comput. complex. **16** (2007), 115–138
1016-3328/07/020115-24
DOI 10.1007/s00037-007-0226-9

computational complexity

POLYNOMIAL IDENTITY TESTING FOR DEPTH 3 CIRCUITS

Neeraj Kayal and Nitin Saxena

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 (STOC 2001) and Dvir–Shpilka (STOC 2005).

Keywords. Identity testing, depth of circuits, Chinese remaindering, rings.

Subject classification. 68Q15, 13P99.

1. Introduction

Polynomial Identity Testing (PIT) is the following problem: given an arithmetic circuit $\mathcal{C}$ computing a polynomial $p(x_1, x_2, \ldots, x_n)$ 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 (1980) and Zippel (1979) 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 (Agrawal & Biswas 2003; Chen & Kao 2000; Lewin & Vadhan 1998) and a derandomization of the polynomial involved in primality testing by Agrawal, Kayal & Saxena (2004) but a complete derandomization remains distant.

Recently, a surprising development was by Impagliazzo & Kabanets (2004) who showed that efficient deterministic algorithms for identity testing would also imply certain arithmetic circuit lower bounds. More specifically, they

showed that if identity testing has an efficient deterministic polynomial time algorithm then (almost) 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 & Shpilka (2005) gave a deterministic polynomial time algorithm for non-commutative formulas. Klivans & Spielman (2001) 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 & Shpilka (2005) gave a deterministic *quasipolynomial time* algorithm for depth 3 arithmetic circuits (wlog $\Sigma\Pi\Sigma$ 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).

EXAMPLE 1.1. The circuit:

$$\mathcal{C}(x_1, x_2, y) \stackrel{\text{def}}{=} (y) \cdot (y + x_1 + x_2) + (x_1) \cdot (x_2) - (y + x_1) \cdot (y + x_2)$$

is a $\Sigma\Pi\Sigma$-circuit computing the identically zero polynomial over the field $\mathbb{Q}$ of rational numbers. $\Diamond$

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 1.2. *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 at most $poly(n \cdot d^k)$ many field operations, 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.*

REMARK 1.3. *Our algorithm works for all fields $\mathbb{F}$. We analyze the time complexity of our algorithm assuming that the elementary field operations (addition, multiplication, inverse computation and zero testing of field elements) take constant time.*

Dvir & Shpilka (2005) gave a structural result for $\Sigma\Pi\Sigma$ circuits $\mathcal{C}$ with bounded top fanin that compute zero. Let $\text{rank}(\mathcal{C})$ be the maximum number of linearly independent linear functions that appear in $\mathcal{C}$. Then they showed that such *simple* and *minimal* (as defined in the next section) $\mathcal{C}$ can have rank at most $poly(log(d))$. 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 1.4. *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:* $(k, d, rank(\mathcal{C})) = (3, 2^{m-1}, m+1)$.

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

The rest of this paper is organized as follows. Section 2 gives an overview of $\Sigma\Pi\Sigma$ circuits. Section 3 proves a new generalization of the well-known Chinese Remaindering Theorem which is crucial to our algorithm. Finally, Section 4 describes the identity test for $\Sigma\Pi\Sigma$ circuits of bounded top fanin.

2. $\Sigma\Pi\Sigma$ arithmetic circuits

As noted by Impagliazzo and Kabanets, the Polynomial Identity Testing problem is closely related to proving arithmetic circuit lower bounds. 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 (Jerrum & Snir 1982; Shamir & Snir 1977) and linear lower bounds on the depth (Shamir & Snir 1980; Tiwari & Tompa 1994) have been shown. However, only weak lower bounds are known for bounded depth arithmetic circuits (Pudlák 1994; Raz & Shpilka 2001). 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:

$$\mathcal{C}(\overline{x}) = \sum_{i=1}^{k} \prod_{j=1}^{d_i} L_{i,j}(\overline{x}) \tag{2.1}$$

where $L_{i,j}$'s are linear functions. Exponential lower bounds on the size of $\Sigma\Pi\Sigma$ arithmetic circuits have been shown over finite fields (Grigoriev & Karpinski 1998) and their function fields (Grigoriev & Razborov 2000). For $\Sigma\Pi\Sigma$ circuits over fields of characteristic zero only the quadratic lower bound of Shpilka & Wigderson (2001) is known.

No efficient algorithm for identity testing of ΣΠΣ circuits is known. Here, we are interested in studying the identity testing problem for a restricted case of ΣΠΣ circuits – when the top fanin is bounded. This case was posed as a challenge by Klivans & Spielman (2001) and a *quasipolynomial time* algorithm was given by Dvir & Shpilka (2005).

2.1. Previous approaches. Let $\mathcal{C}$ be a ΣΠΣ circuit, as in (2.1), computing the zero polynomial. We will call $\mathcal{C}$ *minimal* if no proper subset of the summands 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 maximum number of linearly independent linear functions appearing in $\mathcal{C}$.

The motivation behind the above definition is that any circuit $\mathcal{C}(\overline{x})$ computing the zero polynomial and having addition gate at the top can be (uniquely) decomposed into a sum of subcircuits $p(\overline{x}) \cdot \mathcal{C}_i(\overline{x})$ where each $\mathcal{C}_i(\overline{x})$ is a minimal and simple circuit computing the zero polynomial. The quasipolynomial time algorithm of Dvir & Shpilka (2005) is based on the result: the rank of a minimal and simple ΣΠΣ circuit with bounded top fanin and computing zero is "small". Formally, the result says:

THEOREM 2.2 (Thm 1.4 of Dvir & Shpilka 2005). *Let $k \geq 3, d \geq 2$, and let $\mathcal{C} \equiv 0$ be a simple and minimal ΣΠΣ circuit of degree d with k multiplication gates and n inputs, then rank$(\mathcal{C}) \leq 2^{O(k^2)} \log(d)^{k-2}$.*

Thus, given a circuit $\mathcal{C}$ and k a constant either the $\text{rank}(\mathcal{C}) = O(\log(d)^{k-2})$, in which case we find out in $(d^{\text{rank}(\mathcal{C})}) = 2^{O(\log(d)^{k-1})}$ many steps whether $\mathcal{C}$ is zero. Or the $\text{rank}(\mathcal{C})$ is larger and then we need to check whether a subset of the summands of $\mathcal{C}$ add up to zero. Even this can be done as $\mathcal{C}$ can decompose into sub-circuits in at most 2^k many ways and each such sub-circuit can be treated recursively. Effectively, this gives us a $2^{O(\log(d)^{k-1})}$ time identity test.

This raises 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). In fact, Dvir & Shpilka (2005) conjectured that $\text{rank}(\mathcal{C}) = O(k)$. Here, we give an identity with $k = 3$ that contradicts this conjecture.

