c_{j,n}^{(k)} \cdot \prod_{i=1,\ldots,n-1} (x_i + r_j) \right)\,. \tag{10}$$

By assumption, for all $0 \leq j \leq n$, we have a polynomial-size depth-4 proof of

$$\prod_{i=1}^{n-1} (x_i + r_j) = \sum_{k=0}^{n-1} \left(r_j^{n-1-k} \otimes \mathbf{S}_n^k(x_1, \ldots x_{n-1}) \right)\,.$$

Therefore, for every $0 \leq j \leq n$, we can use Claim C.3 to derive with a depth-4 proof of size linear in the size of (10):

$$(x_n + r_j) \cdot c_{j,n}^{(k)} \cdot \prod_{i=1,\ldots,n-1} (x_i + r_j) = (x_n + r_j) \cdot c_{j,n}^{(k)} \cdot \sum_{k=0}^{n} \left(r_j^{n-k} \otimes \mathbf{S}_n^k(x_1, \ldots x_n) \right) \tag{11}$$

and then substitute the corresponding summand in (10) with the right hand side of (11), for every $0 \leq j \leq n$, to get:

$$\sum_{j=0}^{n} \sum_{i=0}^{n-1} \left(\left((x_n + r_j) \cdot c_{j,n}^{(k)} \cdot r_j^{n-i-1} \right) \otimes \mathbf{S}_{n-1}^i(x_1, \ldots, x_{n-1}) \right)\,. \tag{12}$$

The term in (12) is a depth-3 formula that can be easily proved equal (with a depth-3 proof) to the following term:

$$x_n \otimes \left(\sum_{i=0}^{n-1} \epsilon_i \otimes \mathbf{S}_{n-1}^i(x_1, \ldots, x_{n-1}) \right) + \sum_{i=0}^{n-1} \delta_i \otimes \mathbf{S}_{n-1}^i(x_1, \ldots, x_{n-1})\,, \tag{13}$$

where ϵ_i, δ_i are some constants. By the soundness of the proof system, (13) is equal to $x_n \otimes \mathbf{S}^{k-1}_{n-1}(x_1, \ldots x_{n-1}) + \mathbf{S}^{k}_{n-1}(x_1, \ldots x_{n-1})$. Since x_n occurs only in the left term in (13), this left term equals $x_n \otimes \mathbf{S}^{k-1}_{n-1}(x_1, \ldots x_{n-1})$ and the right term in (13) equals $\mathbf{S}^{k}_{n-1}(x_1, \ldots x_{n-1})$. Since for every $0 \leq i \leq n-1$, the degree of the polynomial computed by $\mathbf{S}^{i}_{n-1}(x_1, \ldots x_{n-1})$ is i, it must be that $\epsilon_k = 1$ and for all $i \neq k,\ \epsilon_i = 0$; similarly, $\delta_k = 1$ and for all $i \neq k,\ \delta_i = 0$. Thus, we can easily prove (by using the zero element axioms) that (13) equals $x_n \otimes \mathbf{S}^{k-1}_{n-1}(x_1, \ldots x_{n-1}) + \mathbf{S}^{k}_{n-1}(x_1, \ldots x_{n-1})$. This concludes the proof of Theorem C.2. ∎

Corollary C.5 *Over any field $\mathbb{F}$, such that $n < |\mathbb{F}|$, any true (family of) identities of the form*

$$\sum_{j=0,\ldots,n} c_j \cdot \prod_{i=1,\ldots,n} (x_i + r_j) = c\,, \quad \textit{for field elements } c_j\textit{'s, } r_j\textit{'s and } c \textit{ (that may depend on } n\textit{)}, \tag{14}$$

have polynomial-size depth-4 equational proofs.

C.1.1 Newton's Identities

In this section we establish polynomial-size depth-4 equational proofs of the Newton identities. This will provide a positive answer to a question posed in [GH03] 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 [GH03] is the same as our definition of straight-line proofs).

Notation: Let X denote the n variables $\{x_1, \ldots, x_n\}$ and, as above, let $\mathbf{S}^k_n(X)$ denote the $\Sigma\Pi\Sigma$ formulas for the symmetric polynomials of degree k (as obtained in Theorem C.1). Recall that $\mathbf{S}^0_n(X) := 1$, that for a negative number k we set $\mathbf{S}^k_n(X) := 0$, and also for $k > n$ we set $\mathbf{S}^k_n(X) := 0$. As in the previous section, for a $\Pi\Sigma$ formula h and a $\Sigma\Pi\Sigma$ formula $F = f_1 + \ldots + f_m$ (where the f_i's are formulas with a product gate at their root [possibly with a single f_i being a linear form]) we write $h \otimes F$ to denote the $\Sigma\Pi\Sigma$ formula computing the product of h and F which is written as: $h \times f_1 + \ldots + h \times f_m$, as was done previously (Section C.1).

The following are the Newton identities for the n variables $X = \{x_1, \ldots, x_n\}$:

$$\sum_{i=0}^{n} \left((-1)^i \cdot \mathbf{S}^i_n(X) \cdot \sum_{j=1}^{n} x_j^{n-i} \right) = 0\,. \tag{15}$$

As written in (15), the Newton identities have depth-5 formulas. Since we would like to demonstrate a depth-4 proof of the Newton identities, we should define the Newton identities with depth-3 formulas. This is done simply by using the notation $\otimes$, as follows:

Definition C.1 (Newton identities) *For n variables $X = \{x_1, \ldots, x_n\}$ define:*

$$(\mathsf{Newton}_n) \qquad \sum_{i=0}^{n} \left((-1)^i \otimes \sum_{j=1}^{n} \left(x_j^{n-i} \otimes \mathbf{S}^i_n(X) \right) \right) = 0\,.$$

Note that the number of product gates in $\mathbf{S}^i_n(X)$, for every i, is $n+1$ (Theorem C.1), and so the Newton identities can be written as polynomial-size (in n) formulas.

Example: Let us illustrate the Newton identities for the case $n = 3$, and show that they are indeed identities. For the sake of clarity, we write the formulas as depth-5 formulas and not depth-3.

$$\begin{aligned}
\mathsf{Newton}_{3,3} &= \underbrace{\mathbf{S}_3^0(x_1,x_2,x_3)}_{=1 \text{ (by definition)}} \cdot (x_1^3+x_2^3+x_3^3) - \mathbf{S}_3^1(x_1,x_2,x_3)\cdot(x_1^2+x_2^2+x_3^2) + \\
&\qquad \mathbf{S}_3^2(x_1,x_2,x_3)\cdot(x_1^1+x_2^1+x_3^1) - \mathbf{S}_3^3(x_1,x_2,x_3)\cdot(x_1^0+x_2^0+x_3^0) \\
&= (x_1^3+x_2^3+x_3^3) - (x_1^1+x_2^1+x_3^1)\cdot(x_1^2+x_2^2+x_3^2) + \\
&\qquad \left(\sum_{i<j} x_i\cdot x_j\right)\cdot(x_1^1+x_2^1+x_3^1) - 3\cdot\mathbf{S}_3^3(x_1,x_2,x_3) \\
&= \left(x_1^3+x_2^3+x_3^3\right) - \left(\sum_{i=1}^{3} x_i^3 + \sum_{i\neq j} x_i^2\cdot x_j\right) + \\
&\qquad \left(\sum_{i\neq j}\left(x_i^2\cdot x_j\right) + 3\cdot\sum_{i<j<h}(x_i\cdot x_j\cdot x_h)\right) - 3\cdot\sum_{i<j<h}(x_i\cdot x_j\cdot x_h) = 0
\end{aligned}$$

Theorem C.6 *There are polynomial-size in n depth-4 equational proofs of the* Newton_n *identities.*

