Polynomial Identity Testing for Depth 3 Circuits

Neeraj Kayal and Nitin Saxena [*]
Department of CSE
IIT Kanpur, India
{kayaln,nitinsa}@cse.iitk.ac.in

Abstract

We study the identity testing problem for depth 3 arithmetic circuits ($\Sigma\Pi\Sigma$ circuit). We give the first deterministic polynomial time identity test for $\Sigma\Pi\Sigma$ circuits with bounded top fanin. We also show that the rank *of a minimal and simple $\Sigma\Pi\Sigma$ circuit with bounded top fanin, computing zero, can be unbounded. These results answer the open questions posed by Klivans-Spielman [KS01] and Dvir-Shpilka [DS05].*

1 Introduction

Polynomial Identity Testing (PIT) is the following problem: given an arithmetic circuit $\mathcal{C}$ computing a polynomial $p(x_1, x_2, \cdots, x_n)$ over a field $\mathbb{F}$, determine if the polynomial is identically zero. Besides being an interesting problem in itself, many other well-known problems such as Primality Testing and Bipartite Matching also reduce to PIT. Moreover fundamental structural results in complexity theory such as IP=PSPACE and the PCP theorem involve the use of identity testing.

The first randomized algorithm for identity testing was discovered independently by Schwartz [Sch80] and Zippel [Zip79] and it involves evaluating the polynomial at a random point and accepting if and only if the polynomial evaluates to zero at that point. This was followed by randomized algorithms that used fewer random bits [CK97, LV98, AB03] and a derandomization of the polynomial involved in primality testing [AKS04] but a complete derandomization remains distant.

Recently, a surprising development was by Impaggliazzo and Kabanets [IK03] who showed that efficient deterministic algorithms for identity testing would also imply strong arithmetic circuit lower bounds. More specifically, they showed that if identity testing has an efficient deterministic polynomial time algorithm then NEXP does not have polynomial size *arithmetic* circuits. This result gave further impetus to research on this problem and subsequently algorithms were developed for some restricted models of arithmetic circuits.

Raz and Shpilka [RS04] gave a deterministic polynomial time algorithm for non-commutative formulas. Klivans and Spielman [KS01] noted that even for depth 3 circuits where the fanin of the topmost gate was bounded, deterministic identity testing was an open problem. Subsequently, Dvir and Shpilka [DS05] gave a deterministic *quasipolynomial time* algorithm for depth 3 arithmetic circuits ($\Sigma\Pi\Sigma$ circuits) where the fanin of the topmost gate is bounded (note that if the topmost gate is a Π gate than the polynomial is zero if and only if one of the factors is zero and the problem is then easily solved). In this paper, we resolve this problem and give a deterministic *polynomial time* algorithm for the identity testing of such $\Sigma\Pi\Sigma$ circuits. Our main theorem is:

Theorem 1.1. *There exists a deterministic algorithm that on input a circuit $\mathcal{C}$ of depth 3 and degree d over a field $\mathbb{F}$, determines if the polynomial computed by the circuit is identically zero in time poly(n, d^k), where k is the fanin of the topmost addition gate and n is the number of inputs. In particular if k is bounded, then we get a deterministic polynomial time algorithm for identity testing of depth 3 circuits.*

Dvir and Shpilka [DS05] gave a structural result for $\Sigma\Pi\Sigma$ circuits $\mathcal{C}$ with bounded top fanin that compute zero. Let rank($\mathcal{C}$) be the rank of the linear functions that appear in $\mathcal{C}$. Then they showed that such simple and minimal $\mathcal{C}$ can have rank atmost $polylog(d)$. They also asked whether the upper bound of rank can be improved to $O(k)$. We answer this in the negative by giving identities of the following form:

Theorem 1.2. *1) Let $\mathbb{F}$ be a field of characteristic 2. Then for any number $m \geq 1$, there is a minimal and simple $\Sigma\Pi\Sigma$ zero-circuit $\mathcal{C}$, over $\mathbb{F}$, having parameters: $(k, d, \text{rank}(\mathcal{C})) = (3, 2^{m-1}, m+1)$.*

2) Let $\mathbb{F}$ be a field of odd characteristic p. Then for any number $m \geq 1$, there is a minimal and sim-

[*] The authors are supported by research funding from Infosys Technologies Limited, Bangalore.

ple $\Sigma\Pi\Sigma$ zero-circuit $\mathcal{C}$, over $\mathbb{F}$, having parameters: $(k, d, \textit{rank}(\mathcal{C})) = (p, p^{m-1}, m)$.

Section 2 gives an overview of $\Sigma\Pi\Sigma$ circuits and section 3 describes the identity test for $\Sigma\Pi\Sigma$ circuits of bounded top fanin.

2 $\Sigma\Pi\Sigma$ Arithmetic Circuits

Proving lower bounds for general arithmetic circuits is one of the central problems of complexity theory. Due to the difficulty of the problem research has focused on restricted models like monotone circuits and bounded depth circuits. For monotone arithmetic circuits, exponential lower bounds on the size [SS77, JS80] and linear lower bounds on the depth [SS80, TT94] have been shown. However, only weak lower bounds are known for bounded depth arithmetic circuits [Pud94, RS01]. Thus, a more restricted model was considered – the model of depth 3 arithmetic circuits (also called $\Sigma\Pi\Sigma$ circuits if we assume alternate addition and multipication gates with addition gate at the top). A $\Sigma\Pi\Sigma$ circuit computes a polynomial of the form:

$$\mathcal{C}(\overline{x}) = \sum_{i=1}^{k} \prod_{j=1}^{d_i} L_{ij}(\overline{x}) \qquad (1)$$

where L_{ij}'s are homogeneous linear functions (or linear forms). Exponential lower bounds on the size of $\Sigma\Pi\Sigma$ arithmetic circuits has been shown over finite fields [GK98]. For general $\Sigma\Pi\Sigma$ circuits over infinite fields only the quadratic lower bound of [SW99] is known.

No efficient algorithm for identity testing of $\Sigma\Pi\Sigma$ circuits is known. Here we are interested in studying the identity testing problem for a restricted case of $\Sigma\Pi\Sigma$ circuits – when the top fanin is bounded. This case was posed as a challenge by Klivans and Spielman [KS01] and a *quasi-polynomial time* algorithm was given by Dvir and Shpilka [DS05].