LEMMA 2.3. *Define*

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

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 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 $a_1,\ldots,a_m \in \mathbb{F}_2$ be such that $(a_1+\cdots+a_m) = 1$. Let us compute $\mathcal{C}$ 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 $T_2 = 0 \pmod{a_1x_1+\cdots+a_mx_m}$. Further,

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

Thus, we deduce: $T_1+T_2+T_3 \equiv 0 \pmod{a_1x_1+\cdots+a_mx_m}$ for any $a_1,\ldots,a_m \in \mathbb{F}_2$, $(a_1+\cdots+a_m) = 1$. Also, notice that $T_1 = 0 \pmod{y}$ (consider the linear factor of T_1 obtained by setting: $b_1 = \cdots = b_m = 0$) and $T_2 = T_3 \pmod{y}$ implying that $T_1+T_2+T_3 = 0 \pmod{y}$. Thus, we get that:

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

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

It is easy to verify that $\mathcal{C}$ is a minimal, simple $\Sigma\Pi\Sigma$ circuit of degree 2^{m-1}. The rank of $\mathcal{C}$ is $(m+1)$ simply because $x_1, \ldots, x_m, y$ occur as linear functions in the three summands of $\mathcal{C}$. □

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 lemma answers in the affirmative.

LEMMA 2.4. *Let p be an odd prime. Define:*

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

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 rank$(\mathcal{C}) = \log_p(d) + 2$.

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

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

$$\left.\prod_{\substack{b_1,\ldots,b_m\in\mathbb{F}_p\\ b_1+\cdots+b_m\equiv -i}}(b_1x_1+\cdots+b_mx_m)\right\} \pmod{y+a_1x_1+\cdots+a_mx_m}$$

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

$$\left.(-1)^{p^{m-1}}\cdot\prod_{\substack{b_1,\ldots,b_m\in\mathbb{F}_p\\ b_1+\cdots+b_m\equiv i}}(b_1x_1+\cdots+b_mx_m)\right)$$

$$\equiv 0 \pmod{y+a_1x_1+\cdots+a_mx_m}.$$

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

$$\mathcal{C}(x_1,\ldots,x_m,y)\equiv 0 \pmod{y+a_1x_1+\cdots+a_mx_m}$$

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

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

By looking at the coefficient of the term of highest degree in y the minimality of $\mathcal{C}$ is obvious. Also, the p summands in $\mathcal{C}$ are coprime because $b_1,\ldots,b_m$ sum upto different values modulo p in different summands.

Thus, $\mathcal{C}$ is a minimal, simple, $\Sigma\Pi\Sigma$ zero circuit of degree p^{m-1}. The rank of $\mathcal{C}$ is $(m+1)$ simply because $x_1,\ldots,x_m,y$ occur as linear functions in the three summands of $\mathcal{C}$. □

Thus, methods of Dvir & Shpilka (2005) are unlikely to give an efficient algorithm and we give new techniques in the subsequent sections that solve the problem.

2.2. Our approach. We now give the basic idea behind our approach to this problem after introducing a little bit of notation.

2.2.1. Terminology – Leading monomial and leading coefficient. Let $\mathbb{F}$ be a field and $\succeq$ be the graded-lexicographic ordering on monomials in $\mathbb{F}[x_1,\ldots,x_n]$. That is, $\succeq$ ranks monomials by their total degree and breaks ties by using lexicographic ordering. For $f(\overline{x})\in\mathbb{F}[\overline{x}]$:

- The *leading monomial* of $f(\overline{x})$, written $LM(f(\overline{x}))$, is the monomial which is ranked highest under $\succeq$ of all monomials which have nonzero coefficients in $f(\overline{x})$. If f is a constant then $LM(f(\overline{x})) = 1$.
- For a monomial $x_1^{\alpha_1}x_2^{\alpha_2}\ldots x_n^{\alpha_n}$ and a polynomial $f(x_1,\ldots,x_n) \in \mathbb{F}[x_1,\ldots,x_n]$, we will denote the coefficient of the monomial $x_1^{\alpha_1}x_2^{\alpha_2}\ldots x_n^{\alpha_n}$ in $f(x_1,\ldots,x_n)$ by $\text{Coeff}(x_1^{\alpha_1}x_2^{\alpha_2}\ldots x_n^{\alpha_n}, f(x_1,\ldots,x_n))$.
- The *leading coefficient* of a polynomial $f(\overline{x})$ is defined to be $\text{Coeff}(LM(f(\overline{x})), f(\overline{x}))$ and is concisely denoted as $LC(f)$.

Note that the leading monomial operator – LM – satisfies the following property:

FACT 2.5. *For $f_1(\overline{x}), f_2(\overline{x}) \in \mathbb{F}[\overline{x}]$,*

(i) $LM(f_1(\overline{x}) \cdot f_2(\overline{x})) = LM(f_1(\overline{x})) \cdot LM(f_2(\overline{x}))$. Thus, it is easy to compute $LM(T)$ when T is given as a product of linear functions.

(ii) If $LM(f_1(\overline{x})) \succeq LM(f_2(\overline{x}))$ then $LM(f_1(\overline{x})) \succeq LM(f_1(\overline{x}) + f_2(\overline{x}))$.

2.2.2. The idea. The input is a circuit $\mathcal{C}(x_1,\ldots,x_n)$ in $\mathbb{F}[x_1,\ldots,x_n]$ which looks like:

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

where, each T_i is a product of linear functions:

$$T_i = L_{i,1} \cdot L_{i,2} \cdot \ldots \cdot L_{i,d}$$

and where, each $L_{i,j}$ looks:

$$L_{i,j} = a_{i,j,0} + a_{i,j,1}x_1 + a_{i,j,2}x_2 + \cdots + a_{i,j,n}x_n$$

for some $a_{i,j,0}, a_{i,j,1}, a_{i,j,2}, \ldots, a_{i,j,n} \in \mathbb{F}$. We want to check if $\mathcal{C}$ computes the identically zero polynomial over $\mathbb{F}$.

By rearranging the terms if necessary we can assume without loss of generality that:

$$LM(T_1) \succeq LM(T_2) \succeq \cdots \succeq LM(T_k)\,.$$

Then by property (ii) of leading monomials we have:

$$LM(T_1) \succeq LM(\mathcal{C})\,. \tag{2.6}$$

We first verify that T_1 divides $\mathcal{C}$ by using a recursive algorithm to be described a short while later. We next check if $\text{Coeff}(LM(T_1), \mathcal{C}(x_1,\ldots,x_n)) = 0$. We

accept $\mathcal{C}$ if and only if it passes both the tests. Clearly, if $\mathcal{C}(x_1, \ldots, x_n) = 0$, the input will pass both the tests and our algorithm will correctly identify $\mathcal{C}(x_1, \ldots, x_n)$ as the zero polynomial. So assume that $\mathcal{C}(x_1, \ldots, x_n) \neq 0$ but it passes both the tests. In that case, by Property (i) of LM we then have

$$LM(\mathcal{C}) \succeq LM(T_1)\,. \tag{2.7}$$

Combining (2.6) and (2.7), we get:

$$LM(\mathcal{C}) = LM(T_1)\,.$$

But

$$\text{Coeff}\big(LM(T_1), \mathcal{C}(x_1, \ldots, x_n)\big) = 0$$

implying that

$$\text{Coeff}\big(LM(\mathcal{C}), \mathcal{C}(x_1, \ldots, x_n)\big) = 0$$

which is a contradiction since $\mathcal{C}(x_1, \ldots, x_n)$ was assumed to be non-zero.