Proof: We start from (Newton_n):

$$\sum_{i=0}^{n}\left((-1)^i\otimes\sum_{j=1}^{n}\left(x_j^{n-i}\otimes\mathbf{S}_n^i(X)\right)\right). \tag{16}$$

By using Theorem C.2, we can obtain from (16), with a polynomial-size depth-4 proof, the following lines:[7]

$$\sum_{i=0}^{n}\left((-1)^i\otimes\sum_{j=1}^{n}\left(x_j^{n-i}\otimes\left(x_j\otimes\mathbf{S}_{n-1}^{i-1}(X\setminus j)+\mathbf{S}_{n-1}^{i}(X\setminus j)\right)\right)\right) = \tag{17}$$

$$\sum_{i=0}^{n}\left((-1)^i\otimes\sum_{j=1}^{n}\left(x_j^{n-i+1}\otimes\mathbf{S}_{n-1}^{i-1}(X\setminus j)\right)+(-1)^i\otimes\sum_{j=1}^{n}\left(x_j^{n-i}\otimes\mathbf{S}_{n-1}^{i}(X\setminus j)\right)\right) = \tag{18}$$

$$\sum_{i=0}^{n}\left((-1)^i\otimes\sum_{j=1}^{n}\left(x_j^{n-i+1}\otimes\mathbf{S}_{n-1}^{i-1}(X\setminus j)\right)\right)+\sum_{i=0}^{n}\left((-1)^i\otimes\sum_{j=1}^{n}\left(x_j^{n-i}\otimes\mathbf{S}_{n-1}^{i}(X\setminus j)\right)\right). \tag{19}$$

[7] We first derive the (depth-3) identity (B_n) from Theorem C.2 with a depth-4 proof. Then, we can substitute each $\mathbf{S}_n^i(X)$ in (16) with the corresponding term from identity (B_n); the substitution is done with a depth-3 proof.

By definition $\mathbf{S}^{i-1}_{n-1}(X \setminus j) = 0$, whenever $i = 0$, and so we obtain from Line (19):

$$\sum_{i=1}^{n}\left((-1)^i \otimes \sum_{j=1}^{n}\left(x_j^{n-i+1} \otimes \mathbf{S}^{i-1}_{n-1}(X \setminus j)\right)\right) + \sum_{i=0}^{n}\left((-1)^i \otimes \sum_{j=1}^{n}\left(x_j^{n-i} \otimes \mathbf{S}^{i}_{n-1}(X \setminus j)\right)\right) = \quad (20)$$

$$\sum_{i=0}^{n-1}\left((-1)^{i+1} \otimes \sum_{j=1}^{n}\left(x_j^{n-i} \otimes \mathbf{S}^{i}_{n-1}(X \setminus j)\right)\right) + \sum_{i=0}^{n}\left((-1)^i \otimes \sum_{j=1}^{n}\left(x_j^{n-i} \otimes \mathbf{S}^{i}_{n-1}(X \setminus j)\right)\right) = \quad (21)$$

$$\sum_{i=0}^{n-1}\left((-1)^{i+1} \otimes \sum_{j=1}^{n}\left(x_j^{n-i} \otimes \mathbf{S}^{i}_{n-1}(X \setminus j)\right)\right) + \sum_{i=0}^{n-1}\left((-1)^i \otimes \sum_{j=1}^{n}\left(x_j^{n-i} \otimes \mathbf{S}^{i}_{n-1}(X \setminus j)\right)\right) + \quad (22)$$

$$(-1)^n \otimes \sum_{j=1}^{n}\left(x_j^0 \otimes \mathbf{S}^{n}_{n-1}(X \setminus j)\right) .$$

Now, the two sums in the upper part of line (22) clearly cancel each other, and thus we are left only with the lower part of line (22), which is 0, since by definition $\mathbf{S}^{n}_{n-1}(X \setminus j) = 0$ (as $n > n-1$). ∎

C.1.2 Interpolation over General Points and Determinants of Vandermonde Matrices

Given a set Z of $n+1$ variables $\{z_0, \ldots, z_n\}$ we define

$$\mathbf{V}_n[Z] := \prod_{0 \le i < k \le n} (z_k - z_i) .$$

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

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ z_0 & z_1 & \ldots & z_n \\ z_0^2 & z_1^2 & \ldots & z_n^2 \\ \vdots & & \ddots & \vdots \\ z_0^n & z_1^n & \ldots & z_n^n \end{pmatrix}$$

Let $X := \{x_0, \ldots, x_{n+1}\}$ and let $Y := \{y_1, \ldots, y_n\}$. We consider the following equation in both the X and Y variables:

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

We now show that $(\mathsf{Van})_n$ is an identity. The proof of this fact uses basic linear algebra. In the sequel (Theorem C.9) we will show that, in fact, the identity (Van_n) can be efficiently proved with equational proofs of depth-4 already.

Proposition C.7 *For every $n \ge 1$, the equation (Van_n) is a true identities.*

Proof: The term $\prod_{j=1}^{n}(y_j + x_i)$ can be written as $\sum_{k=0}^{n} x_i^k \cdot \mathbf{S}_n^{n-k}(Y)$, and so the left hand side of (Van_n) can be written as

$$\sum_{i=0}^{n+1}\left((-1)^i \cdot \mathbf{V}_n\left[X \setminus \{x_i\}\right] \cdot \sum_{k=0}^{n} x_i^k \cdot \mathbf{S}_n^{n-k}(Y)\right) = \sum_{k=0}^{n}\left(\mathbf{S}_n^{n-k}(Y) \cdot \sum_{i=0}^{n+1}\left((-1)^i \cdot \mathbf{V}_n[X \setminus \{x_i\}] \cdot x_i^k\right)\right)$$

Hence, it is sufficient to show that

$$\sum_{i=0}^{n+1}\left((-1)^i \cdot \mathbf{V}_n[X \setminus \{x_i\}] \cdot x_i^k\right) = 0\,, \qquad \text{for all } \; 0 \le k \le n\,.$$

The following claim suffices for that matter.

Claim C.8 *The vector*

$$\mathbf{v} = \left((-1)^0 \cdot \mathbf{V}_n\left[X \setminus \{x_0\}\right], (-1)^1 \cdot \mathbf{V}_n\left[X \setminus \{x_1\}\right], \ldots, (-1)^{n+1} \cdot \mathbf{V}_n\left[X \setminus \{x_{n+1}\}\right]\right)$$

satisfies the equation

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ x_0 & x_1 & \ldots & x_{n+1} \\ x_0^2 & x_1^2 & \ldots & x_{n+1}^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_0^n & x_1^n & \ldots & x_{n+1}^n \\ x_0^{n+1} & x_1^{n+1} & \ldots & x_{n+1}^{n+1} \end{pmatrix} \cdot \mathbf{v}^t = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \mathbf{V}_{n+1}[X] \end{pmatrix} \tag{23}$$

Proof of claim: We apply Cramer's rule, stating that if $\mathbf{B}$ is an $m \times m$ matrix with determinant $\det \mathbf{B} \neq 0$ and $\mathbf{c}$ is a column vector of m field elements and $\mathbf{u}$ is a column vector of m variables $u_1, \ldots, u_m$, then the equation $\mathbf{B} \cdot \mathbf{u} = \mathbf{c}$ has a unique solution, which can be expressed by the formulas

$$u_i = \frac{\det \mathbf{B}_i}{\det \mathbf{B}}, \qquad i = 1, 2, \ldots, m\,,$$

where $\mathbf{B}_i$ denotes the $m \times m$ matrix $\mathbf{B}$ in which the ith column is replaced by $\mathbf{c}$.