2.1 Previous Approaches

Let $\mathcal{C}$ be a $\Sigma\Pi\Sigma$ circuit, as in Equation (1), computing the zero polynomial. We will call $\mathcal{C}$ to be *minimal* if no proper subset of the multiplication gates of $\mathcal{C}$ sums to zero. We say that $\mathcal{C}$ is *simple* if there is no linear function that appears in all the multiplication gates (up to a multiplicative constant). *Rank* of $\mathcal{C}$ is the rank of the linear forms appearing in $\mathcal{C}$.

The quasipolynomial time algorithm of [DS05] is based on the result – rank of a minimal and simple $\Sigma\Pi\Sigma$ circuit with bounded top fanin and computing zero is "small". Formally, the result says:

Theorem 2.1. (Thm 1.4 of [DS05]). Let $k \geq 3, d \geq 2$, and let $\mathcal{C} \equiv 0$ be a simple and minimal $\Sigma\Pi\Sigma$ circuit of degree d with k multiplication gates and n inputs, then $\text{rank}(\mathcal{C}) \leq 2^{O(k^2)} \log(d)^{k-2}$.

Effectively, this means that if we have such a circuit $\mathcal{C}$ and k is a constant then we can check whether it is zero or not in time $O(d^{\text{rank}(\mathcal{C})}) = 2^{O(\log(d)^{k-1})}$. This gave hope of finding a polynomial time algorithm if we can improve the upper bound on the $\text{rank}(\mathcal{C})$ to a constant (i.e. independent of d). Infact, [DS05] conjectured that $\text{rank}(\mathcal{C}) = O(k)$. Here we give an identity that contradicts this conjecture. Thus, methods of [DS05] are unlikely to give an efficient algorithm and we give new techniques in section 3 that solve the problem.

For $k = 3$ [DS05] shows that a minimal, simple $\Sigma\Pi\Sigma$ zero circuit should have rank $O(\log d)$. We show below that this bound is tight.

Lemma 2.2. *Define*

$$\begin{aligned}
&\mathcal{C}(x_1, \ldots, x_m, y) := \\
&\quad \prod_{\substack{b_1,\ldots,b_m \in \mathbb{F}_2 \\ b_1+\cdots+b_m \equiv 0 (\textit{mod } 2)}} (y + b_1x_1 + \cdots + b_mx_m) \\
&\quad + \prod_{\substack{b_1,\ldots,b_m \in \mathbb{F}_2 \\ b_1+\cdots+b_m \equiv 1 (\textit{mod } 2)}} (b_1x_1 + \cdots + b_mx_m) \\
&\quad + \prod_{\substack{b_1,\ldots,b_m \in \mathbb{F}_2 \\ b_1+\cdots+b_m \equiv 1 (\textit{mod } 2)}} (y + b_1x_1 + \cdots + b_mx_m)
\end{aligned}$$

Then, over $\mathbb{F}_2$, $\mathcal{C}$ is a simple and minimal $\Sigma\Pi\Sigma$ zero circuit of degree $d = 2^{m-1}$ with $k = 3$ multiplication gates and having "unbounded" $\textit{rank}(\mathcal{C}) = \log(d) + 2$.

Proof. For brevity denote the output of the three multiplication gates by T_1, T_2, T_3 in order.

Let $a_1, \ldots, a_m \in \mathbb{F}$ be such that $(a_1 + \cdots + a_m) = 1(\text{mod } 2)$. Then what is $\mathcal{C}$ modulo $(a_1x_1 + \cdots + a_mx_m)$? Since $(a_1x_1 + \cdots + a_mx_m)$ occurs as a factor of T_2 we deduce $T_2 = 0(\text{mod } a_1x_1 + \cdots + a_mx_m)$. Further,

$$\begin{aligned}
T_1 &= \prod_{\substack{b_1,\ldots,b_m \in \mathbb{F}_2 \\ b_1+\cdots+b_m \equiv 0 (\text{mod } 2)}} (y + b_1x_1 + \cdots + b_mx_m) \\
&\equiv \prod_{\substack{b_1,\ldots,b_m \in \mathbb{F}_2 \\ b_1+\cdots+b_m \equiv 0 (\text{mod } 2)}} (y + (a_1 + b_1)x_1 + \cdots \\
&\qquad \cdots + (a_m + b_m)x_m) \quad (\text{mod } a_1x_1 + \cdots + a_mx_m) \\
&\equiv \prod_{\substack{b_1,\ldots,b_m \in \mathbb{F}_2 \\ b_1+\cdots+b_m \equiv 1 (\text{mod } 2)}} (y + b_1x_1 + \cdots + b_mx_m) \\
&\qquad (\text{mod } a_1x_1 + \cdots + a_mx_m) \\
&\equiv T_3 \quad (\text{mod } a_1x_1 + \cdots + a_mx_m)
\end{aligned}$$

Thus, we deduce: $T_1 + T_2 + T_3 \equiv 0 \pmod{a_1x_1 + \cdots + a_mx_m}$ for any $a_1, \ldots, a_m \in \mathbb{F}$, $(a_1 + \cdots + a_m) = 1(\text{mod } 2)$. Also, notice that $T_1 = 0(\text{mod } y)$ and $T_2 = T_3(\text{mod } y)$ implying that $T_1 + T_2 + T_3 = 0(\text{mod } y)$. Thus, we get that:

$$\left(y \cdot \prod_{\substack{b_1,\ldots,b_m \in \mathbb{F}_2 \\ b_1+\cdots+b_m \equiv 1(\text{mod } 2)}} (b_1x_1 + \cdots + b_mx_m) \right)$$
$$\text{divides } \mathcal{C}(x_1, \ldots, x_m, y)$$

But the divisor above has a degree higher than that of $\mathcal{C}$ implying that $\mathcal{C} \equiv 0$ (see Lemma 3.4).

Moreover, it is easy to see that $\mathcal{C}$ is a minimal, simple $\Sigma\Pi\Sigma$ circuit of degree 2^{m-1}. ■

The above identity is over a very special field – $\mathbb{F}_2$. Are there minimal, simple $\Sigma\Pi\Sigma$ identities of bounded k but unbounded rank over any field $\mathbb{F}$? We are not sure about fields of characteristic 0 but over fields of prime characteristic the following result answers in the affirmative.