Checking that T_1 divides $\mathcal{C}(x_1, \ldots, x_n)$. We have $T_1 = L_{1,1} \cdot L_{1,2} \cdot \ldots \cdot L_{1,d}$. We recursively verify that $\mathcal{C} \equiv 0 \pmod{L_{1,j}}$ for all $1 \leq j \leq d$. If $L_{1,j}$ is not a constant then note that T_1 vanishes modulo $L_{1,j}$ and that $\mathbb{F}[x_1, \ldots, x_n]/\langle L_{1,j}\rangle \cong \mathbb{F}[y_1, \ldots, y_{n-1}]$ is isomorphic to a polynomial ring in $(n-1)$ variables over the field $\mathbb{F}$. Therefore, verifying $\mathcal{C} \equiv 0 \pmod{L_{1,j}}$ amounts to identity testing of a $\Sigma\Pi\Sigma$ circuit of top fanin $(k-1)$ in $(n-1)$ variables over the field $\mathbb{F}$.

Having verified that $\mathcal{C} \equiv 0 \pmod{L_{1,j}}$ for all $1 \leq j \leq d$, we can deduce by the Chinese Remaindering Theorem that $L \stackrel{\text{def}}{=} \text{lcm}(L_{1,1}, L_{1,2}, \ldots, L_{1,d})$ divides $\mathcal{C}$. Now if the degree of L is as large as that of T_1 then we are done.

In general, however there would exist pathological cases in which T_1 has repeated factors and the degree of L is smaller than that of T_1. The algorithm for the general case has the same structure as above, except that we now work with polynomials over local rings instead of fields. Our main tool will be a generalization of the Chinese Remainder Theorem (CRT). The next section is devoted to this generalization of CRT.

3. Chinese remaindering

This section develops the algebraic tools that we eventually use to prove the main result of this paper. The basic algebraic structure that keeps recurring here is a *local ring*. The advantage of working with local rings is that polynomials over them inherit some of the nice properties of polynomials over fields and this is really helpful in computation.

In our algorithm, the polynomials that we get will be over some *local* ring $R \supseteq \mathbb{F}$ instead of being over $\mathbb{F}$ but we can show that the Chinese remaindering property of polynomials in $\mathbb{F}[z_1, \ldots, z_n]$ continues to hold in $R[z_1, \ldots, z_n]$. Specifically, we need that:

> **Chinese remaindering:** If "coprime" polynomials $f(z_1, \ldots, z_n)$ and $g(z_1, \ldots, z_n)$ divide $p(z_1, \ldots, z_n)$ then $f \cdot g \mid p$ over R.

Throughout this paper, all the rings that we will come across will be finite dimensional algebras over the base field $\mathbb{F}$. Some of the known results related to local rings over $\mathbb{F}$ can be found in the appendix.

3.1. Notation and terminology.

3.1.1. Terminology – Natural ring homomorphism. Let $R \supseteq \mathbb{F}$ be a local ring over a field $\mathbb{F}$ with maximal ideal $\mathcal{M}$ (i.e., $R/\mathcal{M} \equiv \mathbb{F}$). We will denote by R^* the set the group of invertible elements (units) of R. Then every element $r \in R$ can be written uniquely as $r = \alpha + m$ where $\alpha \in \mathbb{F}$ and $m \in \mathcal{M}$ is a nilpotent (i.e., for some index i, $m^i = 0$) element of R. Such an element r is a unit (i.e., $r \in R^*$) if and only if $\alpha \neq 0$. By the term *natural ring homomorphism from R to $\mathbb{F}$*, we will mean the unique non-zero homomorphism $\phi : R \mapsto \mathbb{F}$ that maps every element in $\mathcal{M}$ to zero in $\mathbb{F}$. That is, $\phi(r) = \alpha$. The map ϕ then extends in a natural way to a homomorphism from the polynomial ring $R[z_1, \ldots, z_n]$ to the polynomial ring $\mathbb{F}[z_1, \ldots, z_n]$ so that the polynomial $\sum_\beta a_\beta \overline{z}^\beta$ is mapped to the polynomial $\sum_\beta \phi(a_\beta)\overline{z}^\beta$, where, $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n$ and $\overline{z}^\beta = z_1^{\beta_1} \cdots z_n^{\beta_n}$. We will say that two polynomials $f(\overline{z})$ and $g(\overline{z})$ in $R[\overline{z}]$ are *coprime* if and only if the corresponding polynomials $\phi(f(\overline{z}))$ and $\phi(g(\overline{z}))$ are coprime.

3.1.2. Notation – Set of linear functions over R. Let R be a local ring over a field $\mathbb{F}$ with maximal ideal $\mathcal{M}$. We will denote by $LF_{R/\mathbb{F}}(\overline{x})$ the set of all linear functions in n variables $\overline{x} = (x_1, x_2, \ldots, x_n)$ over R with coefficients from $\mathbb{F}$. That is,

$$LF_{R/\mathbb{F}}(x_1, \ldots, x_n) = \left\{ a_0 + \sum_{i=1}^{i=n} a_i x_i + m \mid m \in \mathcal{M},\ \ \forall i\ a_i \in \mathbb{F}\ ,\ \ \exists i : a_i \neq 0 \right\}$$

3.2. Preliminaries.

For any ring S, 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 $g(z) \in S[z]$ is called *monic* if its leading coefficient is

a unit of S (S^* denotes the group of units 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 3.1 (Gauss' lemma). *Suppose $f(z), g(z) \in S[z]$ and $h(z) \in S^{\text{fr}}[z]$ such that: $f(z) = g(z)h(z)$. If $g(z)$ is monic then $h(z) \in S[z]$.*

PROOF. Let the degrees of f, g and h be α, β and γ respectively. Let

$$f(z) = \sum_{i=0}^{\alpha} f_i z^i \quad \text{where} \quad f_i \in S\,,$$

$$g(z) = \sum_{i=0}^{\beta} g_i z^i \quad \text{where} \quad g_\beta = 1,\ g_i \in S \quad \text{and}$$

$$h(z) = \sum_{i=0}^{i=\gamma} h_i z^i \quad \text{where} \quad h_i \in S^{\text{fr}}\,.$$

Suppose if possible that $h(z) \notin S[z]$. Let $k \in [1 \cdots \gamma]$ be the largest integer such that h_k, the coefficient of z^k in $h(z)$, does not belong to S. Now the coefficient of $z^{\beta+k}$ in $g(z)h(z)$ is

$$\begin{aligned} f_{\beta+k} &= g_\beta h_k + \sum_{j=1}^{\beta} g_{\beta-j} h_{k+j} \\ &= h_k + \sum_{j=1}^{\beta} g_{\beta-j} h_{k+j}\,. \end{aligned}$$

Thus, $f_{\beta+k} \in S^{\text{fr}} \setminus S$. This is a contradiction to the fact that $f(z) \in S[z]$. □

3.3. 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. In showing this, we will often make use of linear transformation of variables. We start out with a lemma which shows that after the application of a suitable linear transformation, any polynomial $p(x_1, x_2, \ldots, x_n) \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ of total degree d can be transformed into a monic polynomial $\hat{p}$ having degree d with respect to the variable x_1.