Note that for every $i = 0, \ldots, n$

$$\det \begin{pmatrix} 1 & \ldots & 1 & 0 & 1 & \ldots & 1 \\ x_0 & \ldots & x_{i-1} & 0 & x_{i+1} & \ldots & x_{n+1} \\ x_0^2 & \ldots & x_{i-1}^2 & \vdots & x_{i+1}^2 & \ldots & x_{n+1}^2 \\ \vdots & \ddots & \vdots & 0 & \vdots & \ddots & \vdots \\ x_0^{n+1} & \ldots & x_{i-1}^{n+1} & \mathbf{V}_{n+1}[X] & x_{i+1}^{n+1} & \ldots & x_{n+1}^{n+1} \end{pmatrix} = (-1)^i \cdot \mathbf{V}_{n+1}[X] \cdot \mathbf{V}_n[X \setminus \{x_i\}]\,.$$

Therefore, if we denote the entries of $\mathbf{v}$ as $v_0, \ldots, v_{n+1}$, then by Cramer's rule, to satisfy Equation (23) we can indeed set the v_i's to the following values

$$v_i = \frac{(-1)^i \cdot \mathbf{V}_{n+1}[X] \cdot \mathbf{V}_n[X \setminus \{x_i\}]}{\mathbf{V}_{n+1}[X]} = (-1)^i \cdot \mathbf{V}_n[X \setminus \{x_i\}]\,. \tag{24}$$

■Claim

This concludes the proof of the theorem. ■

We now illustrate short bounded-depth equational proofs of the (Van_n) identities over any large enough field. The proofs are quite cumbersome, and so we omit certain steps which are similar in nature to the ones we do show.

Theorem C.9 *The identities* (Van_n) *have polynomial-size (in* n*) depth-*4 *proofs over fields* $\mathbb{F}$*, such that* $n < |\mathbb{F}|$*.*

Proof: We start with:

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

By Theorem C.2, we can prove, with a depth-3 proof, that (Van_n) is equal to

$$\sum_{i=0}^{n+1} \left((-1)^i \cdot \mathbf{V}_n \left[X \setminus \{x_i\} \right] \cdot \sum_{k=0}^{n} x_i^k \cdot \mathbf{S}_n^{n-k}(y_1, \ldots, y_n) \right) = 0 \,.$$

Thus, it suffices to prove for every $k = 0, \ldots, n$, with a polynomial-size depth-3 equational proof, the following identity:

$$\sum_{i=0}^{n+1} \left((-1)^i \cdot \mathbf{V}_n \left[X \setminus \{x_i\} \right] \cdot x_i^k \right) = 0. \tag{25}$$

First, we need the following lemma:

Lemma C.10 *For all* $k = 0, \ldots, n$*, the following are true identities (recall that* $X = \{x_0, \ldots, x_{n+1}\}$*):*

1. $\mathbf{S}_{n+1}^k(X \setminus \{x_j\}) = \sum_{i=0}^{k} (-1)^i \cdot x_j^i \cdot \mathbf{S}_{n+2}^{k-i}(X)$ *;*
2. $x_j^\ell \cdot \mathbf{S}_{n+1}^k(X \setminus \{x_j\}) = \sum_{i=0}^{\ell-1} (-1)^{\ell+i+1} \cdot x_j^i \cdot \mathbf{S}_{n+2}^{k+\ell-i}(X)$ *, if* $k + \ell \geq n + 2$ *.*

Proof sketch: We use the identity $\mathbf{S}_{n+2}^{k+1}(X) = x_j \cdot \mathbf{S}_{n+1}^k(X \setminus \{x_j\}) + \mathbf{S}_{n+1}^{k+1}(X \setminus \{x_j\})$, which has a polynomial-size equational proof of depth-3 by Theorem C.2.

For the identity (1), start from

$$\mathbf{S}_{n+1}^{k+1}(X \setminus \{x_j\}) = \mathbf{S}_{n+2}^{k+1}(X) - x_j \cdot \mathbf{S}_{n+1}^k(X \setminus \{x_j\}) \,, \tag{26}$$

and replace $\mathbf{S}_{n+1}^k(X \setminus \{x_j\})$ in the right hand side by $\mathbf{S}_{n+2}^k(X) - x_j \cdot \mathbf{S}_{n+1}^{k-1}(X \setminus \{x_j\})$, which stems from the same identity (26) for $\mathbf{S}_{n+1}^k(X \setminus \{x_j\})$. Continue these iterations, until arriving at the first identity (1).

The second identity (2) is obtained in a similar manner:

$$x_j^\ell \cdot \mathbf{S}_{n+1}^k(X \setminus \{x_j\}) = \\ x_j^{\ell-1} \cdot \left(x_j \cdot \mathbf{S}_{n+1}^k(X \setminus \{x_j\}) \right) .$$

Now, use the identity $x_j \cdot \mathbf{S}^k_{n+1}(X \backslash \{x_j\}) = \mathbf{S}^{k+1}_{n+2}(X) - \mathbf{S}^{k+1}_{n+1}(X \backslash \{x_j\})$, side $\mathbf{S}^{k+1}_{n+1}(X) - \mathbf{S}^{k+1}_{n}(X \backslash \{x_j\})$, to get:

$$x_j^{\ell-1} \cdot \left(\mathbf{S}^{k+1}_{n+2}(X) - \mathbf{S}^{k+1}_{n+1}(X \setminus \{x_j\}) \right) =$$
$$x_j^{\ell-1} \cdot \mathbf{S}^{k+1}_{n+2}(X) - x_j^{\ell-2} \cdot \left(x_j \cdot \mathbf{S}^{k+1}_{n+1}(X \setminus \{x_j\}) \right) .$$

Iterating these substitutions, one gets finally the identity in (2). ∎

We also need the following:

Claim C.11 *For every $k = 0, \ldots, n$ and every $j = 0, \ldots, n+1$, the coefficient of x^j_{n+1} in (25) is:*

$$\sum_{i=0}^{n} \left((-1)^i \cdot \left(\mathbf{S}^{n-j}_{n-1}(X_n \setminus \{x_i\}) \right) \cdot \mathbf{V}_{n-1}\left[X_n \setminus \{x_i\}\right] \cdot x_i^k \right) , \qquad \text{if } k \neq j , \tag{27}$$

and:

$$\sum_{i=0}^{n} \left((-1)^i \cdot \left(\mathbf{S}^{n-j}_{n-1}(X_n \setminus \{x_i\}) \right) \cdot \mathbf{V}_{n-1}\left[X_n \setminus \{x_i\}\right] \cdot x_i^k \right) + (-1)^{n+1} \cdot \mathbf{V}_n\left[X_n\right] ,$$
$$\text{if } k = j . \tag{28}$$

Proof of claim:

Notation: For a number r, we write $\prod\limits^{\backslash r}_{0 \leq j < \ell \leq n} (x_\ell - x_j)$ to denote that in the indices in the product $j \neq r \wedge \ell \neq r$. We also write X_n to denote $X \setminus \{x_{n+1}\} = \{x_0, \ldots, x_n\}$.

