Electronic Colloquium on Computational Complexity, Report No. 95 (2007)

The Ideal Membership Problem and Polynomial Identity Testing

V. Arvind and Partha Mukhopadhyay

Institute of Mathematical Sciences
C.I.T Campus,Chennai 600 113, India
{arvind,partham}@imsc.res.in

Abstract. Given a monomial ideal $I = \langle m_1, m_2, \cdots, m_k\rangle$ where m_i are monomials and a polynomial f as an arithmetic circuit the *Ideal Membership Problem* is to test if $f \in I$. We study this problem and show the following results.

(a) If the ideal $I = \langle m_1, m_2, \cdots, m_k\rangle$ for a *constant* k then there is a randomized polynomial-time membership algorithm to test if $f \in I$. This result holds even for f given by a black-box, when f is of small degree.

(b) When $I = \langle m_1, m_2, \cdots, m_k\rangle$ for a *constant* k and f is computed by a $\Sigma\Pi\Sigma$ circuit with output gate of *bounded fanin* we can test whether $f \in I$ in deterministic polynomial time. This generalizes the Kayal-Saxena result [KS07] of deterministic polynomial-time identity testing for $\Sigma\Pi\Sigma$ circuits with bounded fanin output gate.

(c) When k is not constant the problem is coNP-hard. However, the problem is upper bounded by $\mathrm{coAM}^{\mathrm{PP}}$ over the field of rationals, and by $\mathrm{coNP}^{\mathrm{Mod}_p\mathrm{P}}$ over finite fields.

(d) Finally, we discuss identity testing for certain restricted depth 4 arithmetic circuits.

For ideals $I = \langle f_1, \cdots, f_\ell\rangle$ where each $f_i \in \mathbb{F}[x_1, \cdots, x_k]$ is an arbitrary polynomial but k is a *constant*, we show similar results as (a) and (b) above.

1 Introduction

For a field $\mathbb{F}$ let $\mathbb{F}[x_1, x_2, \cdots, x_n]$ be the ring of polynomials over $\mathbb{F}$ with indeterminates $x_1, x_2, \cdots, x_n$. Let $I \subseteq \mathbb{F}[x_1, x_2, \cdots, x_n]$ be an ideal given by a finite generator set $\{g_1, g_2, \cdots, g_r\}$ of polynomials. Then $I = \{\sum_{i=1}^{r} a_i g_i \mid p_i \in \mathbb{F}[x_1, x_2, \cdots, x_n]\}$, and we write $I = \langle g_1, g_2, \cdots, g_r\rangle$.

Given an ideal $I = \langle g_1, g_2, \cdots, g_r\rangle$ and a polynomial $f \in \mathbb{F}[x_1, x_2, \cdots, x_n]$ the *Ideal Membership* problem is to decide if $f \in I$.

Ideal Membership Testing is a fundamental algorithmic problem with important applications [COX92]. In general, however, Ideal Membership Testing is notoriously intractable. The results of Mayr and Meyer show that it is EXPSPACE-complete [MM82,Mayr89]. Nevertheless, because of its important applications, algorithms for this problem are widely studied, mainly based on the theory of Gröbner bases [COX92].

Polynomial Identity Testing (PIT) is a well-known problem in the field of computational complexity and randomization: given an arithmetic circuit C computing a polynomial in $\mathbb{F}[x_1, x_2, \cdots, x_n]$, the problem is to determine whether the polynomial computed by C is identically zero.

One can view the output of the circuit C as a function from $\mathbb{F}^n \to \mathbb{F}$ and ask whether it is the zero function. In general, this is not the same as asking whether the polynomial computed by C is identically zero as a formal expression in $\mathbb{F}[x_1, x_2, \cdots, x_n]$. Notice that $x^p - x \in \mathbb{F}_p[x]$ computes the zero function on $\mathbb{F}_p$ but as a formal expression $x^p - x$ is not zero in $\mathbb{F}_p[x]$. However, if the formal degree of the circuit C is smaller than the size of $\mathbb{F}$, then the interpretations are equivalent.

Over the years, PIT has played a significant role in our understanding of several important algorithmic problems. Well-known examples are the randomized NC algorithms for the matching problem in graphs [Lov79,MVV87], and the AKS primality test [AKS04]. The PIT problem has also played an indirect role in important complexity results such as $\mathrm{IP} = \mathrm{PSPACE}$ [LFKN92,Sha92] and the proof

ISSN 1433-8092

of PCP theorem [ALMSS92].[1]. The question whether PIT is in P has emerged as an important open problem (see, for example, [AB03,KI03]).

Results of this paper: The main goal of this paper is to bring out interesting connections between Monomial Ideal Membership and Polynomial Identity Testing. The study of monomial ideals is central to the theory of Gröbner bases [COX92]. In Section 2 we explain this in more detail.

Suppose $I = \langle m_1, m_2, \cdots, m_k \rangle$ is a monomial ideal in $\mathbb{F}[x_1, x_2, \cdots, x_n]$ generated by the monomials m_i. In contrast to the general ideal membership problem, testing membership in the monomial ideal I is trivial for a polynomial $f \in \mathbb{F}[x_1, x_2, \cdots, x_n]$ that is given explicitly as an $\mathbb{F}$-linear combination of monomials. We only need to check if each monomial occurring in f is divisible by some generator monomial m_i. However, as we show in this paper, the problem becomes interesting when f is given by an arithmetic circuit. In that case, it turns out that the problem is tractable when k is a constant and its complexity is similar to that of polynomial identity testing. Given a monomial ideal $I = \langle m_1, m_2, \cdots, m_r \rangle$ for monomials $m_i \in \mathbb{F}[x_1, \cdots, x_n]$ and an arithmetic circuit C over $\mathbb{F}$ defining a polynomial $f \in \mathbb{F}[x_1, x_2, \cdots, x_n]$, the *Monomial Ideal Membership* problem is to decide if $f \in I$. In this paper, whenever there is an ideal given by a generating set, it will be assumed that the exponent of any variable that appear in a generator, is given in unary.

We study different versions of the problem by placing restrictions on the arithmetic circuit C and the number of monomials generating the ideal I. We also consider a more general version of the problem where we are allowed only black-box access to the polynomial f. Our main results are the following.

- A randomized test for Monomial Ideal Membership when f given by an arithmetic circuit and $I = \langle m_1, m_2, \cdots, m_k \rangle$ for constant k. This is analogous to the Schwartz-Zippel randomized polynomial identity test [Sch80,Zip79]. A similar randomized test for f given by a black-box when f has small degree.
- When k is unrestricted the problem is coNP-hard, but we show that it is in the counting hierarchy.
- The identity testing problem for $\Sigma\Pi\Sigma$ circuits has recently attracted a lot of research [DS05,KS07]. The main open problem is whether there is a deterministic polynomial-time identity test for $\Sigma\Pi\Sigma$ circuits. For the special case of $\Sigma\Pi\Sigma$ circuits with bounded fanin output gate Kayal and Saxena [KS07] recently gave an ingenious deterministic polynomial-time test.
  Analogous to their result, we consider monomial ideal membership, where f is computed by a $\Sigma\Pi\Sigma$ circuit with bounded fanin output gate, and $I = \langle m_1, m_2, \cdots, m_k \rangle$ for constant k. Using the algorithm of [KS07] we give a *deterministic* polynomial-time algorithm for Monomial Ideal Membership. More interestingly, we develop the algorithm and its correctness proof based on Gröbner basis theory. We believe this approach is somewhat simpler and direct. It avoids properties such as Chinese remaindering in local rings and Hensel lifting that is used in [KS07]. As a byproduct, this gives us a different understanding of the identity testing algorithm of [KS07].

2 Preliminaries

We develop the rudiments of Gröbner basis theory. Details can be found in the text [COX92] and Madhu Sudan's notes [Su98].

Let $\bar{x}$ denote indeterminates $\{x_1, x_2, \cdots, x_n\}$. Let $\mathbb{F}[\bar{x}]$ denotes the polynomial ring $\mathbb{F}[x_1, x_2, \cdots, x_n]$. Let R be a commutative ring. A subring $I \subseteq R$ is an *ideal* of R if $IR \subseteq R$. The

[1] In the sense that properties of low-degree multivariate polynomials are crucial to these proofs.