LEMMA 3.2. *Let $\mathbb{F}$ be a field of size at least $2d$ and $p(x_1, x_2, \ldots, x_n) \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ be any polynomial of total degree d. Then there exists an invertible linear transformation $\tau : x_i \mapsto \sum_{j=1}^{n} \alpha_{i,j} x_j$ such that $\hat{p}(x_1, x_2, \ldots, x_n) \stackrel{\text{def}}{=} p(\tau(x_1), \tau(x_2), \ldots, \tau(x_n))$ has a nonzero coefficient of x_1^d.*

PROOF. Let $p(\overline{x}) = q(\overline{x}) + r(\overline{x})$ where $q(\overline{x}) \neq 0$ is a homogeneous polynomial of degree d and $r(\overline{x})$ consists of all the remaining smaller degree terms of $p(\overline{x})$. Then the coefficient of x_1^d in $\hat{p}(\overline{x})$ is simply $q(\alpha_{1,1}, \alpha_{2,1}, \ldots, \alpha_{n,1})$.

If $\mathbb{F}$ is a finite field then by the Schwartz–Zippel lemma (Schwartz 1980; Zippel 1979):

$$\Pr_{\alpha_{1,1}, \alpha_{2,1}, \ldots, \alpha_{n,1} \in \mathbb{F}} \left[q(\alpha_{1,1}, \alpha_{2,1}, \ldots, \alpha_{n,1}) \neq 0 \right] \geq \left(1 - \frac{d}{\#\mathbb{F}} \right)$$

and so in particular there exists $\alpha_{1,1}, \alpha_{2,1}, \ldots, \alpha_{n,1} \in \mathbb{F}$ such that $q(\alpha_{1,1}, \alpha_{2,1}, \ldots, \alpha_{n,1}) \neq 0$. Now these values of $\alpha_{i,1}$, $i \in [n]$ can be easily extended (using linear algebra) to an invertible linear transformation τ such that $\hat{p}(\overline{x})$ is monic in x_1.

If $\mathbb{F}$ is an infinite field then since $q(\overline{x}) \neq 0$ there will exist $\alpha_{i,1} \in \mathbb{F}$, for all $i \in [n]$ such that $q(\alpha_{1,1}, \alpha_{2,1}, \ldots, \alpha_{n,1}) \neq 0$. Again these values of $\alpha_{i,1}$, $i \in [n]$ can be easily extended to an invertible linear transformation τ such that $\hat{p}(\overline{x})$ is monic in x_1. □

Throughout the rest of 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 natural extension of the map ϕ to a homomorphism from $R[z_1, z_2, \ldots, z_n]$ to $\mathbb{F}[z_1, z_2, \ldots, z_n]$ will also be denoted by ϕ. 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 $\mathbb{F}$ be a field of size at least $2d$ and R be a local ring over $\mathbb{F}$. Let $p(x_1, x_2, \ldots, x_n) \in R[x_1, x_2, \ldots, x_n]$ be any polynomial such that $\phi(p)$ has total degree d. Then there exists an invertible linear transformation $\tau : x_i \mapsto \sum_{j=1}^{n} \alpha_{i,j} x_j$ such that α's are in $\mathbb{F}$ and the coefficient of x_1^d in $\hat{p}(x_1, x_2, \ldots, x_n) \stackrel{\text{def}}{=} p(\tau(x_1), \tau(x_2), \ldots, \tau(x_n))$ is a unit.*

PROOF. We could apply Lemma 3.2 to the polynomial $\phi(p)$ over the field $\mathbb{F}$ to get a τ' such that $\phi(p)(\tau'(x_1), \ldots, \tau'(x_n))$ has a nonzero coefficient of x_1^d. As a result, the coefficient of x_1^d in $p(\tau'(x_1), \ldots, \tau'(x_n))$ is a unit of R. □

Now we prove a Chinese Remainder like theorem for the case of local rings that we will be working with in our identity test.

LEMMA 3.4. *Let R be a local ring over $\mathbb{F}$ and $p, f, g \in R[z_1, z_2, \ldots, z_n]$ be multivariate polynomials such that $\phi(f)$ and $\phi(g)$ are coprime.*

$$\begin{aligned} \textit{If} \quad & p \equiv 0 \pmod{f} \\ \textit{and} \quad & p \equiv 0 \pmod{g} \\ \textit{then} \quad & p \equiv 0 \pmod{f \cdot g}\,. \end{aligned}$$

PROOF. Let the (total) degrees of $\phi(f)$ and $\phi(g)$ be d_f and d_g respectively. We could assume wlog that $\mathbb{F}$ is large enough for else we can go to its extension field. By Lemma 3.3 we can now apply a suitable invertible linear transformation on the variables $z_1, \ldots, z_n$, if needed, and can thus 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, $R(z_1, z_2, \ldots, z_{n-1})$, of $R[z_1, z_2, \ldots, z_{n-1}]$. 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 $\mathbb{F}(z_1, z_2, \ldots, z_{n-1})$. Consequently, there exists $a, b \in \mathbb{F}(z_1, z_2, \ldots, z_{n-1})[z_n]$ such that:

$$a\phi(f) + b\phi(g) = 1 \quad \text{in} \quad \mathbb{F}(z_1, z_2, \ldots, z_{n-1})[z_n]\,. \tag{3.5}$$

Now we want to apply Hensel Lifting lemma (see Lemma 5.5 in the appendix) to the above and so let us define an ideal:

$$\mathcal{I} := \left\{ r \mid r \in R(z_1, \ldots, z_{n-1})[z_n] \text{ and } r \text{ is nilpotent} \right\}.$$

Thus, we can write (3.5) as:

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

By the repeated application of Hensel Lifting we get that there exists a^*, b^*, f^*, g^* in $R(z_1, \ldots, z_{n-1})[z_n]$ such that $(f^* - f), (g^* - g) \in \mathcal{I}$ and:

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

which is the same as saying ($\because \mathcal{I}^t = 0$):

$$a^*f^* + b^*g^* = 1 \quad \text{in} \quad R(z_1, z_2, \ldots, z_{n-1})[z_n]\,.$$

Now since $(f^* - f), (g^* - g) \in \mathcal{I}$ there exists an $m \in \mathcal{I}$ such that $a^*f + b^*g = 1 + m$ in $R(z_1, z_2, \ldots, z_{n-1})[z_n]$. Since m is a nilpotent, there exists $(1+m)^{-1} \in$