Equation (25) equals:

$$\sum_{i=0}^{n} \left((-1)^i \cdot \prod_{0 \leq \ell \leq n}^{\backslash i} (x_{n+1} - x_\ell) \cdot \mathbf{V}_{n-1}\left[X_n \setminus \{x_i\}\right] \cdot x_i^k \right) + (-1)^{n+1} \cdot \mathbf{V}_n\left[X_n\right] \cdot x^k_{n+1} =$$
$$\sum_{i=0}^{n} \left((-1)^i \cdot \sum_{0 \leq j \leq n}^{\backslash i} \left(x^j_{n+1} \cdot \mathbf{S}^{n-j}_{n-1}(X_n \setminus \{x_i\}) \right) \cdot \mathbf{V}_{n-1}\left[X_n \setminus \{x_i\}\right] \cdot x_i^k \right) + (-1)^{n+1} \cdot \mathbf{V}_n\left[X_n\right] \cdot x^k_{n+1} .$$

Thus, for all $j = 0, \ldots, n+1$, if $j \neq k$, the coefficient of x^j_{n+1} is:

$$\sum_{i=0}^{n} \left((-1)^i \cdot \left(\mathbf{S}^{n-j}_{n-1}(X_n \setminus \{x_i\}) \right) \cdot \mathbf{V}_{n-1}\left[X_n \setminus \{x_i\}\right] \cdot x_i^k \right) , \tag{29}$$

and, for all $j = 0, \ldots, n+1$, if $j = k$, the coefficient of x^j_{n+1} is:

$$\sum_{i=0}^{n} \left((-1)^i \cdot \left(\mathbf{S}^{n-j}_{n-1}(X_n \setminus \{x_i\}) \right) \cdot \mathbf{V}_{n-1}\left[X_n \setminus \{x_i\}\right] \cdot x_i^k \right) + (-1)^{n+1} \cdot \mathbf{V}_n\left[X_n\right] . \tag{30}$$

∎Claim

Returning to the main proof of Theorem C.9. We shall prove by induction on n the following identities (recall that the first identity [for all $k = 0, \ldots, n$], which is identical to identity (25), is sufficient to conclude the proof of the theorem):

$$\sum_{i=0}^{n+1} \left((-1)^i \cdot \mathbf{V}_n \left[X \setminus \{x_i\} \right] \cdot x_i^k \right) = 0 \,, \qquad \text{for all } k = 0, \ldots, n, \tag{31}$$

$$\sum_{i=0}^{n+1} \left((-1)^i \cdot \mathbf{V}_n \left[X \setminus \{x_i\} \right] \cdot x_i^{n+1} \right) = \mathbf{V}_{n+1}[X] \,. \tag{32}$$

The proofs of these identities will proceed by showing that the coefficient of x_{n+1}^j in (25) is equal to 0, for every $j = 0, \ldots, n+1$. We only show the proof of (31). The proof of (32) is similar.

By Claim C.11, to prove identity (31) we need to demonstrate a short proof (for all $k = 0, \ldots, n$ and all $j = 0, \ldots, n+1$), that (27) equals 0, when $k \neq j$, and a short proof that (28) equals 0, when $k = j$. This is done in the next two claims. We use the two identities in Lemma C.10.

Claim C.12 *For every $k = 0, \ldots, n$ and every $j = 0, \ldots, n+1$, such that, $k \neq j$, there is a polynomial-size equational proof of:*

$$\sum_{i=0}^{n} \left((-1)^i \cdot \left(\mathbf{S}_{n-1}^{n-j}(X_n \setminus \{x_i\}) \right) \cdot \mathbf{V}_{n-1} \left[X_n \setminus \{x_i\} \right] \cdot x_i^k \right) = 0 \,. \tag{33}$$

Proof of claim:

Case 1: $n - j + k < n$. By the first identity in Lemma C.10, we get from 33:

$$\sum_{i=0}^{n} \left((-1)^i \cdot \left(\sum_{r=0}^{n-j} (-1)^r \cdot x_i^r \cdot \mathbf{S}_n^{n-j-r}(X) \right) \cdot \mathbf{V}_{n-1} \left[X_n \setminus \{x_i\} \right] \cdot x_i^k \right) =$$
$$\sum_{r=0}^{n-j} \mathbf{S}_n^{n-j-r}(X) \cdot \sum_{i=0}^{n} \left((-1)^i \cdot ((-1)^r \cdot x_i^r) \cdot \mathbf{V}_{n-1} \left[X_n \setminus \{x_i\} \right] \cdot x_i^k \right) =$$
$$\sum_{r=0}^{n-j} \mathbf{S}_n^{n-j-r}(X) \cdot \underbrace{\sum_{i=0}^{n} \left((-1)^{i+r} \cdot \mathbf{V}_{n-1} \left[X_n \setminus \{x_i\} \right] \cdot x_i^{k+r} \right)}_{(\star)} \,.$$

By induction hypothesis, the term $(\star)$ in the last formula can be proved equal to 0 with a polynomial-size equational proof.

Case 2: $n - j + k > n$. By the second identity in Lemma C.10, we have a polynomial-size proof of

$$x_i^k \cdot \mathbf{S}_{n-1}^{n-j}(X_n \setminus \{x_i\}) = \sum_{r=0}^{k-1} (-1)^{k+r+1} \cdot x_i^r \cdot \mathbf{S}_n^{n-j+k-r}(X) \,.$$

Thus, we can get from 33 to:

$$\sum_{i=0}^{n}\left((-1)^i\cdot\left(\sum_{r=0}^{k-1}(-1)^{k+r+1}\cdot x_i^r\cdot\mathbf{S}_n^{n-j+k-r}(X)\right)\cdot\mathbf{V}_{n-1}\left[X_n\setminus\{x_i\}\right]\right)=$$
$$\sum_{r=0}^{k-1}\mathbf{S}_{k-1}^{n-j+k-r}(X)\cdot\sum_{i=0}^{n}\left((-1)^i\cdot(-1)^{k+r+1}\cdot x_i^r\cdot\mathbf{V}_{n-1}\left[X_n\setminus\{x_i\}\right]\right)=$$
$$\sum_{r=0}^{k-1}\mathbf{S}_{k-1}^{n-j+k-r}(X)\cdot\underbrace{\sum_{i=0}^{n}\left((-1)^{k+r+1+i}\cdot x_i^r\cdot\mathbf{V}_{n-1}\left[X_n\setminus\{x_i\}\right]\right)}_{(\star)}.$$

By induction hypothesis, the term $(\star)$ in the last formula can be proved equal to 0 with a polynomial-size equational proof.

■Claim

Claim C.13 *For every $k=0,\ldots,n$, and $j=k$, there is a polynomial-size equational proof of:*

$$\sum_{i=0}^{n}\left((-1)^i\cdot\left(\mathbf{S}_{n-1}^{n-j}(X_n\setminus\{x_i\})\right)\cdot\mathbf{V}_{n-1}\left[X_n\setminus\{x_i\}\right]\cdot x_i^k\right)+(-1)^{n+1}\cdot\mathbf{V}_n\left[X_n\right]=0\,,$$

The proofs follow by using the second identity in Lemma C.10. This is similar to the previous claim, and we omit the details.

This completes the polynomial-size equational proof of (Van_n). By inspection of all the proof-lines above (and by using the $\otimes$ notation, when appropriate), it is possible to show that every proof-line consists of depth-4 $\Pi\Sigma\Pi\Sigma$ formulas. ■

C.2 Simulations of Polynomial Identity Testing Procedures

Simulating Dvir-Shpilka PIT algorithm. Let f be a $\Sigma\Pi\Sigma$ formula of the form

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

such that, f is identically zero. 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). *Rank of f*, $rank(f)$, is the rank of the linear forms in f (a linear form being identified with the vector of its coefficients). The core of the algorithm is the following proposition:

Theorem C.14 ([DS06]) *Let f be a minimal and simple $\Sigma\Pi\Sigma$ formula which is identically zero. Let f have degree $d\geq 2$, and the fan-in of the top Σ gate $k\geq 3$. Than $rank(f)\leq 2^{O(k^2)}(\log d)^{k-2}$.*

Whether a formula f of size m, degree d and rank r is identically equal to zero, can be tested in time $\mathrm{poly}(m,d^r)$, 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 C.14, this can be done in quasipolynomial time.