Hilbert basis theorem [COX92] states that any ideal I of $\mathbb{F}[x_1, x_2, \cdots, x_n]$ is *finitely generated*. I.e. we can express $I = \{\sum_{i=1}^{r} p_i g_i \mid p_i \in \mathbb{F}[x_1, x_2, \cdots, x_n]\}$, where the finite collection of polynomials $\{g_1, g_2, \cdots, g_r\}$ is a generating set (or basis) for I.

The notion of monomial ordering is key to defining Gröbner bases. We restrict ourselves to the *lexicographic monomial ordering* which we define below. For $\bar{\alpha} = (\alpha_1, \alpha_2, \cdots, \alpha_n) \in \mathbb{N}^n$, we denote the monomial $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ by $\bar{x}^{\bar{\alpha}}$.

Definition 1. *Let $\bar{\alpha} = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ and $\bar{\beta} = (\beta_1, \beta_2, \cdots, \beta_n) \in \mathbb{N}^n$. We say $\bar{\alpha} > \bar{\beta}$ if, in the vector difference $\bar{\alpha} - \bar{\beta} \in \mathbb{N}^n$, the left-most nonzero entry is positive. We say, $\bar{x}^{\bar{\alpha}} > \bar{x}^{\bar{\beta}}$ (equivalently, $\bar{x}^{\bar{\beta}} < \bar{x}^{\bar{\alpha}}$) if $\bar{\alpha} > \bar{\beta}$.*

The lexicographic monomial ordering naturally fixes a leading monomial $LM(f)$ for any polynomial f. Let $LC(f)$ denote the coefficient of $LM(f)$. Then the *leading term* of f is $LT(f) = LC(f)LM(f)$. Using the monomial ordering, we state the general form of the division algorithm over $\mathbb{F}[x_1, x_2, \cdots, x_n]$.

Theorem 1 (Theorem 3, pp.61). [COX92] *Let $f \in \mathbb{F}[\bar{x}]$ and $(f_1, f_2, \cdots, f_s)$ be an ordered s-tuple of polynomials in $\mathbb{F}[\bar{x}]$. Then f can be written as, $f = a_1 f_1 + a_2 f_2 + \cdots + a_s f_s + r$, where $a_i, r \in \mathbb{F}[\bar{x}]$, and either $r = 0$ or r is an $\mathbb{F}$-linear combination of monomials, none of which is divisible by any of $LT(f_1), LT(f_2), \cdots, LT(f_s)$.*

The proof of the theorem is constructive. We give an intuitive outline as we use it often in the paper. Let $\bar{f}$ denotes the ordering of the polynomials f_i's: $\bar{f} = (f_1, f_2, \cdots, f_s)$. The proof describes a division algorithm Divide$(f; \bar{f})$ which first sorts f by the monomial ordering. The algorithm proceeds iteratively. It tries to eliminate the leading monomial in the current remainder by attempting to divide it with the f_i's in the given order. The f_i that succeeds is the first one whose leading monomial divides the leading monomial of the current remainder. Finally, the remainder r that survives has the above property. The algorithm is guaranteed termination as the monomial ordering is a well ordering. The following time bound for Divide$(f; \bar{f})$ is easy to obtain.

Fact 2 (Section 6, pp.12-5) [Su98] *The running time of Divide$(f; \bar{f})$ is bounded by $O(s \prod_{i=1}^{n} (d_i + 1)^{O(1)})$, where d_i is the maximum degree of x_i among the polynomials $f, f_1, f_2, \cdots, f_s$.*

If the remainder r output by Divide$(f; \bar{f})$ is zero then clearly $f \in \langle f_1, \cdots, f_s \rangle$. However, in general, Divide$(f; \bar{f})$ need not produce zero remainder even if $f \in \langle f_1, \cdots, f_s \rangle$ as the order of division is important. Thus, it cannot be directly used as an ideal membership test. In order to ensure this property, we define *Gröbner bases* (with respect to the lexicographic monomial ordering).

Definition 2. *Fix $<$ as the monomial ordering, and let $J \subseteq \mathbb{F}[\bar{x}]$ be any ideal. Then, the polynomials $g_1, g_2, \cdots, g_t$ form a* Gröbner basis *for J if $J = \langle g_1, g_2, \cdots, g_s \rangle$ and $\langle LT(g_1), \cdots, LT(g_t) \rangle = \langle LT(J) \rangle$*

The following lemma states that the general division algorithm of Theorem 1 carried out w.r.t. a Gröbner basis results in a unique remainder r regardless of the order in which division is applied.

Lemma 1. *Let $G = \{f_1, f_2, \cdots, f_s\}$ be a Gröbner basis for an ideal $J \subseteq \mathbb{F}[\bar{x}]$ and $f \in \mathbb{F}[\bar{x}]$. Then there is a* unique *polynomial $r \in \mathbb{F}[\bar{x}]$ such that f can be written as, $f = a_1 f_1 + a_2 f_2 + \cdots + a_s f_s + r$, for $a_i \in \mathbb{F}[\bar{x}]$, and either $r = 0$ or r is an $\mathbb{F}$-linear combination of monomials, none of which is divisible by any of $LT(f_1), LT(f_2), \cdots, LT(f_s)$.*

By Lemma 1 we can indeed test if $f \in J$ given a Gröbner basis $\{f_1, f_2, \cdots, f_s\}$ for J by computing Divide$(f; \bar{f})$ and checking if the remainder is zero.

The following theorem gives us an easy to test sufficient condition to check if a given generating set for an ideal is already a Gröbner basis.

Theorem 3 (Theorem 3, proposition 4, pp.101). [COX92] *Let I be a polynomial ideal given by a basis $G = \{g_1, g_2, \cdots, g_s\}$ such that all pairs $i \neq j$ $LM(g_i)$ and $LM(g_j)$ are relatively prime. Then G is a Gröbner basis for I.*

Recall from the introduction that a *monomial ideal* is an ideal generated by a finite set of monomials in $\mathbb{F}[\bar{x}]$.[2]

Lemma 2 (Lemma 2, Lemma 3, pp.67-68). [COX92] *Let $I = \langle m_1, m_2, \cdots, m_s \rangle$ be a monomial ideal and $f \in \mathbb{F}[\bar{x}]$. Then, $f \in I$ if and only if each monomial of f is in I. Furthermore, a monomial m is in the ideal I if and only if there exist $i \in [s]$, such that m_i divides m.*

An immediate consequence of Lemma 2 is that we can test in deterministic polynomial time if an explicitly given polynomial $f \in \mathbb{F}[\bar{x}]$ is in a monomial ideal I.

In this paper, we are primarily interested in the monomial ideal membership problem and its connection to PIT. In the proof of certain results we will also be making use of properties of Gröbner bases.

3 Monomial Ideal Membership

In this section we consider monomial ideal membership when f is given by an arithmetic circuit. We show that the problem is in randomized polynomial time if number of generators k for the monomial ideal I is a constant. When k is not a constant we show that it is coNP-hard and s contained in coAM$^{\text{PP}}$. We leave open a tight classification of the complexity of this problem.