$R(z_1, z_2, \ldots, z_{n-1})[z_n]$. Thus, by defining $a' = a^*(1+m)^{-1}$ and $b' = b^*(1+m)^{-1}$ we have:

$$a'f + b'g = 1 \quad \text{in} \quad R(z_1, z_2, \ldots, z_{n-1})[z_n]\,.$$

Now by the hypothesis:

$$\begin{aligned}
& p \equiv 0 && \pmod{f} \\
\Rightarrow \quad & p = fq && \text{for some } q \text{ in } R[z_1, z_2, \ldots, z_{n-1}][z_n] \\
\textit{also}, \quad & p \equiv 0 && \pmod{g} \\
\Rightarrow \quad & fq \equiv 0 && \pmod{g} \\
\Rightarrow \quad & a'fq \equiv 0 && \pmod{g} \text{ in } R(z_1, z_2, \ldots, z_{n-1})[z_n] \\
\Rightarrow \quad & q \equiv 0 && \pmod{g} \text{ in } R(z_1, z_2, \ldots, z_{n-1})[z_n] \\
\therefore \quad & p = fgh && \text{for some } h \text{ in } R(z_1, z_2, \ldots, z_{n-1})[z_n]\,.
\end{aligned}$$

Since, the leading coefficient of z_n in fg is in R^* and $p,\ fg$ are in $R[z_1, z_2, \ldots, z_{n-1}][z_n]$, therefore, by Gauss Lemma (see Lemma 3.1) we get that, in fact, $h \in R[z_1, z_2, \ldots, z_{n-1}][z_n]$ and so:

$$p \equiv 0 \pmod{fg} \quad \text{in} \quad R[z_1, z_2, \ldots, z_n]\,. \qquad \square$$

4. Description of the identity test

4.1. Overview of the algorithm. We now 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 at most 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 at most d in each recursive call and thus, the complexity comes out to be: $poly(d^k \cdot n)$ field operations in $\mathbb{F}$.

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:

$$\mathcal{C} = \beta_1 \cdot T_1 + \beta_2 \cdot T_2 + \cdots + \beta_k \cdot T_k$$

where, each $\beta_i \in R$, each T_i is a product of linear functions:

$$T_i = L_{i,1} L_{i,2} \cdots L_{i,d}$$

and where, each $L_{i,j}$ is a nontrivial linear function:

$$L_{i,j} = a_{i,j,0} + a_{i,j,1}z_1 + a_{i,j,2}z_2 + \cdots + a_{i,j,n}z_n$$

for some $a_{i,j,1}, a_{i,j,2}, \ldots, a_{i,j,n} \in \mathbb{F}$ and $a_{i,j,0} \in \mathcal{M}$. We want to check if $\mathcal{C}$ computes the identically zero polynomial over R. Note that in each T_i, the coefficient of its leading monomial $\mathrm{Coeff}(LM(T_i), T_i)$ is in $\mathbb{F} \subseteq R^*$. We renumber the terms and ensure that:

$$LM(T_1) \succeq LM(T_2) \succeq \cdots \succeq LM(T_k)\,.$$

Note that by the Fact 2.5 of leading coefficients we can efficiently decide if $LM(T_1) \succeq LM(T_2)$ and consequently this renumbering is also efficiently doable. Suppose that T_1 factors over R into a product of *coprime* polynomials $p_1, \ldots, p_\ell$. We recursively verify that:

$$\mathcal{C} \equiv 0 \pmod{p_i} \quad \text{for} \quad 1 \leq i \leq \ell\,.$$

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

$$\mathcal{C} \equiv 0 \left(\mathrm{mod} \prod_{i=1}^{\ell} p_i\right).$$

Our choice of the polynomials p_i ensures that the total degree of $\prod_{i=1}^{\ell} p_i(z_1, \ldots, z_n)$ is at least as large as that of $\mathcal{C}(z_1, \ldots, z_n)$. Finally, by verifying that $\mathrm{Coeff}(LM(T_1), \mathcal{C})$, the coefficient of the leading monomial of T_1 in $\mathcal{C}(z_1, \ldots, z_n)$, is zero we deduce that $\mathcal{C}$ computes the identically zero polynomial over R.

Our choice of the polynomials p_i ensures 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 $R' := R[z_1]/(\tau \circ p_i)$ is again a local ring (see Lemma 5.4).

ii) p_i divides T_1 and so $T_1 \equiv 0 \pmod{p_i}$. Thus $\tau \circ \mathcal{C}$ can be viewed as a $\Sigma\Pi\Sigma$ circuit with top fanin at most $(k-1)$, total degree d and $(n-1)$ variate over the (larger) ring R'. We can check $\mathcal{C} \equiv 0 \pmod{p_i}$ by checking $\tau \circ \mathcal{C} \equiv 0$ over R' recursively.

4.2. The algorithm. **Input:** The three inputs to the algorithm are:

- A local ring R of dimension r over a field $\mathbb{F}$ with maximal ideal $\mathcal{M}$. (In the initial call, $R = \mathbb{F}$ and $\mathcal{M} = \langle 0 \rangle$). In the algorithm we always work with rings in basis form.
- A set of k coefficients $\langle \beta_1, \ldots, \beta_k \rangle$, where $k \geq 1$ and $\forall i : \beta_i \in R$.
- A set of k terms $\langle T_1, \ldots, T_k \rangle$. Each T_i is a product of d_i linear functions in n variables over the ring R. That is, each T_i is of the form $T_i = \prod_{j=1}^{d_i} L_{i,j}$ and each $L_{i,j} \in LF_{R/\mathbb{F}}(x_1, x_2, \ldots, x_n)$.

Output: The input parameters specify the following polynomial over the ring R:

$$p(x_1, \ldots, x_n) \stackrel{\text{def}}{=} \beta_1 T_1 + \cdots + \beta_k T_k \,.$$

The output of the algorithm, $\mathbf{ID}(R, \langle \beta_1, \ldots, \beta_k \rangle, \langle T_1, \ldots, T_k \rangle)$, is YES iff

$$p(x_1, \ldots, x_n) = 0 \,.$$

ALGORITHM. $\mathbf{ID}(R,\ \langle \beta_1, \ldots, \beta_k \rangle,\ \langle T_1, \ldots, T_k \rangle)$:.

Step 1: (Rearranging the terms.) By rearranging the terms if needed ensure that

$$LM(T_1) \succeq LM(T_i) \quad \text{for all} \quad 2 \leq i \leq k \,.$$

Step 2: (Base case of one multiplication gate) If $k = 1$ then we need to check whether $\beta_1 T_1 = 0$ as a member of $R[x_1, x_2, \ldots, x_n]$. Since $LC(T_1)$ is a unit in $\mathbb{F}$, this happens if and only if $\beta_1 = 0$.