Lemma 2.3. *Let p be an odd prime. Define:*

$$\mathcal{C}(x_1, \ldots, x_m) :=$$
$$\sum_{i=0}^{p-1} \prod_{\substack{b_1,\ldots,b_m \in \mathbb{F}_p \\ b_1+\cdots+b_m \equiv i(\text{mod } p)}} (b_1x_1 + \cdots + b_mx_m)$$

Then, over $\mathbb{F}_p$, $\mathcal{C}$ is a simple and minimal $\Sigma\Pi\Sigma$ zero circuit of degree $d = p^{m-1}$ with $k = p$ multiplication gates and having "unbounded" rank$(\mathcal{C}) = \log_p(d) + 1$.

Proof. Fix an $i_0 \in \mathbb{F}_p$ and let $a_1, \ldots, a_m \in \mathbb{F}_p$ such that $(a_1 + \cdots + a_m) = i_0(\text{mod } p)$. Now we compute $\mathcal{C}$ modulo $(a_1x_1 + \cdots + a_mx_m)$:

$$\mathcal{C} = \sum_{i=0}^{p-1} \prod_{\substack{b_1,\ldots,b_m \in \mathbb{F}_p \\ b_1+\cdots+b_m \equiv i(\text{mod } p)}} (b_1x_1 + \cdots + b_mx_m)$$
$$\equiv \sum_{\substack{i=0 \\ i \neq i_0}}^{p-1} \prod_{\substack{b_1,\ldots,b_m \in \mathbb{F}_p \\ b_1+\cdots+b_m \equiv i(\text{mod } p)}} (b_1x_1 + \cdots + b_mx_m)$$
$$(\text{mod } a_1x_1 + \cdots + a_mx_m)$$
$$\equiv \sum_{\substack{i=0 \\ i \neq i_0}}^{p-1} \prod_{\substack{b_1,\ldots,b_m \in \mathbb{F}_p \\ b_1+\cdots+b_m \equiv i(\text{mod } p)}} ((b_1 - a_1)x_1 + \cdots$$
$$\cdots + +(b_m - a_m)x_m) \quad (\text{mod } a_1x_1 + \cdots + a_mx_m)$$
$$\equiv \sum_{i=1}^{p-1} \prod_{\substack{b_1,\ldots,b_m \in \mathbb{F}_p \\ b_1+\cdots+b_m \equiv i(\text{mod } p)}} (b_1x_1 + \cdots + b_mx_m)$$
$$(\text{mod } a_1x_1 + \cdots + a_mx_m)$$
$$\equiv \sum_{i=1}^{\frac{p-1}{2}} \left(\prod_{\substack{b_1,\ldots,b_m \in \mathbb{F}_p \\ b_1+\cdots+b_m \equiv i(\text{mod } p)}} (b_1x_1 + \cdots + b_mx_m) \quad + \right.$$
$$\left. \prod_{\substack{b_1,\ldots,b_m \in \mathbb{F}_p \\ b_1+\cdots+b_m \equiv -i(\text{mod } p)}} (b_1x_1 + \cdots + b_mx_m) \right)$$
$$(\text{mod } a_1x_1 + \cdots + a_mx_m)$$

$$\equiv \sum_{i=1}^{\frac{p-1}{2}} \left(\prod_{\substack{b_1,\ldots,b_m \in \mathbb{F}_p \\ b_1+\cdots+b_m \equiv i(\text{mod } p)}} (b_1x_1 + \cdots + b_mx_m) \quad + \right.$$
$$\left. (-1)^{p^{m-1}} \cdot \prod_{\substack{b_1,\ldots,b_m \in \mathbb{F}_p \\ b_1+\cdots+b_m \equiv i(\text{mod } p)}} (b_1x_1 + \cdots + b_mx_m) \right)$$
$$(\text{mod } a_1x_1 + \cdots + a_mx_m)$$
$$\equiv 0 \ (\text{mod } a_1x_1 + \cdots + a_mx_m)$$

Thus, we deduce that for any $a_1, \ldots, a_m \in \mathbb{F}_p$:

$$\mathcal{C}(x_1, \ldots, x_m) \equiv 0 \quad (\text{mod } a_1x_1 + \cdots + a_mx_m)$$
$$\Rightarrow \left(\prod_{a_1,\ldots,a_m \in \mathbb{F}_p} (a_1x_1 + \cdots + a_mx_m) \right)$$
$$\text{divides } \mathcal{C}(x_1, \ldots, x_m)$$

But the divisor above has a degree higher than that of $\mathcal{C}$ implying that $\mathcal{C} \equiv 0$ (see Lemma 3.4).

Moreover, it is easy to see that $\mathcal{C}$ is a minimal, simple $\Sigma\Pi\Sigma$ circuit of degree p^{m-1}. ■

2.2 Overview of Our Algorithm

In this section we give an overview of our algorithm. The input is a $\Sigma\Pi\Sigma$ circuit $\mathcal{C}(x_1, \ldots, x_n)$ having an addition gate at the top with fanin k and computing a polynomial of total degree atmost d over a field $\mathbb{F}$. Our algorithm is recursive such that in each recursive call k reduces while the base ring (initially, it was $\mathbb{F}$) becomes larger. The intermediate larger rings that appear are all ensured to be local. The dimension of the base ring (over $\mathbb{F}$) increases by a factor of atmost d in each recursive call and thus, the complexity comes out to be $poly(d^k, n)$ (assuming the field operations in $\mathbb{F}$ take constant time).

We will now demonstrate a snapshot of the algorithm. Let R be a local ring over the field $\mathbb{F}$ having maximal ideal $\mathcal{M}$. The circuit $\mathcal{C}(z_1, \ldots, z_n)$ in $R[z_1, \ldots, z_n]$ looks like:

$$\mathcal{C} = T_1 + T_2 + \cdots + T_k$$

where each T_i is a product of linear forms

$$T_i = L_{i1}L_{i2}\cdots L_{id}$$

and where each L_{ij} is a linear form:

$$L_{ij} = a_{ij0} + a_{ij1}z_1 + a_{ij2}z_2 + \cdots + a_{ijn}z_n$$

for some $a_{ij1}, a_{ij2}, \cdots, a_{ijn} \in \mathbb{F}$ and $a_{ij0} \in \mathcal{M}$. We want to check if $\mathcal{C}$ computes the identically zero polynomial over R. We do this by "suitably" picking "coprime" polynomials $p_1, \ldots, p_l$ and recursively verifying that:

$$\mathcal{C} \equiv 0 \ (\text{mod}\ p_i) \quad \text{for } 1 \le i \le l$$

By our version of Chinese Remaindering Theorem for local rings we deduce that:

$$\mathcal{C} \equiv 0 \ (\text{mod} \prod_{i=1}^{l} p_i)$$

Our choice of the polynomials p_i ensures that the total degree of $\prod_{i=1}^{l} p_i(z_1, \ldots, z_n)$ is more than that of $\mathcal{C}(z_1, \ldots, z_n)$. Whence we deduce that $\mathcal{C}$ computes the identically zero polynomial over R.