Lemma 3. *Let, $I = \langle m_1, m_2, \cdots, m_k \rangle$ be a monomial ideal in $\mathbb{F}[x_1, x_2, \cdots, x_n]$. For $i \in [k]$, let $m_i = x_1^{e_{i1}} x_2^{e_{i2}} \cdots x_n^{e_{in}}$. Let $\bar{v}$ be a k-tuple given by $\bar{v} = (j_1, j_2, \cdots, j_k)$, where $j_i \in [n]$. Define the ideal, $I_{\bar{v}} = \langle x_{j_1}^{e_{1j_1}}, \cdots, x_{j_k}^{e_{kj_k}} \rangle$. Then $f \in I$ if and only if, $\forall \bar{v} \in [n]^k$, $f \in I_{\bar{v}}$.*

Proof. Let $f \in I$. So, f can be written as $f = p_1 m_1 + u_2 m_2 + \cdots + p_k m_k$, where $p_i \in \mathbb{F}[\bar{x}]$ for all i. Then, clearly $\forall \bar{v} \in [n]^k$, $f \in I_{\bar{v}}$. To see the other direction, suppose $f \notin I$. Write $f = c_1 M_1 + c_2 M_2 + \cdots + c_t M_t$, where M_i's are the monomials of f and $c_i \in \mathbb{F}$ are the corresponding coefficients. As $f \notin I$, there is a $j \in [t]$, such that $M_j \notin I$. Thus, for all $i \in [k]$, m_i does not divide M_j. So, each of the m_i's contains some x_{ℓ_i}, such that the exponent of x_{ℓ_i} is greater than the exponent of x_{ℓ_i} in M_j. Let $\{\ell_1, \ell_2, \cdots, \ell_k\}$ are k such indexes. Now consider the ideal $I_{\bar{w}}$, where $\bar{w} = (\ell_1, \ell_2, \cdots, \ell_k)$. By Lemma 2, $M_j \notin I_{\bar{w}}$ and hence $f \notin I_{\bar{w}}$. ■

Using Lemma 3, we generalize the Schwartz-Zippel Lemma to a form tailored for Monomial Ideal Membership.

Lemma 4. *Let $f \in \mathbb{F}[x_1, x_2, \cdots, x_n]$ be a polynomial of total degree d and $I = \langle x_1^{e_1}, x_2^{e_2}, \cdots, x_k^{e_k} \rangle$ be a monomial ideal as described in lemma 3. Fix a finite subset $S \subseteq \mathbb{F}$, and let $r_1, r_2, \cdots, r_{n-k}$ be chosen independently and uniformly at random from S.*

Then, $\text{Prob}_{r_i \in S}[f(x_1, x_2, \cdots, x_k, r_1, r_2, \cdots, r_{n-k}) \in I \mid f \notin I] \leq \frac{d}{|S|}$.

[2] Indeed, by Dickson's Lemma an ideal generated by an arbitrary subset of monomials is also generated by a finite subset of monomials and hence is a monomial ideal.

Proof. First we write $f = \sum_{\bar{v}} x_1^{j_1} \cdots x_k^{j_k} f_{\bar{v}}(x_{k+1}, \cdots, x_n)$, where $\bar{v} = (j_1, \cdots, j_k)$. Any term in the above expression with $j_i \geq e_i$ is already in I. Thus, it suffices to consider the sum $\hat{f}$ of the remaining terms. More precisely, Let $\mathcal{A} = [e_1 - 1] \times [e_2 - 1] \times \cdots \times [e_k - 1]$. We can write $\hat{f} = \sum_{\bar{v} \in \mathcal{A}} x_1^{j_1} \cdots x_k^{j_k} f_{\bar{v}}(x_{k+1}, \cdots, x_n)$ where $\bar{v} = (j_1, j_2, \cdots, j_k) \in \mathcal{A}$. As $\hat{f} \notin I$, not all $f_{\bar{v}}$ are identically zero. Choose and fix one such $\bar{u}$. By the Schwartz-Zippel lemma [MR01], $\text{Prob}_{r_i \in S}[f_{\bar{u}}(r_1, r_2, \cdots, r_{n-k}) = 0 \mid f_{\bar{u}}(x_{k+1}, x_{k+2}, \cdots, x_n) \not\equiv 0] \leq \frac{d}{|S|}$.

Notice that for any $\bar{v} = (j_1, j_2, \cdots, j_k) \in \mathcal{A}$, the monomial $x_1^{j_1} \cdots x_k^{j_k}$ is not in I. Thus, the polynomial $f(x_1, x_2, \cdots, x_k, r_1, r_2, \cdots, r_{n-k}) \in I$ iff $\forall \bar{v}$, $f_{\bar{v}}(r_1, r_2, \cdots, r_{n-k}) = 0$. But $f_{\bar{u}}(r_1, r_2, \cdots, r_{n-k}) = 0$ with probability at most $d/|S|$. This completes the proof. ∎

Theorem 4. *Let $f \in \mathbb{F}[\bar{x}]$ be given by an arithmetic circuit C and the ideal $I = \langle m_1, m_2, \cdots, m_k \rangle$ generated by monomials m_i's where k is a constant. For such instances Monomial Ideal Membership can be solved in randomized polynomial time (in $n^{O(k)}$ time).*

Proof. First, we construct all the ideals, $\{I_{\bar{v}} \mid \bar{v} \in [n]^k\}$ as described in Lemma 3. Then for each such $I_{\bar{v}}$, we check if $f \in I_{\bar{v}}$. The correctness of the algorithm follows from Lemma 3. Let $I_{\bar{v}} = \langle x_1^{e_1}, x_2^{e_2}, \cdots, x_k^{e_k} \rangle$. To check $f \in I_{\bar{v}}$, we assign random values to $x_{k+1}, \cdots, x_n$ from S and then evaluate the circuit C in the ring $R = \mathbb{F}[x_1, x_2, \cdots, x_k]/I_{\bar{v}}$. To evaluate the circuit in R, we need to compute each gate operation modulo $I_{\bar{v}}$, starting from the input gates. Notice that, as $\langle x_1^{e_1}, x_2^{e_2} \cdots, x_k^{e_k} \rangle$ is a Gröbner basis for $I_{\bar{v}}$, by Lemma 1 the actual order in which we evaluate the gates is not important. Let, $e = \sum_{i=1}^{k} e_i$. Then it is easy to see that the running time of the algorithm is poly(n, s, e^k) (notice that e_i's are in unary). Furthermore, by Lemma 4, the success probability of the algorithm is seen to be $\geq 1 - (d/|S|)$. So, it is enough to consider sampling from a set S s.t, $|S| = 2d$ using $O(\log d)$ random bits. ∎

When the monomial ideal I is not generated by a constant number of monomials the monomial ideal membership problem is coNP hard over any field.

Theorem 5. *Given a polynomial f as an arithmetic circuit, and a monomial ideal $I = \langle m_1, m_2, \cdots, m_k \rangle$, it is* coNP*-hard to test whether $f \in I$.*

Proof. Indeed, we prove the coNP-hardness even for f given by a $\Pi\Sigma$ arithmetic circuit. First we consider the case when the field $\mathbb{F}$ is $\mathbb{Q}$. We give a reduction from 3-CNF. Let $F = C_1 \wedge C_2 \wedge \cdots \wedge C_\ell$ is a 3-CNF formula over $\{x_1, x_2, \cdots, x_n\}$, with C_i are the clauses. Introduce new variables $\{y_1, y_2, \cdots, y_n\}$ for $\{\bar{x}_1, \bar{x}_2, \cdots, \bar{x}_n\}$. Next, we encode each of the clause as a linear form (sum of variables). For example, if $C_1 = x_1 \vee x_2 \vee \bar{x}_3$ then we encode it as $x_1 + x_2 + y_3$. Thus we get a polynomial C corresponding to $F : C(\bar{x}, \bar{y}) = \prod_{i=1}^{\ell} L_i(\bar{x}, \bar{y})$, where L_i's are the linear form corresponding to C_i. Clearly, $C(\bar{x}, \bar{y})$ represents a $\Pi\Sigma$ circuit. Define a monomial ideal, $I = \langle x_i y_i \mid 1 \leq i \leq n \rangle$. It follows that, if F is satisfiable then not all the monomials of C are in I. So, in that case $C \notin I$ by Lemma 2. Conversely assume that $C \notin I$. That means, C has at least one monomial m such that m does not contain both x_i and y_i for any i. So, the variables of m correspond to a satisfying assignment for F (set the variables those are not in m to zero).

Now, let the characteristic of the field be finite. The only place the proof differs from the above is, we need to encode each clause as a sum of all seven monomials representing the satisfying assignment of that clause. For example, an assignment $\{1, 0, 1\}$ of $\{x_1, x_2, x_3\}$ corresponds to a monomial $x_1 y_2 x_3$. Thus a clause $C_1 = x_1 \vee x_2 \vee \bar{x}_3$ will be encoded as a sum of all possible monomials except

$y_1y_2x_3$. Note that the polynomial C corresponding to F is represented by a $\Pi\Sigma\Pi$ circuit. The rest of the argument follows exactly as above. ∎

Next, we show some upper bounds for Monomial Ideal Membership when the number of monomial generators is not restricted to a constant.