Step 3: (Verifying that $p(x_1, \ldots, x_n) \equiv 0 \pmod{T_1}$) We shall verify that T_1 divides $p(x_1, \ldots, x_n)$ by using recursion to verify that all the distinct coprime factors of T_1 divide $p(x_1, \ldots, x_n)$. Since T_1 is the product of linear functions over R, it can easily be written as the product of coprime factors, each factor being of the form

$$S = (l + m_1)(l + m_2) \ldots (l + m_t)$$

where $l \in \mathbb{F}[x_1, \ldots, x_n]$ is a linear function in n variables over $\mathbb{F}$ and for all $i \in [t]$, $m_i \in \mathcal{M}$. Now to verify that each such factor S divides $p(x_1, \ldots, x_n)$ do the following:

> **Step 3.1** (Applying a linear transformation.) Define a linear tranformation σ acting on the variables $x_1, \ldots, x_n$ such that σ sends $l \mapsto x_1$ and transforms $x_2, \ldots, x_n$ such that it is an invertible linear map. Such a σ can be found by elementary linear algebra. Now S divides $p(x_1, \ldots, x_n)$ if and only if $\sigma(S)$ divides $\sigma(p(x_1, \ldots, x_n))$.

Step 3.2 (Recursively verify $\sigma(S)$ divides $\sigma(p)$). Define the ring R' as:

$$R' \stackrel{\text{def}}{=} R[x_1]/\big(\sigma(S)\big) \tag{4.1}$$

Note that $\sigma(T_1) \equiv 0 \pmod{\sigma(S)}$. For all i between 2 and k compute γ_i and T_i' such that:

$$\sigma(T_i) = \gamma_i T_i' \pmod{\sigma(S)} \quad \text{where} \quad \gamma_i \in R' \,,\; T_i' \in LF_{R'/\mathbb{F}}(x_2, \ldots, x_n)\,.$$

(Basically, the linear factors of T_i having zero coefficients of $x_2, \ldots, x_n$ get "collected" in γ_i while the other linear factors collect in T_i'.)

Recursively call $\mathbf{ID}(R',\ \langle \beta_2\gamma_2, \ldots, \beta_k\gamma_k\rangle\,,\ \langle T_2', \ldots, T_k'\rangle)$. If the recursive call returns **NO** then output **NO** and exit.

Step 4: (Comparing coefficient of the highest monomial.) Compute the coefficient of $LM(T_1)$ in $p(x_1, \ldots, x_n)$ and output YES iff its zero.

4.3. Proof of correctness. The proof of correctness is now straightforward. We continue using the notation set in the last subsection. The claim here is summarized as:

THEOREM 4.2. *Let R be a local ring of dimension r over a field $\mathbb{F}$. Then*

$$\boldsymbol{ID}\big(R,\ \langle \beta_1, \ldots, \beta_k\rangle\,,\ \langle T_1, \ldots, T_k\rangle\,\big)$$

returns YES iff $\beta_1 T_1 + \cdots + \beta_k T_k = 0$ in $R[x_1, \ldots, x_n]$. Furthermore, the time taken is $poly(nrd^k)$ field operations in $\mathbb{F}$, where d is the maximum degree of any term.

PROOF. **Time complexity.** Note that in all the recursive calls that

$$\mathbf{ID}\big(R,\ \langle \beta_1, \ldots, \beta_k\rangle\,,\ \langle T_1, \ldots, T_k\rangle\,\big)$$

makes to $\mathbf{ID}(\cdot,\cdot,\cdot)$ the dimension of the base ring R increases by a factor of at most d whereas the value of k, the number of terms, decreases by one. Moreover, there are at most d such recursive calls. Therefore, if $h(k, r)$ denotes the time taken by

$$\mathbf{ID}\big(R,\ \langle \beta_1, \ldots, \beta_k\rangle\,,\ \langle T_1, \ldots, T_k\rangle\,\big)$$

then we have the following recurrence:

$$h(k, r) \leq d \cdot h(k-1, dr) + poly(nrd^k)\,.$$

Thus, we get that $h(k,r) = poly(nrd^k)$.

Correctness. We prove the correctess of the output of

$$\mathbf{ID}\big(R,\ \langle\beta_1,\ldots,\beta_k\rangle\,,\ \langle T_1,\ldots,T_k\rangle\,\big)$$

by induction on k:

Claim 4.3. ***ID***$(R,\ \langle\beta_1,\ldots,\beta_k\rangle\,,\ \langle T_1,\ldots,T_k\rangle)$ *returns YES iff*

$$\beta_1 T_1 + \cdots + \beta_k T_k = 0\,.$$

Proof of Claim 4.3. The base case of the induction is when $k = 1$, handled and explained by Step 2.

Now we assume that $k \geq 2$ and that the claim is true for values smaller than k. Let $T_1 = S_1 \cdot S_2 \cdot \ldots \cdot S_m$. In Step 3 we verify that S_i divides $p(x_1,\ldots,x_n)$ for all $i \in [m]$. Then by Lemma 3.4, we deduce that $T_1 = \prod_{i\in[m]} S_i$ divides $p(x_1,\ldots,x_n)$. Thus, we get that

$$p(x_1,\ldots,x_n) = T_1 \cdot q(x_1,\ldots,x_n) \quad \text{for some} \quad q \in R[x_1,\ldots,x_n]\,.$$

Since $LC(T_1)$ is a unit of R we have $LM(p) = LM(T_1)\cdot LM(q)$ and in particular that $LM(p) \succeq LM(T_1)$. On the other hand, since $p = \sum_{i\in[k]} \beta_i T_i$ and $LM(T_1) \succeq LM(T_i)\ \ \forall i \in [k]$ we have that $LM(T_1) \succeq LM(p)$. We therefore deduce that $LM(p) = LM(T_1)$. Finally, in Step 4 we compute the coefficient of $LM(T_1)$ in p and by the above observations it is the same as $LC(p)$. Now $p = 0$ over R iff $LC(p) = 0$ as required. □

This completes the proof of correctness and time complexity analysis of our algorithm. □

5. 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 1.4 are all over fields of prime characteristic. We believe that the bounded rank conjecture of Dvir & Shpilka (2005) 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.

Appendix: Useful facts about local rings

In this appendix, we consider local rings over a field $\mathbb{F}$. Any such ring $R \supseteq \mathbb{F}$ that we consider will be a finite dimensional algebra over the field $\mathbb{F}$. [1]

We first collect some results related to decomposition of rings into simpler rings. A ring R is said to be *decomposable* if there are subrings R_1, R_2 such that:

- $R_1 \cdot R_2 = R_2 \cdot R_1 = 0$, i.e., for all $r_1 \in R_1, r_2 \in R_2$, $r_1 \cdot r_2 = r_2 \cdot r_1 = 0$.
- $R_1 \cap R_2 = \{0\}$.
- $R = R_1 + R_2$, i.e., for every $r \in R$ there are $r_1 \in R_1, r_2 \in R_2$ such that $r = r_1 + r_2$.

We denote such a ring decomposition as $R = R_1 \times R_2$. The subrings R_1, R_2 are called *component* rings of R.

EXAMPLE 5.1. The ring $R := \mathbb{F}[x]/(x^2 - x)$ decomposes as: $R = R \cdot x \times R \cdot (1-x) \cong \mathbb{F} \times \mathbb{F}$. Here, $R \cdot x$ is a short-hand for the set $\{r \cdot x \mid r \in R\}$. Note that $R \cdot x$, $R \cdot (1 - x)$ are subrings of R and have x, $(1 - x)$ as their (multiplicative) identity elements respectively. ◊

An element $r \in R$ is called an *idempotent* if $r^2 = r$. The following lemma shows how idempotents help in decomposing a commutative ring.