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 a proof of $f = 0$ of size $\text{poly}(m, d^r)$. For if f is in variables $x_1, \ldots x_n$, then we can find a formula $f^\star$ in variables $y_1, \ldots y_r$, degree d, and a polynomial size, and linear functions $g_1(\overline{x}), \ldots g_r(\overline{x})$, such that:

1. $f^\star(y_1 \ldots y_n)$ is identically zero, and
2. $f(\overline{x}) = f^\star(y_1/g_1(\overline{x}), \ldots y_k/g_k(\overline{x}))$ has a poly size proof.

By expressing $f^\star$ as a sum of monomials, $f^\star = 0$ has a proof of size $\text{poly}(m, d^r)$. 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 $\text{poly}(m, d^r)$.

Finally, when proving (in contrast to computing) $f = 0$, we can assume that f is simple and minimal, and Theorem C.14 gives quasipolynomial size proofs of $f = 0$, for a fixed k.

C.3 Discussion on Relations with Kayal-Saxena's PIT Algorithm

For a $\Sigma\Pi\Sigma$ formula of top fan-in $k = 3$ the algorithm of Kayal and Saxena [KS07b] runs as follows: assume that f is simple and let $\mathcal{C}$ be the set of linear forms in f. For every $l \in \mathcal{C}$ we check whether

$$f \text{mod } l = 0.$$

This can be done in polynomial time. Clearly, if $f = 0$ then $f \text{mod } l = 0$ for every $l \in \mathcal{C}$. The crucial observation of [KS07b] is that the converse is also true: if $f \text{mod} l = 0$ for every $l \in \mathcal{C}$ then $f = 0$. For we then have

$$f \text{mod} (\prod \mathcal{C}) = 0$$

and hence

$$f \text{modRad} (\prod \mathcal{C}) = 0.$$

By the ABC lemma, $deg(Rad(\prod \mathcal{C})) > deg(f)$, which implies that $f = 0$.

In an equational proof, we can check each of the conditions $f \text{mod } l = 0$. Apparently, if we want to use this information in an equational proof, we must actually divide f by l, that is, to prove that

$$f = f' \cdot l,$$

for some f'. The formula f' can be more complicated than f, which prevents the iteration of this procedure.

D Proofs Omitted from Section 4 – Lower Bounds

D.1 Full Equational Proofs over Specific Rings

Let $\mathcal{R}$ be an arbitrary ring. Consider the equation

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

where $x_i, i = 1, \ldots, n$ are variables and $a_i, b_i, i = 1, \ldots, n$ are elements of $\mathcal{R}$. For $X \subseteq [n]$, let Γ_X be the formula $\prod_{i \in X} a_i \cdot \prod_{i \in [n] \setminus X} b_i$. Let $\mathcal{R}^\star$ be the ring of polynomials in variables $a_i, b_i, i \in [n]$ over $\mathcal{R}$.

For $H \subseteq \mathcal{R}^\star$, let $J(H)$ be the ideal generated by the polynomials in H. Let $I := J(\Gamma_X, X \subseteq [n])$, and let

$$\mathcal{S} := \mathcal{R}^\star / I.$$

In order to prove Theorem D.2, we first prove the following lemma:

Lemma D.1 *Let $H \subseteq \mathcal{R}^\star$. If $I = J(H)$ then $|H| \geq 2^n$.*

Proof: For a polynomial h, let $h^{(k)}$ denote its k-th homogeneous part. I is generated by homogeneous polynomials of degree n, and hence for every $g \in I$ and $k < n$, $g^{(k)} = 0$. Moreover, we can assume that also $g^{(k)} = 0$, for $k > n$, i.e., $h \in H$ are homogeneous polynomials of degree n. This follows from the fact that if $\Gamma_X = \sum_{h \in H} h \cdot g_h$ then $\Gamma_X = \sum_{h \in H} h^{(n)} \cdot g_h^{(0)}$. If H are homogeneous polynomials of degree n s.t. $\Gamma_X \in J(H)$, then Γ_X is a linear combination 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 vector of its coefficients. The set $\Gamma_X, X \subseteq [n]$ is linearly independent, is of size 2^n, and hence $|H| \geq 2^n$. ∎

Theorem D.2 *Consider equation (E) as an equation over $\mathcal{S}$, where the constants a_i, b_i are identified with the respective polynomials a_i, b_i in $\mathcal{S}$. Then (E) is an identity. Moreover, every equational proof of (E) over $\mathcal{S}$ contains at least 2^n lines.*

Proof: That (E) is an identity follows from (2) on page 12. Moreover, (2) implies that for every ideal J, (E) is an identity in $R^\star/J$ iff $I \subseteq J$.

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. We can assume that the constant symbols in P are presented as elements of the polynomial ring $R^\star$, in such a way that different elements of $R^\star$ represent different elements of S. Let us define the set $H \subseteq R^\star$ as follows: if P contains the constant axioms $g_3 = g_1 + g_2$ resp. $g_3 = g_1 \cdot g_2$, we add to H the polynomials $g_3 - (g_1 + g_2)$ resp. $g_3 - (g_1 \cdot g_2)$. Then $|H| \leq m$ and from the definition, $H \subseteq I$. Hence $J(H) \subseteq I$. P is a correct proof over the ring $R^\star/J(H)$, since every line of P is satisfied in this ring, and therefore (E) is an identity in $R^\star/J(H)$. Hence $I \subseteq J(H)$, and finally $J(H) = I$. By the previous lemma $|H| \geq 2^n$, an therefore $m \geq 2^n$. ∎

D.2 One-Way Proofs over Infinite Rings

Recall that (D) is the equation

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

where $x_i, i = 1, \ldots, n$ are variables and $a_i, b_i, c_i, d_i \in F$ if $i \in [n]$. (D) can be written as

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

where $\Gamma_X = \prod_{i \in X} a_i \cdot \prod_{i \in [n] \setminus X} b_i + \prod_{i \in X} c_i \cdot \prod_{i \in [n] \setminus X} d_i$, and hence (D) is an identity iff $\Gamma_X = 0$ for every $X \subseteq [n]$.

Let $a_i, b_i, c_i, d_i, i \in [n]$ be integers. $\mathsf{Span}(a_i, b_i, c_i, d_i, i \in [n])$ will be the set of integers of the following form:

1. $\prod_{i\in X} a_i \cdot \prod_{i\in Y} b_i$,
2. $\prod_{i\in X} c_i \cdot \prod_{i\in Y} d_i$,

where X, Y are disjoint subsets of $[n]$ s.t. $X \cup Y \neq \emptyset$.

We say that $a_i, b_i, c_i, d_i, i \in [n]$ have *independent span*, if $0, 1 \notin \mathsf{Span}(a_i, b_i, c_i, d_i, i \in [n])$, and every $c \in \mathsf{Span}(a_i, b_i, c_i, d_i, i \in [n])$ can be uniquely expressed from $a_i, b_i, c_i, d_i, i \in [n]$ as 1) or 2).

Lemma D.3 *Let F be an infinite field. Then there exist $a_i, b_i, c_i, d_i, i \in [n]$ in F such that they have independent span and (D) is an identity. If F contains Q, then they can be chosen as rational numbers of the form p/q with p, q integers with absolute values $\leq 2^{O(n^2)}$.*

Proof: Let R be the ring of polynomials $F[a_i, b_i, c_i, d_i, i \in [n]]$. Let Δ be the set of polynomials of the form

1. h, $h - 1$,
2. $h - g$,

where h, g are different polynomials of the form 1) or 2) from the definition of Span. It is sufficient to find $v \in F^{4n}$ s.t. for every $X \subseteq [n]$, $\Gamma_X(v) = 0$ and for every $f \in \Delta$, $f(v) \neq 0$. The first condition will guarantee that (D) is an identity, and the latter that the span of v is independent.