Theorem 6. *1. For $\mathbb{F} = \mathbb{Q}$, Monomial Ideal Membership is in* $\mathrm{coAM}^{\mathrm{PP}}$ *where the input monomial ideal $I = \langle m_1, m_2, \cdots, m_k\rangle$ is given by a list of monomials and $f \in \mathbb{F}[\bar{x}]$ is given by an arithmetic circuit C.*
2. For $\mathbb{F} = \mathbb{F}_p$, Monomial Ideal Membership is in $\mathrm{coNP}^{\mathrm{Mod}_p\mathrm{P}}$.

Proof. For the first part, suppose $\mathbb{F} = \mathbb{Q}$ and C is the input arithmetic circuit computing $f \in \mathbb{F}[\bar{x}]$ and the monomial ideal I is $\langle m_1, m_2, \cdots, m_k\rangle$. We'll show that *Nonmembership* is in $\mathrm{AM}^{\mathrm{PP}}$. It suffices for the $\mathrm{AM}^{\mathrm{PP}}$ algorithm to exhibit a nonzero monomial m of f such that $m \notin \langle m_1, m_2, \cdots, m_k\rangle$. I.e. m_i does not divide m for $i = 1, 2, \cdots, k$. The base AM machine (call it M) will guess such a monomial $m = x_1^{e_1}x_2^{e_2}\cdots x_n^{e_n}$ by nondeterministically picking the tuple $(e_1, \cdots, e_n) \in \mathbb{N}^n$ and check that m_i does not divide m for all i. It remains to verify that m is a nonzero monomial of f. W.l.o.g. we can assume that $f \in \mathbb{Z}[\bar{x}]$. We will describe a $\mathrm{BPP}^{\#\mathrm{P}}$ algorithm that takes as input $\langle C, m\rangle$ and makes one #P query to decide if m is a nonzero monomial in f. Write f as a finite sum $f = \sum_{\bar{\alpha}\in\mathbb{N}^n} c_\alpha \bar{x}^{\bar{\alpha}}$. Since the input to C are the indeterminates and constants, the numbers $c_{\bar{\alpha}}$ are bounded in absolute value by 2^K, where the size of $K \in \mathbb{Z}^+$ in binary is bounded by some polynomial in input size. Now, we observe that $c_{\bar{e}} \neq 0$ iff m occurs in f, where $\bar{e} = (e_1, e_2, \cdots, e_n)$. The BPP machine guesses a random prime p of polynomial size, where the size is chosen suitably, so that $c_{\bar{e}} \neq 0$ iff $c_{\bar{e}} \neq 0 (\mathrm{mod}\ p)$ with high probability. Now we define the #P query that the BPP machine will make by defining a suitable NP machine N. The input to N is the triple (m, C, p) and the number of accepting paths has the property $\mathit{acc}_N(m, C, p) = c_{\bar{e}} (\mathrm{mod}\ p)$. Such an NP machine N would clearly suffice. We now define the NP machine N. W.l.o.g. we can assume that each gate of C has fanin two and is either a multiply gate or a plus gate. Suppose there are t plus gates in C. The NP machine N nondeterministically branches into 2^t computation paths, where on each path it picks exactly one of the two inputs to the plus gate. As a result, on each of the 2^t computation paths N has picked a multiplicative subcircuit of C. Let $\pi \in \{0, 1\}^t$ denote such a computation path of N and let C_π denote the corresponding multiplicative subcircuit of C. Notice that each C_π defines a monomial with a coefficient $c_\pi m_\pi$, and from C_π in deterministic polynomial time we can compute m_π and $c_\pi (\mathrm{mod}\ p)$. Next, machine N proceeds as follows: if $m_\pi = m$ then N extends π into $c_\pi \mathrm{mod}\ p$ accepting computation paths, and otherwise N rejects along π. Clearly, $\mathit{acc}_N(m, C, p) = c_{\bar{e}} (\mathrm{mod}\ p)$.

For the second part when $\mathbb{F} = \mathbb{F}_p$ the proof is similar. The crucial difference is that we do not need to evaluate the circuit modulo a randomly chosen prime. Furthermore, we only need the number of accepting paths of N modulo p. Hence a $\mathrm{Mod}_p\mathrm{P}$ oracle suffices with an NP base machine. ∎

4 Monomial Ideal Membership for $\Sigma\Pi\Sigma$ circuits

Consider instances (f, I) of Monomial Ideal Membership where f is given by a $\Sigma\Pi\Sigma$ circuit with top gate of bounded fanin and $I = \langle m_1, m_2, \cdots, m_k\rangle$ a monomial ideal for constant k. By Lemma 3 this problem reduces to testing if f is in a monomial ideal of the form $I = \langle x_1^{e_1}, x_2^{e_2}, \cdots, x_k^{e_k}\rangle$. As the quotient ring $\mathbb{F}[x_1, x_2, \cdots, x_k]/I$ is a local ring and $f \in I$ if and only if $f \equiv 0$ over the local ring $\mathbb{F}[x_1, x_2, \cdots, x_k]/I$ we can apply the Kayal-Saxena deterministic identity test [KS07] for such $\Sigma\Pi\Sigma$ circuit over local rings[3] to check this in overall time polynomial in the circuit size.

[3] More precisely, over local rings that allow polynomial-time arithmetic in them.

However, in this section we develop the algorithm and its correctness proof based on Gröbner basis theory. The algorithm is essentially from [KS07]. But the Gröbner basis approach is somewhat simpler and direct. It avoids invoking properties such as Chinese remaindering in local rings and Hensel lifting. The added bonus is that we get a different correctness proof for the Kayal-Saxena identity test.

Definition 3. *A $\Sigma\Pi\Sigma$ circuit C with n inputs over a field $\mathbb{F}$ computes a polynomial of the form: $C(x_1, x_2, \cdots, x_n) = \sum_{i=1}^{k} \prod_{j=1}^{d_i} L_{ij}(x_1, x_2, \cdots, x_n)$, where k is the fanin of the top Σ gate, and d_i are the fanins of the k different Π gates and L_{ij}'s are linear forms over $\mathbb{F}[x_1, x_2, \cdots, x_n]$.*

First, we transform the circuit C into another circuit C' as follows: Let $L_{ij} = \sum_{t=1}^{n} \alpha_{ijt} x_t + \beta$ for $\alpha_{ijt}, \beta \in \mathbb{F}$. We replace each such L_{ij} by $L'_{ij} = \sum_{t=1}^{n} \alpha_{ijt} x_t + \beta y$, where y is a new indeterminate. Let d be the maximum of the fanins of the Π gates. For a Π gate of fanin d_i introduce $d - d_i$ new input fanin wires each carrying y.

Proposition 1. *For $I = \langle x_1^{e_1}, x_2^{e_2}, \cdots, x_k^{e_k} \rangle$ and a $\Sigma\Pi\Sigma$ circuit C defined as above, $C \in I$ if and only if $C' \in \langle x_1^{e_1}, x_2^{e_2}, \cdots, x_k^{e_k}, y - 1 \rangle$.*

Notice that in the process of making this transformation the resulting ideal is not a monomial ideal any more.

Thus, we can assume that in the circuit C itself every L_{ij} is of the form $\sum_{t=1}^{n} \alpha_t x_t$ and the degree of the polynomial computed at each Π gate is d. We can naturally associate to L_{ij} its coefficient vector $(\alpha_1, \alpha_2, \cdots, \alpha_n) \in \mathbb{F}^n$. A collection of linear forms is *independent* if their coefficient vectors forms a linearly independent set in $\mathbb{F}^n$.