Our choice of the polynomials p_i will ensure two things:

i) There is an invertible linear transformation τ on the variables $\overline{z}$ such that it 'simplifies' the polynomial p_i:

$$\tau \circ p_i(z_1, \ldots, z_n) = (z_1+m_1)\cdot(z_1+m_2)\cdots(z_1+m_s)$$

where, $m_j \in \mathcal{M}$. Thus, the ring $S_i := R[z_1]/(\tau \circ p_i)$ is a local ring.

ii) p_i 'occurs' in one of the T_j's thus, $\tau \circ \mathcal{C}$ can be viewed as a $\Sigma\Pi\Sigma$ circuit with top fanin atmost $(k-1)$, total degree d and $(n-1)$ variate over the (larger) ring S_i. Thus, we can check $\mathcal{C} = 0 \ (\text{mod}\ p_i)$ by checking $\tau \circ \mathcal{C} = 0$ over S_i recursively.

3 The Algorithm

In this section we give a deterministic polynomial time algorithm that tests whether a given $\Sigma\Pi\Sigma$ arithmetic circuit of bounded top fanin computes the zero polynomial. The basic idea is the same as used in the proof of Lemmas 2.2 and 2.3– look at the values of $\mathcal{C}$ modulo product of linear forms. Here, the polynomials that we get will be over some *local* ring $R \supset \mathbb{F}$ instead of being over $\mathbb{F}$ but we can show that some of the "nice" properties of $\mathbb{F}[z_1, \ldots, z_n]$ continue to hold in $R[z_1, \ldots, z_n]$. Specifically, we need that:

1) if *coprime* $f(z_1, \ldots, z_n)$, $g(z_1, \ldots, z_n)$ divide $p(z_1, \ldots, z_n)$ then $f \cdot g \mid p$ in R.

2) if the total degree of $f(z_1, \ldots, z_n)$ is more than that of $p(z_1, \ldots, z_n)$ then over R:

$$f(z_1, \ldots, z_n) | p(z_1, \ldots, z_n) \ \Rightarrow \ p(z_1, \ldots, z_n) = 0$$

3.1 Local Rings

3.1.1 Preliminaries

In this article we shall be working with some special kinds of rings known as *local* rings. For the sake of completeness we define local rings and mention their elementary properties. We refer the interested reader to [McD74] for further properties of such rings.

Definition 3.1. A commutative ring R is said to be a *local ring* if it has a unique maximal ideal.

Example: Consider ring $R = \mathbb{F}[x_1, x_2]/(x_1^3, x_2(x_2 + x_1))$. Observe that R is a local ring with the unique maximal ideal $\mathcal{M}$ generated by x_1, x_2. Also note that $\mathcal{M}$ is the set of *nilpotent* elements, i.e., for any element $m \in \mathcal{M}$ there is a $k \ge 1$ such that $m^k = 0$ in R.

Indeed we shall be considering rings R which are finite dimensional commutative algebras over some field $\mathbb{F}$. In that case, the unique maximal ideal $\mathcal{M}$ of R consists of all the nilpotent elements of R. Moreover, every element $r \in R$ can be uniquely written as $r = \alpha + m,\ \alpha \in \mathbb{F}$ and $m \in \mathcal{M}$. This implies that there is a unique ring homomorphism $\phi : R \to \mathbb{F}$ such that $\phi(\alpha + m) = \alpha$. Further, if the dimension of R over $\mathbb{F}$ is d then there is an integer $t \in [d]$ such that the product of any t (not necessarily distinct) elements of $\mathcal{M}$ is zero in R.

We can define the *ring of fractions* S^{fr} of a ring S as the set of elements $\frac{u}{v}$ where, $u, v \in S$ and v is not a zero divisor of S. Clearly, S^{fr} is also a ring. We will be considering polynomials over rings S and S^{fr}. A polynomial $f(z) \in S[z]$ is called *monic* if its leading coefficient is a unit of S. The following is a well known lemma that relates polynomial factorization over the ring S to its ring of fractions S^{fr}.

Lemma 3.2 (Gauss' Lemma)**.** *Suppose $f, g \in S[z]$ and $h \in S^{fr}[z]$ such that: $f = gh$. If g is monic then $h \in S[z]$.*

Proof. A proof for the case of $S = \mathbb{Z}$ can be found in any algebra text, eg. [NZM91]. The proof for general S is similar in spirit. ∎

3.1.2 Properties of multivariate polynomials over local rings

In this section we will show that (multivariate) polynomials over local rings have divisibility properties analogous to those of polynomials over fields. Throughout this section we will assume that R is a local ring over a field $\mathbb{F}$ and the natural ring homomorphism from R to $\mathbb{F}$ is ϕ. The map ϕ can be extended in the natural way to a homomorphism from $R[z_1, z_2, \cdots, z_n]$ to $\mathbb{F}[z_1, z_2, \cdots, z_n]$. The unique maximal ideal of R is $\mathcal{M}$ and t is the least integer such that $\mathcal{M}^t = 0$ in R.

Lemma 3.3. *Let R be a local ring and $p, f, g \in R[z_1, z_2, \cdots z_n]$ be multivariate polynomials such that $\phi(f)$ and $\phi(g)$ are coprime. Moreover,*

$$p \equiv 0 \pmod{f}$$

$$p \equiv 0 \pmod{g}$$

$$\textit{Then} \quad p \equiv 0 \pmod{fg}$$

Proof. Let the (total) degrees of $\phi(f)$ and $\phi(g)$ be d_f and d_g respectively. Then by applying a suitable invertible linear transformation on the variables $z_1, z_2, \cdots, z_n$ if needed, we can assume without loss of generality that the coefficients of $z_n^{d_f}$ in f and that of $z_n^{d_g}$ in g are both units of R. Consequently, in the product fg the coefficient of $z_n^{d_f+d_g}$ is also a unit.