LEMMA 5.2. *A commutative ring R decomposes iff R has an idempotent element other than* $0, 1$.

PROOF. Suppose $R = R_1 \times R_2$ is a nontrivial decomposition and let the identity element 1 of R be expressible as $1 = s + t$ where $s \in R_1$, $t \in R_2$. Then we have:

$$\begin{aligned}
& 1 \cdot 1 = (s+t) \cdot (s+t) \\
\Rightarrow \quad & 1 = s^2 + t^2 \qquad [\because s \cdot t = 0] \\
\Rightarrow \quad & s + t = s^2 + t^2 \\
\Rightarrow \quad & s - s^2 = t^2 - t \\
\Rightarrow \quad & s - s^2 = 0 \qquad \left[\because s - s^2 \in R_1 \cap R_2 = \{0\}\right] \\
\Rightarrow \quad & s \text{ is an idempotent}.
\end{aligned}$$

[1] It is possible to define infinite dimensional local rings over $\mathbb{F}$ but we do not need them in our application and shall not consider such rings.

Note that if $s = 0$ then $t = 1$ and then $R_1 = 0$ (as for all $r_1 \in R_1,\ r_1 \cdot t = 0$). Similarly, if $s = 1$ then $R_2 = 0$. As R_1, R_2 are nonzero subrings of R we deduce that $s \neq 0, 1$ and hence s is an idempotent other than $0, 1$.

Conversely, suppose that $s \neq 0, 1$ is an idempotent of R. Then consider the subrings $R \cdot s$ and $R \cdot (1-s)$. Note that s, $(1-s)$ are the identity elements of Rs, $R(1-s)$ respectively. For any two elements $rs \in Rs$ and $r'(1-s) \in R(1-s)$: $rs \cdot r'(1-s) = rr'(s-s^2) = 0$. If $r \in Rs \cap R(1-s)$ then $rs = 0$ and $r(1-s) = 0$ implying that $r = 0$. Finally, we can express any $r \in R$ as: $r = rs + r(1-s)$. Thus, R decomposes as: $R = Rs \times R(1-s)$. □

In this paper we called a ring *local* if it is commutative and indecomposable. Let us now see a structural property of such local rings.

LEMMA 5.3. *For a field $\mathbb{F}$, consider a ring R of the form:*

$$R = \mathbb{F}[x_1, \ldots, x_n] \big/ \left(x_1^{e_1}, \ldots, x_n^{e_n}, h_1(x_1, \ldots, x_n), \ldots, h_\ell(x_1, \ldots, x_n)\right).$$

Then,

1) *R is indecomposable.*

2) *R has a unique maximal ideal $\mathcal{M}$ such that $\mathcal{M} =$ set of nilpotents of R.*

PROOF (1). Any element r of R looks like $a_0 + a_1(\overline{x})x_1 + \cdots + a_n(\overline{x})x_n$, where, $a_0 \in \mathbb{F}$ and $a_1(\overline{x}), \ldots, a_n(\overline{x}) \in \mathbb{F}[x_1, \ldots, x_n]$.

Suppose $a_0 = 0$. Since, $x_1^{e_1} = \cdots = x_n^{e_n} = 0$ we have that:

$$\begin{aligned} r^{e_1+\cdots+e_n} &= \left(a_1(\overline{x})x_1 + \cdots + a_n(\overline{x})x_n\right)^{e_1+\cdots+e_n} \\ &= 0\,. \end{aligned}$$

Suppose $a_0 \neq 0$. Let $r_0 := r - a_0$ and $e := e_1 + \cdots + e_n$. Then we have:

$$\begin{aligned} (a_0 + r_0)\left(a_0^e - a_0^{e-1}r_0 + \cdots + (-1)^{e-1}a_0 r_0^{e-1} + (-1)^e r_0^e\right) &= a_0^{e+1} + (-1)^e r_0^{e+1} \\ &= a_0^{e+1} \qquad [\because r_0^e = 0] \\ &\in \mathbb{F}^* \\ \Rightarrow r &\in R^*\,. \end{aligned}$$

Thus, every element r of R is either a nilpotent or a unit depending upon whether $a_0 = 0$ or not.

Now suppose R is decomposable. By Lemma 5.2 there has to be a nontrivial idempotent $t \in R$. But we have:

$$\begin{aligned} & t^2 = t \\ \Rightarrow \quad & t(t-1) = 0 \\ \Rightarrow \quad & t = 0 \text{ or } 1 \qquad \left[\because \text{ either } t \text{ or } (t-1) \text{ is a unit in } R \right]. \end{aligned}$$

This contradiction shows that R is indecomposable. □

PROOF (2). Define a set $\mathcal{M} := R \setminus R^*$. As shown above $\mathcal{M}$ is the set of nilpotents of R and hence is an ideal. $\mathcal{M}$ is maximal because any element outside it is a unit. $\mathcal{M}$ is unique because it contains all the non-units of R. □

Now we consider the special form of local rings that appear in (4.1) and show how to do computations in that ring in an "efficient" way.

LEMMA 5.4. *Suppose we are given (in basis form) a sequence of rings, over a field $\mathbb{F}$, as:*

$$\begin{aligned} & R_0 := \mathbb{F} \quad \textit{having maximal ideal } \mathcal{M}_0 = 0 \\ & R_1 := R_0[x_1]/(x_1^{e_1}) \quad \textit{having maximal ideal } \mathcal{M}_1 = (x_1) = x_1 \cdot R_1 \\ & \quad \vdots \\ & R_k := R_{k-1}[x_k]/\left((x_k + r_{k,1}) \cdots (x_k + r_{k,e_k})\right), \quad \textit{where, } r_{k,1}, \ldots, r_{k,e_k} \in \mathcal{M}_{k-1}. \\ & \qquad \textit{Also, the maximal ideal of } R_k \textit{ is } \mathcal{M}_k = (x_1, \ldots, x_k). \end{aligned}$$

Define $D_i := e_1 \cdots e_i$, for all $i \in [k]$. Then the addition operation in R_k takes $O(D_k)$ field operations in $\mathbb{F}$ and the multiplication operation in R_k takes $O(kD_k^2)$ field operations in $\mathbb{F}$.

PROOF. Inductively, we can check that R_k is indeed a local ring. Since $(x_k + r_{k,1}) \cdots (x_k + r_{k,e_k}) = 0$ and $r_{k,1}, \ldots, r_{k,e_k} \in \mathcal{M}_{k-1}$ we have that, in the ring R_k:

$$x_k^{e_k} = r_{e_k-1} x_k^{e_k-1} + \cdots + r_1 x_k + r_0 \quad \text{for some} \quad r_{e_k-1}, \ldots, r_0 \in \mathcal{M}_{k-1}.$$

As $r_{e_k-1}, \ldots, r_0$ are nilpotents in R_k we deduce from the above equation that x_k is a nilpotent too. Hence, by Lemma 5.3, R_k is a local ring with the ideal of nilpotents equal to $(x_1, \ldots, x_k)$.