First we fix some notation. Let R denote the polynomial ring $\mathbb{F}[x_1, x_2, \cdots, x_k]$, where k will be clear from the context where R is used. For $\alpha = (e_{k+1}, e_{k+2}, \cdots, e_n) \in \mathbb{N}^{n-k}$, let $\bar{x}^{\bar{\alpha}}$ denote $x_{k+1}^{e_{k+1}} x_{k+2}^{e_{k+2}} \cdots x_n^{e_n}$. The only monomial ordering we use is the lex-ordering defined in Definition 1 w.r.t. the order $x_1 < x_2 < \cdots < x_n$. We can consider an $f \in \mathbb{F}[x_1, \cdots, x_n]$ as a polynomial in $R[x_{k+1}, x_{k+2}, \cdots, x_n]$. More precisely, we can write $f = \sum_{\bar{\alpha} \in \mathbb{N}^{n-k}} A_{\bar{\alpha}} \bar{x}^{\bar{\alpha}}$, where $A_{\bar{\alpha}} \in \mathbb{F}[x_1, x_2, \cdots, x_k] \setminus \{0\}$. Let $\bar{\alpha_1}$ be such that $\bar{x}^{\bar{\alpha_1}}$ is the lex-largest term such that $A_{\bar{\alpha_1}} \neq 0$. Then we denote the R-leading term $A_{\bar{\alpha_1}} \bar{x}^{\bar{\alpha_1}}$ of f by $LT_R(f)$. Likewise, $LM_R(f) = \bar{x}^{\bar{\alpha_1}}$ and $LC_R(f) = A_{\bar{\alpha_1}}$ is the R-leading monomial and R-leading coefficient of f. For any $f, g \in \mathbb{F}[x_1, \cdots, x_n]$, it is clear that $LM_R(fg) = LM_R(f) LM_R(g)$, $LC_R(fg) = LC_R(f) LC_R(g)$.

Let $f \in \mathbb{F}[x_1, \cdots, x_n]$ and $I = \langle f_1, f_2, \cdots, f_\ell \rangle$ be an ideal such that each f_i is in $\mathbb{F}[x_1, x_2, \cdots, x_k]$. Then the following easy lemma states a necessary and sufficient condition for f to be in I.

Lemma 5. *Let $I \subseteq \mathbb{F}[\bar{x}]$ be an ideal generated by the polynomials $f_1, f_2, \cdots, f_\ell$ such that for all $i \in [\ell]$, $f_i \in \mathbb{F}[x_1, x_2, \cdots, x_k]$. Let g be any polynomial in $\mathbb{F}[\bar{x}]$. Write $g = \sum_{\bar{\alpha} \in \mathbb{N}^{n-k}} A_{\bar{\alpha}} \bar{x}^{\bar{\alpha}}$. Then $g \in I$ if and only if for all $\bar{\alpha}$, $A_{\bar{\alpha}} \in I$.*

Consider polynomials $f, g \in \mathbb{F}[x_1, x_2, \cdots, x_n]$ and an ideal I such that $g \in \langle I, f \rangle$. The following useful lemma gives a sufficient condition on f under which the remainder r obtained when we invoke Divide$(g; f)$ (of Theorem 1) is in the ideal I.

Lemma 6. *Let $I = \langle f_1, f_2, \cdots, f_\ell \rangle$ be an ideal in $\mathbb{F}[x_1, \cdots, x_n]$ where $f_i \in \mathbb{F}[x_1, \cdots, x_k] = R$. Suppose f is a polynomial such that $LM(f)$ contains only variables from $\{x_{k+1}, x_{k+2}, \cdots, x_n\}$ (i.e. $LM(f) = LM_R(f)$). Then for any polynomial g in the ideal $\langle I, f \rangle$ we can write $g = qf + r$ for polynomials q and r such that $r \in I$ and no monomial of r is divisible by $LM(f)$.*

Proof. The lemma is an easy consequence of the properties of the Divide algorithm explained in Theorem 1. Notice that Divide$(g; f)$ will stop with a remainder polynomial r such that $g = qf + r$ with the property that no monomial of r is divisible by $LM(f)$. However, we only know that $r \in \langle I, f\rangle$, because both g and qf are in $\langle I, f\rangle$. We now show that r must be in I. First, as $r \in \langle I, f\rangle$ we can write $r = \sum_{i=1}^{\ell} a_i f_i + af$, for polynomials a_i and a. Following Lemma 5, we write $a_i = \sum_{\bar{\alpha}} a_{i\bar{\alpha}} \bar{x}^{\bar{\alpha}}$ for each i and also $a = \sum_{\bar{\alpha}} a_{\bar{\alpha}} \bar{x}^{\bar{\alpha}}$. Notice that we can assume $a_{\bar{\alpha}} \notin I$ for all nonzero $a_{\bar{\alpha}}$. Otherwise, we can move that term to the $\sum a_i f_i$ part. Since $LM(f)$ does not divide any monomial of r, it follows that $LM(af)$ does not occur in a nonzero term of r. Therefore, $LT(af)$ must be cancelled by some term of $\sum_{i=1}^{\ell} a_i f_i$. Clearly, $LT(af)$ is of the form $c \cdot a_{\bar{\beta}} \bar{x}^{\bar{\alpha}}$ for some α, β, where $LC(f) = c \in \mathbb{F}$ and $a_{\bar{\beta}} = LC_R(a)$. Now, in $\sum_{i=1}^{\ell} a_i f_i$ the coefficient of $\bar{x}^{\bar{\alpha}}$ is $\sum_{i=1}^{\ell} a_{i\bar{\alpha}} f_i$ which must be equal to $-c \cdot a_{\bar{\beta}}$. Since $c \in \mathbb{F}$ it follows that $a_{\bar{\beta}}$ is in I contradicting the assumption that none of the nonzero $a_{\bar{\gamma}}$ is in I. ∎

Again, let $I = \langle f_1, f_2, \cdots, f_\ell\rangle$ such that the f_i are in $\mathbb{F}[x_1, x_2, \cdots, x_k]$. Consider two polynomials f and g such that $LM(f)$ contains only variables from $x_{k+1}, x_{k+2}, \cdots, x_n$ and either $LM(f) > LM(g)$ or $LM_R(f) = LM_R(g)$ and $LC_R(g) \in I$. Then, g is in the ideal $\langle I, f\rangle$ if and only if $g \in I$.

Lemma 7. *Let $I = \langle f_1, f_2, \cdots, f_\ell\rangle$ be an ideal in $\mathbb{F}[x_1, \cdots, x_n]$ such that each f_i is in $\mathbb{F}[x_1, x_2, \cdots, x_k] = R$. Suppose f is a polynomial such that $LM(f)$ is over the variables only from $\{x_{k+1}, x_{k+2}, \cdots, x_n\}$ (i.e. $LM(f) = LM_R(f)$). Then for any polynomial g such that either $LM(f) > LM(g)$, or $LM_R(f) = LM_R(g)$ and $LC_R(g) \in I$, g is in the ideal $\langle I, f\rangle$ if and only if g is in the ideal I.*

Proof. Suppose $g \in \langle I, f\rangle$ and $g \notin I$. We can write $g = a + bf$, for polynomials a and b, where $a \in I$. Also, we can assume that $b \notin I$, for otherwise $g \in I$ and we are done. Let $b = \sum_{\bar{\alpha}\in\mathbb{N}^{n-k}} b_{\bar{\alpha}} \bar{x}^{\bar{\alpha}}$, where $b_{\bar{\alpha}} \in \mathbb{F}[x_1, x_2, \cdots, x_k]$ and we can assume $b_{\bar{\alpha}} \notin I$ for all $\bar{\alpha}$ (otherwise we can move that term as part of a). Notice that $LT_R(bf) = LT_R(b) \cdot LT_R(f) = cb_{\bar{\beta}} LM_R(b) LM_R(f) = cb_{\bar{\beta}} \bar{x}^{\bar{\gamma}}$ for some $\bar{\gamma}$ and for some $b_{\bar{\beta}}$, where $c = LC_R(f) \in \mathbb{F}$. Since $b_{\bar{\beta}} \notin I$ it follows that $LC_R(bf) \notin I$. Write $a = \sum_{\bar{\alpha}\in\mathbb{N}^{n-k}} a_{\bar{\alpha}} \bar{x}^{\bar{\alpha}}$. By Lemma 5, $a \in I$ implies each $a_{\bar{\alpha}} \in I$. In particular, $a_{\bar{\gamma}} \in I$ and is *not* equal to $-LC_R(b \cdot f) = -cb_{\bar{\beta}}$ as $b_{\bar{\beta}} \notin I$. Thus, the monomial $LM_R(bf)$ survives in $a + bf$. It follows that $LM_R(g) = LM_R(a + bf) \geq LM_R(bf) \geq LM_R(f)$ which forces $LM_R(f) = LM_R(g)$ and $LC_R(g) \in I$ by assumption. If $b \notin R$ then $LM_R(b \cdot f) > LM_R(f)$ which implies $LM_R(g) > LM_R(f)$ contradicting assumption. If $b \in R$ then $LT_R(g) = LT_R(a + bf) = (a_{\bar{\alpha}} + b) LM_R(f)$ for some $a_{\bar{\alpha}}$, which forces $b \in I$ because both $LT_R(g), a_{\bar{\alpha}} \in I$. ∎

Let $I \subseteq \mathbb{F}[x_1, \cdots, x_n]$ be an ideal and g_1, g_2 are two polynomials such that f is in the ideals $\langle I, g_1\rangle$ and $\langle I, g_2\rangle$. Using some Gröbner basis theory we give a sufficient condition on I, g_1 and g_2 under which we can infer that f is in the ideal $\langle I, g_1 g_2\rangle$.