Now think of f and g as polynomials in one variable z_n with coefficients coming from the ring of fractions – $R(z_1, z_2, \cdots, z_{n-1})$ – of $R[z_1, z_2, \cdots, z_{n-1}]$. Now since $\phi(f)$ and $\phi(g)$ are coprime over $\mathbb{F}$, they are also coprime as univariate polynomials in z_n over the function field $\mathbb{F}(z_1, z_2, \cdots, z_{n-1})$. Consequently, there exists $a, b \in \mathbb{F}(z_1, z_2, \cdots, z_{n-1})[z_n]$ such that:

$$a\phi(f) + b\phi(g) = 1 \text{ in } \mathbb{F}(z_1, z_2, \cdots, z_{n-1})[z_n].$$

That is,

$$af + bg = 1 \text{ in } (R/\mathcal{M})(z_1, z_2, \cdots, z_{n-1})[z_n].$$

By the well known Hensel Lifting lemma we get that there exist $a^*, b^* \in R(z_1, z_2, \cdots, z_{n-1})[z_n]$ such that:

$$a^*f + b^*g = 1 \text{ in } (R/\mathcal{M}^t)(z_1, z_2, \cdots, z_{n-1})[z_n]$$
$$\text{which is } R(z_1, z_2, \cdots, z_{n-1})[z_n]$$

Now by the assumption of the lemma:

$$\begin{array}{rrl}
 & p \equiv 0 & \pmod{f} \\
\Rightarrow & p = fq & \text{for some } q \text{ in } R[z_1, z_2, \cdots, z_{n-1}][z_n] \\
also, & p \equiv 0 & \pmod{g} \\
\Rightarrow & fq \equiv 0 & \pmod{g} \\
\Rightarrow & a^*fq \equiv 0 & \pmod{g} \text{ in } R(z_1, z_2, \cdots, z_{n-1})[z_n] \\
\Rightarrow & q \equiv 0 & \pmod{g} \text{ in } R(z_1, z_2, \cdots, z_{n-1})[z_n] \\
\therefore & p = fgh & \text{for some } h \text{ in } R(z_1, z_2, \cdots, z_{n-1})[z_n]
\end{array}$$

Since, the leading coefficient of z_n in fg is in R^* and p, fg are in $R[z_1, z_2, \cdots, z_{n-1}][z_n]$, therefore by Gauss Lemma (see Lemma 3.2) we get that in fact $h \in R[z_1, z_2, \cdots, z_{n-1}][z_n]$ and so

$$p \equiv 0 \pmod{fg} \text{ in } R[z_1, z_2, \cdots, z_n]$$

∎

Lemma 3.4. *Suppose that $p, f \in R[z_1, z_2, \cdots, z_n]$ and p has total degree d. Moreover f has total degree $d' > d$ and contains at least one monomial of degree d' whose coefficient is a unit in R. Then, $p \equiv 0 \pmod{f} \Rightarrow p = 0$ in $R[z_1, z_2, \cdots, z_n]$.*

Proof.
Since $p \equiv 0 \pmod{f}$ we have

$$p = fg \text{ for some } g \in R[z_1, z_2, \cdots, z_n].$$

By applying a suitable linear transformation of the variables $z_1, z_2, \cdots, z_n$, if needed, we can assume that the coefficient of $z_n^{d'}$ in f is a unit of R. Now view p, f, g as univariate polynomials in z_n over the ring $R[z_1, z_2, \cdots, z_{n-1}]$ and let the degree of g with respect to z_n be t. Then the coefficient of $z_n^{d'+t}$ on the rhs is non-zero whereas all the terms on the lhs have degree at most $d < d' + t$, a contradiction. ∎

3.2 Description of the Identity Test

Let the given circuit over field $\mathbb{F}$ be:

$$\mathcal{C}(x_1, \ldots, x_n) = T_1 + T_2 + \cdots + T_k$$

where, for all $i \in [k]$, $T_i = \prod_{j=1}^{d} L_{ij}$. Further, $L_{ij} = \sum_{k=1}^{n} a_{ijk}x_k$ where $a_{ijk} \in \mathbb{F}$.

In this section we will say that polynomials $a, b, c, d \in \mathbb{F}[z_1, \ldots, z_n]$ satisfy $a \equiv b \pmod{c, d}$ iff

$$(a(z_1, \ldots, z_n) - b(z_1, \ldots, z_n))$$
$$\text{is in } \mathbb{F}[z_1, \ldots, z_n]/(c(z_1, \ldots, z_n), d(z_1, \ldots, z_n))$$

Input: The two inputs to the algorithm are:

- $\langle T_1, \ldots, T_k \rangle$, where $k \geq 1$ and T_i's are products of linear forms in $\mathbb{F}[x_1, \ldots, x_n]$ and have total degree d.

- $\langle l_{11} \cdots l_{1e_1},\ \ldots,\ l_{m1} \cdots l_{me_m} \rangle$, where $m \geq 0$, $e_1, \ldots, e_m \in [d]$ and l_{ij}'s are linear forms in $\mathbb{F}[x_1, \ldots, x_n]$ such that:

$$\begin{array}{llllll} l_{11} & = \ldots & = l_{1e_1} & = & x_1 \\ l_{21} & = \ldots & = l_{2e_2} & = & x_2 \ (\mathrm{mod}\ x_1) \\ l_{31} & = \ldots & = l_{3e_3} & = & x_3 \ (\mathrm{mod}\ x_1, x_2) \\ & \vdots & \vdots & & \\ l_{m1} & = \ldots & = l_{me_m} & = & x_m \ (\mathrm{mod}\ x_1, \ldots, x_{m-1}) \end{array}$$

Output: The output of the algorithm, **ID**$(\langle T_1, \ldots, T_k \rangle, \langle l_{11} \cdots l_{1e_1}, \ldots, l_{m1} \cdots l_{me_m} \rangle)$, is YES iff

$$T_1 + \cdots + T_k \ = \ 0 \ \ (\mathrm{mod}\ l_{11} \cdots l_{1e_1}, \ldots, l_{m1} \cdots l_{me_m}).$$

ID$(\ \langle T_1, \ldots, T_k \rangle\ ,\ \langle l_{11} \cdots l_{1e_1}, \ldots, l_{m1} \cdots l_{me_m} \rangle)\ )$:

Step 1: (Defining a local ring) Let us define a *local* ring R as:

$$R \stackrel{\text{def}}{=} \mathbb{F}[x_1, \ldots, x_m]/\mathcal{I}$$

where, $\mathcal{I} = (l_{11} \cdots l_{1e_1}, \ldots, l_{m1} \cdots l_{me_m})$. Thus, each T_i can be viewed as a polynomial in $R[x_{m+1}, \ldots, x_n]$ and we want to check whether

$$T_1 + \cdots + T_k \ = \ 0 \quad \text{in } R.$$

We will say that two polynomials $a(x_1, \ldots, a_n)$, $b(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_n]$ are *coprime over* R if $a(x_1, \ldots, a_n)(\mathrm{mod}\ x_1, \ldots, x_m)$ and $b(x_1, \ldots, x_n)(\mathrm{mod}\ x_1, \ldots, x_m)$ are coprime in the standard sense over $\mathbb{F}$.