In order to have $\Gamma_X = 0$ for every $X \subseteq [n]$ is to choose some $z_1, \ldots z_n$, and let the coefficients satisfy the equations

$$b_i = a_i \cdot z_i,\ d_i = c_i \cdot z_i,\ i \in [n], \qquad \text{and} \qquad \prod_{i\in[n]} a_i + \prod_{i\in[n]} c_i = 0.$$

Let $R^\star$ be the ring of polynomials $F[a_i, b_i, z_i, i \in [n]]$. Let $I^\star \subseteq R^\star$ be the ideal generated by $\lambda := \prod_{i\in[n]} a_i + \prod_{i\in[n]} c_i$. Since λ is irreducible, $I^\star$ is a prime ideal. For a polynomial $f \in R$ define $f^\star \in R^\star$ as $f(b_i/(a_i \cdot z_i), d_i/(c_i \cdot z_i), i \in [n])$. Let $I := \{f \in R, f^\star \in I^\star\}$. Then also $I \subseteq R$ is a prime ideal. Moreover, $\Gamma_X \in I$ for every $X \subseteq [n]$. Let us show that for every $f \in \Delta$, f is not in I resp. $f^\star \notin I^\star$. If f is a polynomial from the definition of Span then $f^\star$ is of the form

$$f^1_{X,Y} = \prod_{i\in X\cup Y} a_i \cdot \prod_{i\in Y} z_i, \text{ or } \qquad f^2_{X,Y} \prod_{i\in X\cup Y} c_i \cdot \prod_{i\in Y} z_i,$$

where X, Y are disjoint and at least one is not empty. We must show that for every such $X, Y \subseteq [n]$ and $X', Y' \subseteq [n]$ and $i, j = 1, 2$, i) $f^i_{X,Y} \notin I^\star$, $f^i_{X,Y} - 1 \notin I^\star$, and ii) if $f^i_{X,Y} - f^j_{X',Y'}$ then $X = X', Y = Y'$ and $i = j$. $I^\star$ is generated by λ which is homogeneous of degree n. Hence every $g \in I^\star$ has all monomials of degree at least n. This, together with the fact that I is prime, implies i). Moreover, λ does not contain the variables z_i, and hence if $g \in I^\star$ then $g(z_i/c_i) \in I^\star$. This implies that if $f^i_{X,Y} - f^j_{X',Y'} \in I^\star$ then $Y = Y'$. (Otherwise set some $z_i \in Y \setminus Y' \cup Y' \setminus Y$ to zero.) Setting all z_i to 1 in $f^i_{X,Y} - f^j_{X',Y'}$, we must obtain a polynomial with monomials of degree $\geq n$. Hence $X \cup Y = X' \cup Y = [n]$, and so $X = X'$. We also have $i = j$. Otherwise we would have $\prod_{i\in[n]} a_i - \prod_{i\in[n]} c_i \in I^\star$, which would imply that $\prod_{i\in[n]} a_i \in I^\star$. We have shown that $f \in \Delta$ implies $f \notin I$. Since I is prime, also $g \notin I$ where $g := \prod_\Delta f$. If we assume that F is algebraically closed, there exists a point $v \in F^{4n}$ s.t. $f(v) = 0$ for every $f \in I$ and $g(v) \neq 0$. Otherwise g would

vanish on the variety $V(I)$, and so $g \in Rad(I) = I$. Moreover, this v can be chosen in such way that $v_i \neq 0, i = 1, \ldots 4n$.

If F is not algebraically closed, let $\overline{F}$ be its algebraic closure. For $f \in R$, define f' to be the rational function in variables $a_1, \ldots a_n, c_2 \ldots c_n, z_1, \ldots z_n$, obtained from f by the substitution

$$b_i := a_i z_i,\ d_i = c_i z_i, \qquad c_1 := -(a_1 \cdot a_n)/(c_2 \ldots c_n) \qquad (\star).$$

Then Γ'_X are identically zero. Define Δ' as the set of rational functions of the form 1) h', $h' - 1$ and 2) $g' - h'$, where g, h are different polynomials from the definition of Span. The rational functions in Δ' are non-trivial, since by the above argument there exists a point in $\overline{F}^{3n-1}$ where they are non-zero. In general, if we have a set of m non-trivial rational functions of degree d in k variables, and $S \subseteq F$ is s.t. $|S| > m.d$ and the functions are defined on S, there exists $v \in S^k$ s.t. all the rational functions are non-zero at v. This implies that there exists $v \in F^{3n-1}$ s.t. for every $f \in \Delta'$, $f(v) \neq 0$. Moreover, Δ' contains $2^{O(n)}$ rational functions of degree $\leq O(n)$. Hence if F contains the integers, v can be chosen s.t. for every $i = 1, \ldots 3n-1$, v_i is an integer s.t. $v_i \leq 2^{O(n)}$. If we then compute b_i, d_i by means of $(\star)$, we obtain elements of F resp. Q with the desired properties. ∎

We need the following definitions.

1. *Symbolic coefficient* is a product of constant symbols.

2. *An expansion* of a formula f is a formula obtained from f by opening all the brackets in f. I.e., it is a sum of products of the form $s \cdot \alpha$, where s is a symbolic coefficient and α a monomial. s will be called *a symbolic coefficient of α in f*. (α can have more symbolic coefficients in f).

3. Let g be a subformula of f. Then $f(g/0)$ denotes the formula obtained by replacing g by 0 in f. Then $f(g^{\perp})$ is defined as follows: understand f as a tree. Then g determines a unique path from its source to the source of f. $f(g^{\perp})$ is a product of all formulas h such that the path contains a product gate $h \cdot h'$ or $h' \cdot h'$ s.t. the path proceeds to h'. If no such h exists, set $f(g^{\perp}) := 1$.

Lemma D.4 *Let $S = S_1, \ldots S_m$ be a one-way proof of (D), where the coefficients have independent span. If α is a monomial occurring in some S_i with a nonzero coefficient, then it has the form $\prod_{i \in X} x_i$, for some $X \subseteq [n]$.*

1. *If $\alpha = \prod_{i \in X} x_i$ has a nonzero symbolic coefficient in S_i then it has exactly two nonzero symbolic coefficients in S_i: one with the value $\prod_{i \in X} a_i \prod_{i \in [n] \setminus X} b_i$, and the other with value $\prod_{i \in X} c_i \prod_{i \in [n] \setminus X} d_i$. In the former case, if $s = s_1, \ldots s_k$ then s_j have values $\prod_{i \in X_j} a_i \prod_{i \in Y_j} b_i$, where $X_j, j = 1, \ldots k$ resp. $Y_j, j = 1, \ldots k$ form a disjoint cover of X resp. $[n] \setminus X$. Similarly in the latter case.*

2. *If S_i contains a formula of the form $C_1 + C_2$ where C_1 and C_2 are nonzero constants then $(C_1 + C_2)^{\perp}$ contains at most one α with a nonzero coefficient. In this case the coefficient has value 1, and $C_1 + C_2$ has value zero.*

Proof: That every monomial in the proof is of the form $\prod_{i \in X} x_i$ follows from the fact that a one-way proof is analytic.

Next, let us show that (1) implies (2). Assume that there exists a monomial α such that α has nonzero symbolic coefficient s in $(C_1 + C_2)^{\perp}$. Then α has both a coefficient $C_1 \cdot s$ and $C_2 \cdot s$ in S_i. Hence, by part (1), $C_1 s + C_2 s$ has value zero and so has $C_1 + C_2$. Also, part (1) implies that s has value 1. Otherwise s could be expressed both as $\prod_{i \in X} a_i \prod_{i \in Y} b_i$ and $\prod_{i \in X'} c_i \prod_{i \in Y'} d_i$. This also implies that no other β can occur in $(C_1 + C_2)^{\perp}$ with a nonzero coefficient, for otherwise α and β would have a symbolic coefficients in S_i of the same value, which is impossible by (1) and independence of span.