For induction assume that the addition operation in R_{k-1} takes time: $O(D_{k-1})$. Let $r := (\alpha_{e_k-1} x_k^{e_k-1} + \cdots + \alpha_1 x_k + \alpha_0)$ and $r' := (\alpha'_{e_k-1} x_k^{e_k-1} + \cdots +$

$\alpha'_1 x_k + \alpha'_0$) be two elements in R_k such that for all $0 \leq i \leq e_k - 1$, $\alpha_i, \alpha'_i \in R_{k-1}$. Now the addition operation: $r + r'$ entails computing e_k additions (of the form $\alpha_i + \alpha'_i$) in R_{k-1}. Thus, addition in R_k takes time: $e_k \cdot O(D_{k-1}) = O(D_k)$.

Again for induction assume that the multiplication operation in R_{k-1} takes time: $O((k-1)D_{k-1}^2)$. Then the multiplication operation: $r \cdot r'$ entails e_k^2 multiplications (of the form $\alpha_i \cdot \alpha'_j$) in the ring R_{k-1} and those many additions. Hence, the time taken for multiplication in R_k is:

$$\begin{aligned} e_k^2 O\big((k-1)D_{k-1}^2\big) + e_k^2 O(D_{k-1}) &= O\big((k-1)D_k^2\big) + e_k O(D_k) \\ &= O(kD_k^2)\,. \end{aligned}$$

□

Recall that something called Hensel's Lifting was crucial in proving the Chinese Remaindering property for polynomials over local rings in Lemma 3.4. We present the statement of Hensel's Lifting lemma below.

LEMMA 5.5 (Hensel's lifting). *Let R be a ring and $\mathcal{I}$ be an ideal. Let $f(z) \in R[z]$ and $f = gh \pmod{\mathcal{I}}$ be a factorization of f over $R/\mathcal{I}$ such that there exists $a, b \in R[z]$, $ag + bh = 1 \pmod{\mathcal{I}}$. Then,*

- *There are efficiently computable $g^*, h^*, a^*, b^* \in R[z]$ satisfying:*

$$\begin{aligned} f &= g^* h^* \pmod{\mathcal{I}^2} \\ g^* &= g \pmod{\mathcal{I}} \quad \text{and} \quad h^* = h \pmod{\mathcal{I}} \\ a^* g^* + b^* h^* &= 1 \pmod{\mathcal{I}^2}\,. \end{aligned}$$

- *Also, g^*, h^* above are unique in the sense that for any other g', h' satisfying the above conditions we have some $u \in \mathcal{I}$ such that:*

$$\begin{aligned} g' &= g^*(1+u) \pmod{\mathcal{I}^2} \\ h' &= h^*(1-u) \pmod{\mathcal{I}^2}\,. \end{aligned}$$

PROOF. See Lidl & Niederreiter (1994) for the proof. □

Acknowledgements

The research was supported by Infosys Technologies Limited, Bangalore and IIT Kanpur, India.

We thank Manindra Agrawal for many insightful discussions on this work. We thank Jaikumar Radhakrishnan for pointing out a correction in the conference version of this paper.

References

M. Agrawal & S. Biswas (2003). Primality and identity testing via chinese remaindering. *Journal of the ACM* **50**(4), 429–443.

M. Agrawal, N. Kayal & N. Saxena (2004). Primes is in P. *Annals of Mathematics* **160**(2), 781–793.

Z. Chen & M. Kao (2000). Reducing Randomness via Irrational Numbers. *SIAM Journal of Computing* **29**(4), 1247–1256.

Z. Dvir & A. Shpilka (2005). Locally decodable codes with 2 queries and polynomial identity testing for depth 3 circuits. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing*, 592–601.

D. Grigoriev & M. Karpinski (1998). An Exponential Lower Bound for Depth 3 Arithmetic Circuits. In *Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, 577–582.

D. Grigoriev & A. A. Razborov (2000). Exponential Lower Bounds for Depth 3 Arithmetic Circuits in Algebras of Functions over Finite Fields. *Appl. Algebra Eng. Commun. Comput.* **10**(6), 465–487.

R. Impagliazzo & V. Kabanets (2004). Derandomizing polynomial identity tests means proving circuit lower bounds. *Computational Complexity* **13**(1/2), 1–46.

M. Jerrum & M. Snir (1982). Some Exact Complexity Results for Straight-Line Computations over Semirings. *Journal of the ACM* **29**(3), 874–897.

A. R. Klivans & D. Spielman (2001). Randomness efficient identity testing of multivariate polynomials. In *Proceedings of the 33rd annual ACM Symposium on Theory of Computing*, 216–223.

D. Lewin & S. Vadhan (1998). Checking polynomial identities over any field: towards a derandomization? In *Proceedings of the 30th annual ACM Symposium on Theory of Computing*, 438–447. ACM Press.

R. Lidl & H. Niederreiter (1994). *Introduction to finite fields and their applications*. Cambridge University Press.

P. Pudlák (1994). Communication in Bounded Depth Circuits. *Combinatorica* **14**(2), 203–216.

R. Raz & A. Shpilka (2001). Lower bounds for matrix product, in bounded depth circuits with arbitrary gates. In *Proceedings of the 33rd annual ACM Symposium on Theory of Computing*, 409–418. ACM Press.

R. Raz & A. Shpilka (2005). Deterministic polynomial identity testing in non-commutative models. *Computational Complexity* **14**(1), 1–19.

J. T. Schwartz (1980). Fast Probabilistic Algorithms for Verification of Polynomial Identities. *Journal of the ACM* **27**(4), 701–717.

E. Shamir & M. Snir (1977). Lower bounds on the number of multiplications and the number of additions in monotone computations. Research Report RC6757.

E. Shamir & M. Snir (1980). On the Depth Complexity of Formulas. *Mathematical Systems Theory* **13**, 301–322.

A. Shpilka & A. Wigderson (2001). Depth-3 arithmetic circuits over fields of characteristic zero. *Computational Complexity* **10**(1), 1–27.

P. Tiwari & M. Tompa (1994). A Direct Version of Shamir and Snir's Lower Bounds on Monotone Circuit Depth. *Information Processing Letters* **49**(5), 243–248.

R. Zippel (1979). Probabilistic Algorithms for Sparse Polynomials. In *International Symposium on Symbolic and Algebraic Computation*, volume 72 of *Lecture Notes in Computer Science*, 216–226. Springer-Verlag.

Manuscript received 24 October 2006

Neeraj Kayal
Institute for Advanced Study
Einstein Drive
Princeton, NJ 08540, USA
kayaln@ias.edu

Nitin Saxena
Centrum voor Wiskunde en Informatica
Kruislaan 413
1098 SJ, Amsterdam, The Netherlands
nitin.saxena@cwi.nl