Step 2: (Base case of one multiplication gate) If $k = 1$ then we need to check whether

$$T_1 = 0 \ (\mathrm{mod}\ \mathcal{I}).$$

Let $f(x_1, \ldots, x_m)$ be the product of those linear factors of T_1 that contain only the variables $x_1, \ldots, x_m$. Viewing T_1 as a polynomial over the ring R, the above congruence holds iff

$$f(x_1, \ldots, x_m) = 0 \ (\mathrm{mod}\ \mathcal{I}).$$

By simply expanding out f, the above condition can be checked in time $poly(d^m)$ and then **output** the result.

Step 3: (When all the T_i's are in R) Let d' be the maximum degree of $T_1, \ldots, T_k$ as polynomials over R.

If $d' = 0$ then each of $T_1, \ldots, T_k$ is in the ring R and hence we can check

$$T_1 + \cdots + T_k = 0 \ (\mathrm{mod}\ \mathcal{I})$$

in time $poly(d^m)$ and **output** the result.

Thus, in the subsequent steps $k \geq 2$ and $d' \geq 1$.

Step 4: (Collecting "useful" linear forms) Form the *largest* set $S = \{s_1, \ldots, s_B\}$ of linear forms in $\mathbb{F}[x_{m+1}, \ldots, x_n]$ such that the elements of S satisfy:

- for each $i \in [B]$ there is a $j \in [k]$ such that $(s_i + r)$ is a linear factor of T_j for some $r \in R$.
- for every $i \neq j \in [B]$, s_i, s_j are coprime.

Since $d' \geq 1$, S is not empty. For each $i \in [B]$, let $f_i \in [d']$ be the largest number such that $(s_i + r_1), \ldots, (s_i + r_{f_i})$ are linear factors (with repetition) of some T_j, say T_{π_i}, where $r_1, \ldots, r_{f_i} \in R$. Furthermore, for an $i \in [B]$, let $s_{i1}, \ldots, s_{if_i} \in \mathbb{F}[x_1, \ldots, x_n]$ be all the linear forms (with repetition) that occur in T_{π_i} and are congruent to $s_i(\mathrm{mod}\ x_1, \ldots, x_m)$.

The way we have defined f_i's we have that for any $j \in [k]$, s_i can occur atmost f_i times among the linear factors of T_j taken $(\mathrm{mod}\ x_1, \ldots, x_m)$. Thus, we get the following bound:

$$(f_1 + \ldots + f_B) \geq d'.$$

If $(f_1 + \ldots + f_B) = d'$ then form the set U of T_j's that produce monomials (in the variables $x_{m+1}, \ldots, x_n$) of degree d'. Wlog let $U = \{T_1, \ldots, T_{k'}\}$ and note that $k' \geq 1$. For $i \in [k']$, let:

$$T_i = g_i(x_1, \ldots, x_m) \cdot \left(\prod_{j=1}^{f_1} (s_1 + r_{i,1j}) \right) \cdots$$
$$\cdots \left(\prod_{j=1}^{f_B} (s_B + r_{i,Bj}) \right)$$

where, for all $i_1 \in [k']$, $i_2 \in [B]$, $i_3 \in [d']$, $r_{i_1,i_2i_3} \in R$ and $g_{i_1} \in \mathbb{F}[x_1, \ldots, x_m]$.

Note that the coefficient of any degree d' monomial (in the variables $x_{m+1}, \ldots, x_n$) in $T_1 + \ldots + T_{k'}$ is a multiple (in $\mathbb{F}$) of:

$$\sum_{i \in [k']} g_i(x_1, \ldots, x_m).$$

We can clearly check whether this is zero $(\mathrm{mod}\ \mathcal{I})$, in time $poly(d^m)$. If it is not zero then **output** NO.

Step 5: (Going modulo various products of linear forms) For $i \in [B]$, define a linear tranformation σ_i acting on the variables $x_1, \ldots, x_n$ such that σ_i fixes $x_1, \ldots, x_m$, sends $s_i \mapsto x_{m+1}$ and transforms $x_{m+2}, \ldots, x_n$ such that it is an invertible linear map. Let $B' \in [B]$ be such that $B' = B$ if $(f_1 + \ldots + f_B) = d'$ otherwise B' is the smallest number such that $(f_1 + \ldots + f_{B'}) > d'$.

Output a YES iff each of the following recursive calls return a YES:

$$\textbf{ID}\Big(\ \langle \sigma_1(T_i) \rangle_{i \in [k] \setminus \{\pi_1\}}\ ,\ \langle l_{11} \cdots l_{1e_1}, \ldots, l_{m1} \cdots l_{me_m}, \sigma_1(s_{11} \ldots s_{1f_1}) \rangle\ \Big)$$

$$\vdots \qquad \vdots$$

$$\textbf{ID}\Big(\ \langle \sigma_{B'}(T_i) \rangle_{i \in [k] \setminus \{\pi_{B'}\}}\ ,\ \Big\langle l_{11} \cdots l_{1e_1}, \ldots, l_{m1} \cdots l_{me_m}, \sigma_{B'}(s_{B'1} \ldots s_{B'f_{B'}}) \Big\rangle\ \Big)$$

3.3 Proof of Correctness

We continue using the notation set in the last subsection. The claim here is summarized as:

Theorem 3.5. *$\textbf{ID}(\ \langle T_1, \ldots, T_{\tilde{k}} \rangle\ ,\ \langle 0 \rangle\ )$ returns YES iff $T_1 + \cdots + T_{\tilde{k}} = 0$ in $\mathbb{F}$. Furthermore, the time taken is $poly(n, d^{\tilde{k}})$.*

Proof. Note that in all the recursive calls that $\textbf{ID}(\langle T_1, \ldots, T_{\tilde{k}} \rangle\ ,\ \langle 0 \rangle)$ makes to $\textbf{ID}(\cdot, \cdot)$ the size of the first argument reduces by one and that of the second argument increases by one, thus $m \leq \tilde{k}$. Therefore, if $h(k)$ denotes the time taken by $\textbf{ID}(\ \langle T_1, \ldots, T_k \rangle\ ,\ \langle l_{11} \cdots l_{1e_1}, \ldots, l_{m1} \cdots l_{me_m} \rangle\ )$ then we have the following recurrence:

$$\begin{aligned} h(k) &\leq B' \cdot h(k-1) + poly(n, d^m) \\ &\leq (d+1) \cdot h(k-1) + poly(n, d^{\tilde{k}}) \end{aligned}$$

Thus, we get that $h(\tilde{k}) = poly(n, d^{\tilde{k}})$.