(2). Proceed by induction w.r. to lines in S. For S_1 the statement holds by the properties of (D). The only rules that change symbolic coefficients in S_i are constant rules.

The rules $f \cdot 0 \to 0$ and $f + 0 \to f$ can only decrease the number of symbolic coefficients with value zero. The rules $f \cdot 1 \to f$ and $f \to f \cdot 1$ only decrease/increase occurrences of 1 in symbolic coefficients. The rule $a \cdot b \to c$ preserves the statement.

Consider the rule $C_1 + C_2 \to C_3$, where both C_1, C_2 are nonzero (otherwise we can take it as an instance of the rule $f + 0 \to f$). So assume that the rule was applied to S_i. Let α be a monomial. Every symbolic coefficient s of α in S_{i+1} i) is a symbolic coefficient of α in $S_i((C_1 + C_2)/0)$, or ii) there exists s' a symbolic coefficient of α in $S_i((C_1 + C_2)^{\perp})$ such that s has the form $C_3 \cdot s'$ and α has symbolic coefficients $C_1 \cdot s'$, $C_2 \cdot s'$ in S_i. In the case ii), if some such s' is nonzero then by the inductive assumption, every symbolic coefficient of α in $S_i((C_1 + C_2)/0)$ is zero. In addition, by part (2), $C_3 = 0$ and so α does not have a non-zero symbolic coefficient in S_{i+1}. If there is no non-zero s' from ii), the statement follows immediately. ∎

Theorem D.5 *Let F be an infinite field. Then there exist $a_i, b_i, c_i, d_i, i \in [n]$ s.t. (D) is an identity, and every one-way proof of (D) must have at least 2^n proof lines. If F contains rational numbers, the coefficients can be chosen as $\frac{p}{q}$, where p, q are integers with $|p|, |q| \leq 2^{O(n^2)}$.*

Proof: By Lemma D.3, we can chose the coefficients in such a way that (D) is an identity and they have independent span. In particular, every monomial α of the form $\prod_{i \in X} x_i$ has a nonzero symbolic coefficient in (D). Let $S = S_1, \ldots S_m$ be a proof of (D). For every monomial α of the given form, there exists a line S_i such that α has a nonzero symbolic coefficient in S_i, but does not have a nonzero symbolic coefficient in S_{i+1}. This is possible only if S_i contains a term of the form $C_1 + C_2$, the rule $C_1 + C_2 \to 0$ is applied to S_i, and α has a nonzero coefficient in $(C_1 + C_2)^{\perp}$. By the previous Lemma, part (2), this can occur for at most one monomial at a given line. ∎

D.3 Regular Depth-3 Analytic Proofs

In this section we show that every regular depth-3 analytic proof of (Bin) must have exponential number of lines.

D.3.1 Notation and Terminology

Recall that every proof-line in an analytic proof (which is by definition a straight-line proof) is a formula (and not an equality). Each depth-3 $\Sigma\Pi\Sigma$ formula Φ in an analytic proof can be written as $\phi_1 + \ldots + \phi_k$ for some $k \geq 0$. Thus, we can think of each proof-line Φ in an analytic proof as a

multiset of $\Pi\Sigma$ *formulas*, where each $\Pi\Sigma$ formula in the multiset is a summand ϕ_i of Φ. An element of such a multiset will be called a *summand*.

Note that in every proof-line in an analytic proof at most one or two summands can change from one line to the consecutive line. In the latter case, it is by means of a distributivity rule. The elementary operation $(f+g)\cdot h \to f\cdot h + g\cdot h$ will be called the *distributivity-down* operation, and the converse elementary operation $f\cdot h + g\cdot \to (f+g)\cdot h$ will be called the *factoring* operation.

Definition D.1 (Descendant) *For two summands appearing in two different proof-lines, we define the* descendant *relation as the transitive closure of the following relation. For any summand f, f is a descendant of itself. Let S, T be two consecutive proof-lines, S precedes T, and let M, N be the corresponding multisets of S, T, respectively.*

Case 1: *Assume that $f \in M$ and that in $S \to T$, f transforms into $g \in N$. Then g is the descendant of f.*

Case 2: *Assume that $f \in M$ and that in $S \to T$, f transforms into a sum $g + h$ by means of distributivity down. In this case $g, h \in N$, and both g and h are the descendants of f.*

Case 3: *Assume that $f, g \in M$ and that in the proof f and g transform into $h \in N$ by means of distributivity up. Then h is the descendant of both f and g.*

Case 4: *Assume that $f \in M$ and f is not changed in $S \to T$. Then f occurs in both M and T, and f in M is the descendant of f in M.*

We say that a summand f is an ancestor of *g, if g is a descendant of f.*

We can think of an analytic proof with m proof-lines as a *graph* consisting of m levels, each level i contains the summands occurring in proof-line i as nodes, and such that each node in level i has an outgoing edge to its descendant(s) in the previous level $i-1$ (for $i > 1$).

D.3.2 Regular Analytic Symbolic Proofs

We define a fragment of analytic symbolic proofs, called *regular analytic symbolic proofs*. We shall use the following two definitions for that purpose.

For technical reasons we need to define the notion of *Atomic formulas* are essentially formulas computing single monomials:

Definition D.2 (Atomic and non-atomic formulas) *A formula Φ is* atomic *if it has the form $\phi_1 \times \cdots \times \phi_k$, for $k \geq 1$, where each ϕ_i $(1 \leq i \leq k)$ is either a variable or a sum of one or more field elements; otherwise, Φ is said to be* non-atomic.

Notation: Let π be an analytic depth-3 proof, and let f be a summand in f. We denote by $\mathsf{desc}(f)$ the set of all summands in π that are descendants of f, and by $\mathsf{ances}(f)$ the set of all summands in π that are ancestors of f.

The idea of the regularity condition of analytic symbolic proofs we are about to define is to guarantee that if a forward distribution rule is applied on $A \times (B + C)$, which breaks the formula into the sum of two terms $A \times B$ and $A \times C$, then the two formulas $A \times B$ and $A \times C$, as well as any other two formulas that originate from $A \times B$ and $A \times C$ (possibly also originating by other formulas), might not be united together again by means of the backward distributivity rule (in fact, this rule is the only rule that can "unite" two separate summands into a product formula) .

Definition D.3 (Regular analytic symbolic proofs) *Let π be an analytic symbolic proof. We say that π is a* regular analytic symbolic proof *(or* regular proof *for short), if for every factoring operation $f + g \to h$ in the proof, if h is non-atomic or has non-atomic descendants,* then f and g have no common ancestors *(that is,* $\mathsf{ances}(f) \cap \mathsf{ances}(g) = \emptyset$*).*

In other words, regular proofs are such that for every summand h with non-atomic descendants, h's ancestors induces a *tree* rooted in h.

Comment 7 *In the definition of regular proofs we need to specifically refer to non-atomic vertices, as otherwise some formulas computing the zero polynomial might not be provable (that is, one cannot derive* 0 *from them). Consider for example the formula* $(x+1) \times (x-1) - x \times x - 1$.