Lemma 8. *Let $I = \langle f_1, f_2, \cdots, f_\ell\rangle$ be an ideal of $\mathbb{F}[x_1, x_2, \cdots, x_n]$, where f_i are polynomials in $\mathbb{F}[x_1, x_2, \cdots, x_k]$. Suppose g_1 and g_2 are polynomials such that: $g_2 = \prod_{i=1}^{d_2} (x_{k+1} - \alpha_i)$, where each α_i is a linear form over $x_1, x_2, \cdots, x_k$, and the leading term $LT(g_1)$ of g_1 has only variables from $\{x_{k+2}, x_{k+3}, \cdots, x_n\}$. Then $f \in \langle I, g_1 g_2\rangle$ if and only if $f \in \langle I, g_1\rangle$ and $f \in \langle I, g_2\rangle$.*

Proof. The reverse implication is obvious. We prove the forward direction. Suppose $f \in \langle I, g_1\rangle$ and $f \in \langle I, g_2\rangle$. As $f \in \langle I, g_2\rangle$, we can write $f = a + bg_2$, where $a \in I$ and b is an arbitrary polynomial. Notice that it suffices to prove bg_2 is in the ideal $\langle I, g_1 g_2\rangle$. Now, since $f \in \langle I, g_1\rangle$ and $a \in I$ it follows that $bg_2 = f - a \in \langle I, g_1\rangle$. By applying Lemma 6 to ideal I and polynomial g_1 observe that we can write $bg_2 = \alpha g_1 + \beta$, where β is a polynomial in I such that none of the monomials of β is divisible by $LT(g_1)$. We have the following equation $b \cdot \prod_{j=1}^{d_2}(x_{k+1} - \alpha_j) = \alpha g_1 + \beta$.

Substituting $x_{k+1} = \alpha_1$ in the above equation, we get $(\alpha g_1)|_{x_{k+1}=\alpha_1} = -\beta|_{x_{k+1}=\alpha_1}$. Notice that $LT(g_1|_{x_{k+1}=\alpha_1}) = LT(g_1)$, as $LT(g_1)$ contains variables only from $x_{k+2}, \cdots, x_n$. Thus the above substitution implies $LT(\beta|_{x_{k+1}=\alpha_1}) = -LT((\alpha g_1)|_{x_{k+1}=\alpha_1}) = -LT(\alpha|_{x_{k+1}=\alpha_1}) \cdot LT(g_1|_{x_{k+1}=\alpha_1}) = -LT(\alpha|_{x_{k+1}=\alpha_1}) \cdot LT(g_1)$.

Thus $LM(g_1)$ divides $LM(\beta|_{x_{k+1}=\alpha_1})$. On the other hand, since $LM(g_1)$ does not divide any monomial of β, $LM(g_1)$ cannot divide any monomial of $LM(\beta|_{x_{k+1}=\alpha_1})$ as the substitution only introduces variables from $\{x_1, \cdots, x_k\}$. This gives a contradiction unless $\beta|_{x_{k+1}=\alpha_1} = 0$, which in turn implies $\alpha|_{x_{k+1}=\alpha_1} = 0$.

Thus we have proved that $(x_{k+1} - \alpha_1)$ is a factor of both α and β. This leads us to the following similar identity: $b \cdot \prod_{j=2}^{d_2}(x_{k+1} - \alpha_j) = \alpha_1 g_1 + \beta_1$, where $\alpha_1 = \alpha/(x_{k+1} - \alpha_1)$ and $\beta_1 = \beta/(x_{k+1} - \alpha_1)$. Clearly, by repeating the above argument we finally get, $b = \alpha' g_1 + \beta'$, for some polynomials α' and β' where $\alpha = \alpha' g_2$ and $\beta = \beta' g_2$. Putting it together we get $bg_2 = \alpha' g_1 g_2 + \beta' g_2 = \alpha' g_1 g_2 + \beta$. As $\beta \in I$, it follows that bg_2 is in the ideal $\langle I, g_1 g_2 \rangle$. This completes the proof. ∎

Let $I = \langle P_1, P_2, \cdots, P_k \rangle$ be an ideal in $\mathbb{F}[x_1, \cdots, x_n]$ such that $P_i \in \mathbb{F}[x_1, x_2, \cdots, x_i]$ and $LT(P_i) = x_i^{d_i}$ for each i. For $i \neq j$ the leading terms $LT(P_i) = x_i^{d_i}$ and $LT(P_j) = x_j^{d_j}$ are clearly relatively prime. Therefore by Theorem 3, it follows that $\{P_1, P_2, \cdots, P_k\}$ is in fact a Gröbner basis for I. We summarize this observation.

Lemma 9. *Let $I = \langle P_1, P_2, \cdots, P_k \rangle$ be an ideal in $\mathbb{F}[x_1, \cdots, x_n]$ such that each P_i is in $\mathbb{F}[x_1, x_2, \cdots, x_i]$ and $LT(P_i) = x_i^{d_i}$. Then $\{P_i\}_{i \in [k]}$ is a Gröbner basis for I.*

Let $f \in \mathbb{F}[x_1, x_2, \cdots, x_k]$ be a given polynomial and d be the maximum of $\deg(f)$ and $\deg(P_i), 1 \leq i \leq k$. We can invoke Divide$(f; P_1, P_2 \cdots, P_k)$ (Theorem 1) to test whether $f \in I$. By Fact 2 the running time for this test is $O(d^k)$.

Now we state the main theorem of this section.

Theorem 7. *Let $C \in \mathbb{F}[x_1, x_2 \cdots, x_n]$ be given by a $\Sigma\Pi\Sigma(\ell, d)$ circuit for a constant ℓ and $I = \langle m_1, m_2, \cdots, m_k \rangle$ be a monomial ideal for constant k. For such instances, Monomial Ideal Membership can be checked in deterministic polynomial time. Specifically, the running time is bounded by $n^k \mathrm{poly}(n, d^{max\{\ell,k\}})$.*

By Lemma 3 it clearly suffices to give a polynomial-time deterministic algorithm for testing if a $\Sigma\Pi\Sigma(\ell, d)$ circuit C is in a monomial ideal of the form $\langle x_1^{e_1}, \cdots, x_k^{e_k} \rangle$. As explained in the beginning of this section, we transform the circuit C to C' in which all linear forms are made homogeneous using a new indeterminate y, and $C \in I$ if and only if $C' \in \langle x_1^{e_1}, \cdots, x_k^{e_k}, y - 1 \rangle$. In fact, in the following theorem we prove a stronger result which along with Lemma 3 yields Theorem 7.

Theorem 8. *Let C be a given $\Sigma\Pi\Sigma(\ell, d)$ circuit for a constant ℓ and $I = \langle P_1, P_2, \cdots, P_k \rangle$ be an ideal in $\mathbb{F}[x_1, \cdots, x_n]$ such that $P_i \in \mathbb{F}[x_1, x_2, \cdots, x_i]$ and $LT(P_i) = x_i^{d_i}$ for each i. Further, suppose $d_i \leq d$ for all $i \in [k]$. Then testing if $C \in I$ can be done deterministically in time* $\mathrm{poly}(d^{max\{\ell,k\}})$.