To show that the output of $\textbf{ID}(\langle T_1, \ldots, T_{\tilde{k}} \rangle\ , \langle 0 \rangle)$ is correct we prove the correctness of
$\textbf{ID}(\ \langle T_1, \ldots, T_k \rangle\ ,\ \langle l_{11} \cdots l_{1e_1}, \ldots, l_{m1} \cdots l_{me_m} \rangle\ )$ by induction on k:

Claim 3.5.1. *$\textbf{ID}(\ \langle T_1, \ldots, T_k \rangle\ ,\ \langle l_{11} \cdots l_{1e_1}, \ldots, l_{m1} \cdots l_{me_m} \rangle\ )$ returns YES iff*

$$T_1 + \cdots + T_k = 0 \ (mod\ l_{11} \cdots l_{1e_1}, \ldots, l_{m1} \cdots l_{me_m}).$$

Proof of Claim 3.5.1. The base case of the induction is when $k = 1$, handled by Step 2. In this case T_1 can be written as $f(x_1, \ldots, x_m) \cdot F(x_{m+1}, \ldots, x_n)$ such that $f \in R$ while $F \in R[x_{m+1}, \cdots, x_n]$ with coefficients of the highest degree monomials (in $x_{m+1}, \ldots, x_n$) of F coming from $\mathbb{F}$. Clearly, $T_1 = 0$ in R iff $f = 0 \pmod{\mathcal{I}}$. This can be checked by expanding out $f(x_1, \ldots, x_m)$, since the expansion will have atmost d^m terms we can do this in time $poly(d^m)$.

Now we assume that $k \geq 2$ and that the claim is true for values smaller than k. If all the linear forms occurring in $T_1, \ldots, T_k$ are in R then in Step 3 we just expand out T_i's and check whether the sum is zero $\pmod{\mathcal{I}}$. Otherwise in Step 4 we collect the maximum number of linear forms (possibly repeated) $\{s_{11}, \ldots, s_{1f_1}, \cdots, s_{B1}, \ldots, s_{Bf_B}\}$ such that for all $i \in [B]$, $s_{i1} \cdots s_{if_i}$ occurs in some T_j and the polynomials

$$\{s_{11} \cdots s_{1f_1}\ , \ldots,\ s_{B1} \cdots s_{Bf_B}\}$$

are mutually coprime over R.

Recall that d' is the maximum degree of $T_1, \ldots, T_k$ as polynomials in $R[x_{m+1}, \ldots, x_n]$. In Step 4 if we do not have "enough" linear forms i.e. $f_1 + \ldots + f_B = d'$ then observe that the sum of the degree d' terms in the expansion of $(T_1 + \ldots + T_k)$ is:

$$\left(\sum_{i \in [k']} g_i(x_1, \ldots, x_m) \right) \cdot s_1^{f_1} \cdots s_B^{f_B}$$

Thus, for $T_1 + \ldots + T_k$ to vanish $\pmod{\mathcal{I}}$ it is necessary that $\sum_{i \in [k']} g_i$ vanishes $\pmod{\mathcal{I}}$, which can be checked in time $poly(d^m)$. If it vanishes then we have:

$$\begin{aligned} &\text{degree of } (T_1 + \ldots + T_k) \text{ as polynomials over } R \text{ is } < d' \\ &\qquad \leq (f_1 + \ldots + f_{B'}) \end{aligned}$$

With this assurance we move on to the most "expensive" step – Step 5. Firstly, note that $\sigma_i(s_{i1}) = \ldots = \sigma_i(s_{if_i}) = \sigma_i(s_i) = x_{m+1} \pmod{x_1, \ldots, x_m}$ so the input of the B' calls to **ID** are well-formed. Observe that for any invertible linear transformation σ_i that is sending the variables $x_1, \ldots, x_n$ to their linear combinations we have:

$$\textbf{ID}\Big(\ \langle \sigma_i(T_j) \rangle_{j \in [k] \setminus \{\pi_i\}}\ ,\ \langle l_{11} \cdots l_{1e_1}, \ldots, l_{m1} \cdots l_{me_m}, \sigma_i(s_{i1} \ldots s_{if_i}) \rangle\ \Big)$$

$$\text{iff}$$

$$\textbf{ID}\Big(\ \langle T_j \rangle_{j \in [k] \setminus \{\pi_i\}}\ ,\ \langle l_{11} \cdots l_{1e_1}, \ldots, l_{m1} \cdots l_{me_m},\ s_{i1} \ldots s_{if_i} \rangle\ \Big)$$

Thus, induction hypothesis ensures that if the following two tests return YES:

$$\textbf{ID}\Big(\ \langle\sigma_1(T_j)\rangle_{j\in[k]\setminus\{\pi_1\}}\ ,\ \langle l_{11}\cdots l_{1e_1},\dots,l_{m1}\cdots l_{me_m},\sigma_1(s_{11}\dots s_{1f_1})\rangle\ )$$

and

$$\textbf{ID}\Big(\ \langle\sigma_2(T_j)\rangle_{j\in[k]\setminus\{\pi_2\}}\ ,\ \langle l_{11}\cdots l_{1e_1},\dots,l_{m1}\cdots l_{me_m},\sigma_2(s_{21}\dots s_{2f_2})\rangle\ )$$

then we can deduce that:

$$(T_1+\cdots+T_k)=0\ (\text{mod}\ \mathcal{I},\ s_{11}\dots s_{1f_1})\quad\text{and}$$

$$(T_1+\cdots+T_k)=0\ (\text{mod}\ \mathcal{I},\ s_{21}\dots s_{2f_2})$$

Since, $s_1,\ s_2$ were coprime over $\mathbb{F}$ we have that $s_{11}\dots s_{1f_1},\ s_{21}\dots s_{2f_2}$ are also coprime over R. Thus, by Lemma 3.3 we can combine the above two conditions to get:

$$(T_1+\cdots+T_k)=0\ (\text{mod}\ \mathcal{I},\ s_{11}\cdots s_{1f_1}\cdot s_{21}\cdots s_{2f_2})$$