Proposition D.6 (Completeness of regular depth-3 analytic $\mathbb{P}(\mathcal{R})$ proofs) *Regular depth-*3 *analytic* $\mathbb{P}(\mathcal{R})$ *proofs constitute a complete and sound proof systems for all depth-*3 *identities* $f = 0$ *over* $\mathcal{R}$*.*

Proof: Soundness stems from induction on proof length, using the soundness of the rules. For the completeness, we can use the same completeness argument as in Theorem 1.1. That is, one starts from f and expands all its monomials by using the distributivity-down operation. By straightforward inspection, this process is *analytic and regular* (that is, conforms to the conditions of analytic regular proofs). After expanding all monomials, we get a sum of atomic formulas. We can now cancel out all the monomials one by one, and by assumption that $f = 0$ is a true identity, we can reach the 0 formula in the end. ∎

D.3.3 The Lower Bound Proof

Recall the identity (Bin_n) is:

$$(x+y)^n + \sum_{i=0,\ldots,n} a_n x^i y^{n-i} = 0.$$

The formula $(x+y)^n$ will be denoted by A, and B_i will be the formulas $a_i x^i y^{n-i}$, $i = 0, \ldots, n$.

Let $\mathcal{S} = (S_1, \ldots, S_t)$ be a regular depth-3 analytic proof of (Bin_n).

Notation: Let $\mathsf{udesc}(A)$ be the set of *unique descendants of* A, that is, those summands whose only ancestor in the initial line S_1 is A. Similarly we define $\mathsf{udesc}(B)$ as the set of summands whose only ancestors in the initial line are in the set $B_0, \ldots B_n$. The set $\mathsf{udesc}_0(A) \subseteq \mathsf{udesc}(A)$ is defined as the set of summands $f \in \mathsf{udesc}(A)$ such that every descendant of f other than f itself is not in $\mathsf{udesc}(A)$.

We say that a formula f is *non-trivial*, if it defines a non-zero polynomial. Every summand f in a depth-3 analytic proof of (Bin_n) is a product of depth one formulas in the variables x and y. If f is a non-trivial summand, the *mixed degree of* f is defined as the number of such formulas in f which define a linear form that depends on both x and y, i.e., a linear form $ax + by + c$ with a, b nonzero constants. If f is trivial, the mixed degree is zero. The mixed degree of f is denoted $m(f)$.

Lemma D.7 (Expansion of A) *Assume that for every $f \in \mathsf{udesc}_0(A)$, f has mixed degree at most s. Then $|\mathsf{udesc}_0(A)| \geq 2^{n-s}$.*

Proof: Let us consider the proof graph restricted to $\mathsf{udesc}(A)$. The regularity restriction implies that factoring is never applied to two formulas in $\mathsf{udesc}(A)$, and hence the graph is a binary tree. We assume the tree, call it T, to be directed from the root A towards the leaves in $\mathsf{udesc}_0(A)$. At the root is a formula of mixed degree n and the leaves are formulas of mixed degree at most s. Moreover,

1. if an inner node f has an out-degree one, and g is the only descendant of f, then $m(f) = m(g)$, and
2. if f has out-degree two with two descendants g, h then either i) $m(g), m(h) \geq m(f) - 1$, ii) $m(g) = 0$ and $m(h) = m(f)$, or iii) $m(h) = 0$ and $m(g) = m(f)$.

For 1), note that f and g are two equivalent formulas (up to ordering of addition and multiplication gates, addition of 0 constants and product by the 1 constants). Thus, if they are non-trivial then they are also products of equivalent depth-one formulas (again, up to ordering of addition and multiplication gates, addition of 0 constants and product by the 1 constants). 2) corresponds to an application of distributivity $f \to g + h$. Hence f is of the form $(l_1 + l_2)f_0$ and g resp. h are $l_1 f_0$ resp. $l_2 f_0$. If f is trivial then i) applies. Assume that f is non-trivial. Hence f_0 is non-trivial and at least one of l_1 and l_2 is non-trivial. If both l_1 and l_2 are non-trivial, the mixed degree of g resp. h is at least $m(f_0) \geq m(f) - 1$ and we obtain i). If l_1 is trivial then $m(g) = 0$ and $m(h) = m(f)$, since h defines a product of the same linear forms as f. This gives ii). The remaining case iii) is similar.

Let us now define T_0 to be a tree obtained from T by a) deleting all nodes with $m(f) = 0$, together with their successors, and b) identifying nodes f, g s.t. there exists a non-branching path form f to g. By b), T_0 is a full binary tree, i.e., a tree with every inner node of out-degree two, and by 2), the mixed degree decreases at every node at most by one. Hence T_0 has depth at least $n - s$ and it contains at least 2^{n-s} leaves. ∎

For a summand f, let us define the *syntactic mixed degree of* f as the number of depth one formulas in f containing both x and y. This includes, for instance, formulas like $0 \cdot x + y$, where the corresponding linear form does not depend on x, and we do not require f to be non-trivial. We denote the syntactic mixed degree by $m^\star(f)$. Clearly, $m^\star(f) \geq m(f)$.

Lemma D.8 (Key) *Every* $f \in \mathsf{udesc}(B)$ *has syntactic mixed degree at most* $\log(n+1)$.

Proof: For $f \in \mathsf{udesc}(B)$, define $\mathsf{ances}_0(f)$ to be the set of predecessors of f in the first line, that is, a subset of $B_0, \ldots B_n$.

We shall prove that for every $f \in \mathsf{udesc}(B)$,

$$|\mathsf{ances}_0(f)| \geq 2^{m^\star(f)}.$$

This is by induction on the number of proof lines t in $\mathcal{S}$. If $t = 1$, f is one of $B_0, \ldots B_n$ and hence $m^\star(f) = 0$ and $|\mathsf{ances}_0(f)| = 1$.

Let $t > 1$ and assume that f has been obtained by means of the factoring operation $h + g \to f$, where h, g appear on line S_{t-1}. Then h has the form $l_1 \cdot h_0$ and g the form $l_2 \cdot h_0$, and f is the formula $(l_1 + l_2)h_0$, where l_1, l_2 are depth-one. Hence $m^\star(g), m^\star(h) \geq m^\star(h_0) \geq m^\star(f) - 1$. By the inductive assumption $|\mathsf{ances}_0(g)| \geq 2^{m^\star(g)} \geq 2^{m^\star(f)-1}$ and $|\mathsf{ances}_0(h)| \geq 2^{m^\star(h)} \geq 2^{m^\star(f)-1}$. By the regularity

condition (note that f is non-atomic, provided that $m^\star(f) > 0$), $\mathsf{ances}_0(h) \cap \mathsf{ances}_0(g) = \emptyset$, and so $|\mathsf{ances}_0(f)| = |\mathsf{ances}_0(g)| + |\mathsf{ances}_0(h)| \geq 2^{m^\star(f)-1} + 2^{m^\star(f)-1} = 2^{m^\star(f)}$.

If f has been obtained by a different rule, it has exactly one predecessor g on the line $t-1$. Inspecting the rules, we see that $m^\star(f) \leq m^\star(g)$ and the statement follows.

Since $\mathsf{ances}_0(f) \subseteq B_0, \ldots B_n$, we obtain

$$n + 1 \geq 2^{m^\star(f)}.$$

and so $m^\star(f) \leq \log(n+1)$. ∎

Corollary D.9 *Every regular analytic depth-3 proof of* (Bin_n) *requires size* $2^{\Omega(n)}$.

Proof: Let $\mathcal{S}$ be a regular analytic depth-3 proof of (Bin_n). For every non-zero $f \in \mathsf{udesc}_0(A)$ there exists $g \in \mathsf{udesc}(B)$ such that the factoring operation is applied to f and g. Hence $m(f) \leq m^\star(f) \leq m^\star(g) + 1$. By the previous lemma we then have $m(f) \leq \log(n+1) + 1$. This, by lemma D.7 implies that $|\mathsf{udesc}_0(A)| \geq 2^{n-\log(n+1)-1}$. ∎