Proof. We first describe the algorithm and then prove its correctness and running time bound.

As explained in the beginning of the section, we can assume that all linear forms appearing in C are homogeneous and C itself is a homogeneous degree d polynomial. By Lemma 9, the generating set for I is a Gröbner basis. Let $C(x_1, x_2, \cdots, x_n) = \sum_{i=1}^{\ell} T_i$. For all $i \in [\ell]$, $T_i = \prod_{j=1}^{d} L_{ij}$, where L_{ij}'s are the linear forms over $\mathbb{F}[x_1, x_2, \cdots, x_n]$.

If $\ell = 1$, then $C = T_1$. Let $g(x_1, x_2, \cdots, x_k)$ be the product of those linear forms of T_1 using only variables from $\{x_1, x_2, \cdots, x_k\}$. Clearly, $g(x_1, x_2, \cdots, x_k)$ has at most d^k monomials. We explicitly compute g by multiplying out all such linear forms. By Lemma 5, clearly $C \in I$ if and only if $g \in I$, which can be checked in time poly(d^k) following the Fact 2.

So, assume $\ell > 1$. If all the linear forms appearing in $T_1, T_2, \cdots, T_\ell$ are only over $\{x_1, x_2, \cdots, x_k\}$, then again the ideal membership testing is easy. Because, in time poly(d^k) we can write C itself as an $\mathbb{F}$-linear combination of monomials in $x_1, x_2, \cdots, x_k$ and apply Fact 2 to check if $f \in I$ in time poly(d^k).

Now we consider the general case. By inspection we can write each $T_i = \beta_i T'_i$ where the β_i are products of linear forms over only $x_1, x_2, \cdots, x_k$, whereas each linear form in T'_i involves at least one other variable.[4] If $\beta_i \in I$ (which we can test in polynomial time using Fact 2) we drop the term T_i from the sum $\sum_{i=1}^{\ell} T_i$. This enables us to write C as $C = \beta_1 T'_1 + \beta_2 T'_2 + \cdots + \beta_m T'_m$ for some $m \leq \ell$, where we have assumed for simplicity of notation that $\beta_i \notin I$ for first m terms.

As before, let $R = \mathbb{F}[x_1, x_2, \cdots, x_k]$. W.l.o.g, assume that $LM_R(T'_1) \geq LM_R(T'_i)$ for all $i \in [2, 3, \cdots, m]$. We can determine $LT_R(T'_i)$ for each T'_i in polynomial time since they are given as product of linear forms. Thus, $LM_R(T'_1) \geq LM_R(C)$. Now, let $r \in R$ be the coefficient of $LM_R(T'_1)$ in C. We can compute r in polynomial time by computing the coefficient γ_i of $LM_R(T'_1)$ in each T'_i and computing $r = \sum_{i=1}^{m} \beta_i \gamma_i$. Then we check that $r \in I$ (which is a necessary condition for C to be in I by Lemma 5). By Fact 2 we can check $r \in I$ in time poly(d^k). It is clear that, either $LM_R(T'_1) > LM_R(C)$ or $LM_R(T'_1) = LM_R(C)$ and $r \in I$. Thus, by the Lemma 7, $C \in I$ if and only if $C \in \langle I, T'_1 \rangle$.

Next, we group the linear forms in T'_1: let, $T'_1 = T_{11} T_{12} \cdots T_{1t}$, such that for all $i \in [t]$,

$$T_{1i} = (L_i + m_{i1})(L_i + m_{i2}) \cdots (L_i + m_{is_i}),$$

where $\{L_i\}_{i=1}^{t}$ are *distinct linear forms* in $\mathbb{F}[x_{k+1}, \cdots, x_n]$ and m_{ij}'s are linear forms in $\mathbb{F}[x_1, \cdots, x_k]$. Notice that the polynomials T_{1i} are relatively prime to each other.

We next compute t linear transformations $\{\sigma_1, \sigma_2, \cdots, \sigma_t\}$ from $\mathbb{F}^n$ to $\mathbb{F}^n$ with the following property: for $i \in [t]$, σ_i fixes $\{x_i\}_{i=1}^{k}$, maps L_i to x_{k+1} and maps $\{x_{k+2}, x_{k+3}, \cdots, x_n\}$ to some suitable linear forms in such a way that, σ_i is an invertible linear transformation. As L_i's are over $\{x_{k+1}, \cdots, x_n\}$, it is easy to see that such σ_i exist and are easy to compute.

Let $C_1 = \sum_{j \in [\ell] \setminus \{1\}} T_j$. For $i \in [t]$, let $C_{1i} = \sigma_i(C_1)$ and let I_{1i} be the ideal $\langle I, \sigma_i(T_{1i}) \rangle$. The algorithm will now recursively check for each of the $\Sigma\Pi\Sigma(\ell - 1, d)$ circuits C_{1i}, that C_{1i} is in the ideal I_{1i} and declare $C \in I$ if and only if $C_{1i} \in I_{1i}$ for each i.

Notice that the ideal I_{1i} has generating set $G = \{P_1, P_2, \cdots, P_k, P_{k+1}\}$, where $P_{k+1} \in \mathbb{F}[x_1, x_2, \cdots, x_{k+1}]$ and $LM(P_{k+1}) = x_{k+1}^{d_{k+1}}$. By Lemma 9, G is a Gröbner basis for I_{1i}.

The correctness of the algorithm follows directly from the following claim.

Claim. For each $s : 1 \leq s \leq t$ $C \in \langle I, T_{11} T_{12} \cdots T_{1s} \rangle$ if and only if $C_{1i} \in I_{1i}$ for $1 \leq i \leq s$.

In particular, $C \in \langle I, T'_1 \rangle$ if and only if $C_{1i} \in I_{1i}$ for $1 \leq i \leq t$.

Proof of Claim: The forward implication is easy: if $C \in \langle I, T_{11} T_{12} \cdots T_{1s} \rangle$ then clearly $C \in \langle I, T_{1i} \rangle$ for each $1 \leq i \leq s$. As each σ_i is an invertible linear map it follows in turn that $\sigma_i(C) \in \langle I, \sigma_i(T_{1i}) \rangle = I_{1i}$ for $1 \leq i \leq s$. Since $C_{1i} = \sigma_i(C) - \sigma_i(T_1)$ and $\sigma_i(T_1) \in \langle \sigma_i(T_{1i}) \rangle$ it follows that $C_{1i} \in I_{1i}$ for $1 \leq i \leq s$.

We prove the other direction of the claim by induction on s. The base case $s = 1$ is trivial. Inductively assume it is true for $s - 1$. I.e. if $C_{1i} \in I_{1i}$ for $1 \leq i \leq s - 1$ then $C \in \langle I, T_{11} T_{12} \cdots T_{1(s-1)} \rangle$.

[4] If there are no linear forms contributing to the product β_i (respectively, T'_i) we will set it to 1.

We now prove the induction step for s. Suppose $C_{1i} \in I_{1i}$ for $1 \leq i \leq s$. Let $T = T_{11}T_{12}\cdots T_{1(s-1)}$. By induction hypothesis we have $C \in \langle I, T\rangle$. Furthermore, $C_{1s} \in I_{1s}$ implies by definition that $C \in \langle I, T_{1s}\rangle$. Now we apply the linear map σ_s to obtain $\sigma_s(C) \in \langle I, \sigma_s(T)\rangle$ and $\sigma_s(C) \in \langle I, \sigma_s(T_{1s})\rangle$. The map σ_s ensures that $LT(T_{1s})$ is of the form $x_{k+1}^{\deg T_{1s}}$. Furthermore, by the definition of σ_s it follows that $LT(\sigma_s(T))$ has only variables in $\{x_{k+2}, \cdots, x_n\}$. Letting $g_1 = \sigma_s(T)$ and $g_2 = \sigma_s(T_{1s})$ in Lemma 8, it follows immediately that $\sigma_s(C) \in \langle I, \sigma_s(T \cdot T_{1s})\rangle$ which implies the induction step since σ_s is invertible.