By extending this argument, we get that if all the B' calls to **ID** return YES then:

$$(T_1+\cdots+T_k)=0\ (\text{mod}\ \mathcal{I},\ s_{11}\cdots s_{1f_1}\dots s_{B'1}\cdots s_{B'f_{B'}})$$

Now since the degree of $(s_{11}\cdots s_{1f_1}\dots s_{B'1}\cdots s_{B'f_{B'}})$ is more than the degree of $(T_1+\cdots+T_k)$ as polynomials over R, by Lemma 3.4 we conclude that:

$$T_1+\cdots+T_k=0\ (\text{mod}\ \mathcal{I}).$$

Thus, when the algorithm returns YES it is right. When the algorithm returns NO it is easy to see that $(T_1+\cdots+T_k)$ is indeed not zero in R. □

■

4 Conclusion

We give an efficient algorithm for the identity testing of $\Sigma\Pi\Sigma$ circuits with bounded top fanin. The problem of identity testing for general $\Sigma\Pi\Sigma$ arithmetic circuits remains open. Also, it would be interesting to see if this method can be generalized for $\Sigma\Pi\Sigma\Pi$ circuits where the fanin of the topmost addition gate is bounded.

The identities given in Theorem 1.2 are all over fields of prime characteristic. We believe that the bounded rank conjecture of [DS05] might hold true over fields of characteristic 0, for example, $\mathbb{Q}$. Proving such a result might give new insights into the structure of $\Sigma\Pi\Sigma$ identities.

Acknowledgements

We thank Manindra Agrawal for many insightful discussions on this work.

References

[AB03] Manindra Agrawal, Somenath Biswas. *Primality and identity testing via chinese remaindering.* Journal of the ACM, **50**(4), 2003, 429-443.

[AKS04] Manindra Agrawal, Neeraj Kayal, Nitin Saxena. *Primes is in P.* Annals of Mathematics, **160**(2), 2004, 781-793.

[CK97] Zhi-zhong Chen, Ming Yang Kao. *Reducing Randomness via irrational numbers.* Proceedings of the 29th annual ACM Symposium on Theory of Computing, ACM Press, 1997, 200-209.

[DS05] Zeev Dvir, Amir Shpilka. *Locally Decodable Codes with 2 queries and Polynomial Identity Testing for depth 3 circuits.* Proceedings of the 37th annual ACM Symposium on the Theory of Computing, ACM Press, 2005.

[GK98] Dima Grigoriev, Marek Karpinski. *An exponential lower bound for depth* 3 *arithmetic circuits.* Proceedings of the 30th annual ACM Symposium on the Theory of Computing, ACM Press, 1998, 577-582.

[IK03] Russell Impaggliazzo, Valentine Kabanets. *Derandomizing Polynomial Identity Testing means proving circuit lower bounds.* Proceedings of the 35th annual Symposium on Theory of Computing, ACM Press, 2003, 355-364.

[JS80] Mark Jerrum, Marc Snir. *Some exact complexity results for straight-line computations over semirings.* Technical Report CRS-58-80, University of Edinburgh, 1980.

[KS01] Adam Klivans, Daniel Spielman. *Randomness efficient identity testing of multivariate polynomials.* Proceedings of the 33rd annual Symposium on Theory of Computing, ACM Press, 2001, 216-223.

[LV98] Daniel Lewin, Salil Vadhan. *Checking polynomial identities over any field: towards a derandomization?* Proceedings of thirtieth annual ACM Symposium on Theory of Computing, ACM Press, 1998, 438-447.

[Mas84] R. C. Mason. *Diophantine Equations Over Function Fields.* London Mathematical Society Lecture Note Series, 96, Cambridge University Press, 1984.

[McD74] Bernard R. McDonald. *Finite Rings with Identity.* Marcel Dekker, Inc., 1974.

[NZM91] I. Niven, H. Zuckerman, H. Montgomery. *An Introduction to the Theory of Numbers.* John Wiley & Sons, Inc., 5^{th} edition, 1991.

[Pal93] R. E. A. C. Paley. *Theorems on Polynomials in a Galois Field.* Quarterly Journal of Math., 4:52-63, 1993.

[Pud94] Pavel Pudlak. *Communication in bounded depth circuits.* Combinatorica, 14(2):203-216, 1994.

[RS01] Ran Raz, Amir Shpilka. *Lower bounds for matrix product, in bounded depth circuits with arbitrary gates.* Proceedings of the 33^{rd} annual ACM Symposium on Theory of Computing, ACM Press, 2001, 409-418.

[RS04] Ran Raz, Amir Shpilka. *Deterministic Polynomial identity testing in noncommutative models.* Conference on Computational Complexity, 2004.

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

[SS77] Eli Shamir, Marc Snir. *Lower bounds on the number of multiplications and the number of additions in monotone computations.* Research Report RC6757, IBM Thomas J. Watson Research Center, Yorktown Heights, N.Y., 1977.

[SS80] Eli Shamir, Marc Snir. *On the depth complexity of formulas.* Mathematical Systems Theory, 13:301-322, 1980.

[Sto81] W. W. Stothers. *Polynomial identities and Hauptmoduln.* Quarterly Journal of Math., Oxf. II. Ser. 32:349-370, 1981.

[SW99] Amir Shpilka, Avi Wigderson. *Depth-*3 *arithmetic formulae over fields of characteristic zero.* Proceedings of the 14^{th} annual IEEE Conference on Computational Complexity, IEEE Computer Society, 1999.

[TT94] Prasoon Tewari, Martin Tompa. *A direct version of Shamir and Snir's lower bounds on monotone circuit depth.* Information Processing Letters, 49(5):243-248, 1994.

[Zip79] Richard Zippel. *Probabilistic algorithms for sparse polynomials.* Proceedings of the International Symposium on Symbolic and Algebraic Computation, Springer Verlag, 1979, 216-226.