Claim. The above algorithm runs in time poly$(n, d^{\max\{\ell,k\}})$.

Proof of Claim: To analyze the running time, we need to observe the following recurrence relation : let $T(\ell, n)$ is the time required to test $C \in I$. It is easy to see from the description of the algorithm that, $T(\ell, n) \leq tT(\ell-1, n) + \text{poly}(n, d^k)$. So, $T(\ell, n) = \text{poly}(n, d^{\max\{\ell,k\}})$ as $t = O(d)$. ■

Theorem 7 is an immediate consequence of Theorem 8. For $I = \langle 0\rangle$, Theorem 7 is actually the Kayal-Saxena deterministic test with a new proof.

5 Monomial Ideal Membership for black-box polynomials

In Theorem 4 we have shown that monomial ideal membership is in randomized polynomial time when $f \in \mathbb{F}[\bar{x}]$ is given as an arithmetic circuit and the monomial ideal is given by a constant number of generator monomials. We now show that even if f is accessed only via a *black-box*, if the degree of f is *polynomial in the input size* we can still solve monomial ideal membership in randomized polynomial time (assuming I is generated by constant number of monomials). In [OT88], Ben-Or and Tiwari gave an interpolation algorithm for sparse multivariate polynomials over integers. Our algorithm is an easy application of their result. We first recall their result in a form suitable for us.

Theorem 9. [OT88] *Let $f \in \mathbb{Z}[x_1, x_2, \cdots, x_n]$ be a t-sparse multivariate polynomial given as a black-box (by t-sparse we mean the number of monomials in f is bounded by t), d be the degree of f, and b be a bound on the size of its coefficients. There is a deterministic algorithm that queries the black-box for values of f on different inputs and reconstructs the entire polynomial f in time* poly(t, n, d, b).

Ben-Or and Tiwari's result directly gives a deterministic polynomial time algorithm for Monomial Ideal Membership when f is a t-sparse black-box polynomial over $\mathbb{Z}$, and I is any monomial ideal. The algorithm simply reconstructs f and checks if each of its monomials is in I.

Next, suppose f is a black-box polynomial of small degree and I is a monomial ideal generated by constant number of monomials.

Theorem 10. *Let $f \in \mathbb{Z}[\bar{x}]$ of degree d given as a black-box such that b is a bound on the size of its coefficients. Suppose $I = \langle m_1, m_2, \cdots, m_k\rangle$ for constant k. Then we can test if $f \in I$ in randomized time* poly(n^k, d^k, b).

Proof. By Lemma 3, it suffices to give a randomized polynomial time algorithm for testing if $f \in I_{\bar{v}}$, where $\bar{v} \in [n]^k$. W.l.o.g. assume $I_{\bar{v}} = \langle x_1^{e_1}, x_2^{e_2}, \cdots, x_k^{e_k}\rangle$. Fix $S = \{1, 2, \cdots, s\}$ and assign random values $\{r_1, r_2, \cdots, r_{n-k}\}$ to $\{x_{k+1}, \cdots, x_n\}$ from S. Note that $f(x_1, x_2, \cdots, x_k, \bar{r})$ is a d^k-sparse polynomial. By Theorem 9 we can reconstruct $f(x_1, x_2, \cdots, x_k, \bar{r})$ in poly(n, d^k, b) time. Let $g(x_1, x_2, \cdots, x_k) = f(x_1, x_2, \cdots, x_k, \bar{r})$. Our randomized algorithm declares $f \in I_{\bar{v}}$ if each monomial of g is in I. By Lemma 4, it follows that the success probability of the algorithm is at least $1 - \frac{d}{s}$. ■

6 Bounded variable Ideal Membership

In this section we discuss our results for the ideal membership problem when $I = \langle f_1, \cdots, f_\ell \rangle$ such that $f_i \in \mathbb{F}[x_1, \cdots, x_k]$ for a constant k and the polynomial f is given by an arithmetic circuit. We call this variant *bounded variable Ideal Membership*.

A pioneering result in polynomial Ideal Membership testing is Hermann's algorithm that is based on the following theorem.

Theorem 11 (Hermann's theorem). [He26] *Consider polynomials $f, f_1, f_2, \cdots, f_m \in \mathbb{F}[x_1, x_2, \cdots, x_k]$ for a field $\mathbb{F}$ such that $\max\{\deg(f_1), \deg(f_2), \cdots, \deg(f_m), \deg(f)\} \leq d$. If f is in the ideal $I = \langle f_1, f_2, \cdots, f_m \rangle$ then f can be expressed as $f = \sum_{i=1}^{m} g_i f_i$ where $\deg(g_i) \leq (2d)^{2^k}$ for each i.*

Suppose f is given explicitly as an $\mathbb{F}$-linear combination of terms. Using the bounds of Hermann's theorem, Hermann's algorithm treats the coefficients of g_i as unknowns and does membership testing in $\langle f_1, f_2, \cdots, f_m \rangle$ by solving a system of linear equations with $m(2d)^{k2^k}$ unknowns. This can be solved using Gaussian elimination in time $m^{O(1)}(2d)^{O(k2^k)}$.

Similarly, for an explicitly given $f \in \mathbb{F}[x_1, \cdots, x_n]$, $n > k$, using Lemma 5 we can apply Hermann's algorithm to test if membership of f in $\langle f_1, f_2, \cdots, f_m \rangle$ in time polynomial in the size of f and $m^{O(1)}(2d)^{O(k2^k)}$. If k is a constant, this gives a polynomial running time bound.

A natural question here is the complexity of Ideal Membership when f is given by an arithmetic circuit whose membership we want to test in ideal $I = \langle f_1, f_2, \cdots, f_m \rangle$, where $f_i \in \mathbb{F}[x_1, \cdots, x_k]$ for constant k. Recall that in Theorem 4 we showed a similar problem for *monomial* ideals with constant number of monomials is in randomized polynomial time. In this section we will restrict ourselves to polynomials f computed by arithmetic circuits of polynomial degree in the input size. We can follow essentially the same proof idea in the Theorem 4. Notice that $f \in I$ if and only if $f \equiv 0$ in the ring $R[x_{k+1}, x_{k+2}, \cdots, x_n]$ where $R = \mathbb{F}[x_1, x_2, \cdots, x_k]/I$. We need the following proposition about zeros of a univariate polynomial over an arbitrary ring.

Proposition 2. *Let R be an arbitrary commutative ring containing a field $\mathbb{F}$. If $f \in R[x]$ is a nonzero polynomial of degree d then $f(a) = 0$ for at most d distinct values of $a \in \mathbb{F}$.*

Proof. Suppose $a_1, a_2, \cdots, a_{d+1} \in \mathbb{F}$ are distinct points such that $f(a_i) = 0, 1 \leq i \leq d+1$. Then, we can write $f(x) = (x - a_1)q(x)$, for $q(x) \in R[x]$. Now, dividing $q(x)$ by $x - a_2$ yields $q(x) = (x - a_2)q'(x) + q(a_2)$, for some $q'(x) \in R[x]$. Thus, $f(x) = (x - a_1)(x - a_2)q'(x) + (x - a_1)q(a_2)$. Putting $x = a_2$ in this equation gives $(a_2 - a_1)q(a_2) = 0$. But $a_2 - a_1$ is a nonzero element in $\mathbb{F}$ and is hence invertible. Therefore, $q(a_2) = 0$. Consequently, $f(x) = (x - a_1)(x - a_2)q'(x)$. Applying this argument successively for the other a_i finally yields $f(x) = g(x)\prod_{i=1}^{d+1}(x - a_i)$ for some nonzero polynomial $g(x) \in R[x]$. Since $\prod_{i=1}^{d+1}(x - a_i)$ is a monic polynomial, this forces $\deg(f) \geq d + 1$ which is a contradiction. ∎

Using an induction argument as in [TZ06, Lemma D.3], we can now easily derive the following analog of the Schwartz-Zippel test for arbitrary commutative rings.

Lemma 10. *Let R be an arbitrary commutative ring containing a field $\mathbb{F}$. Let $g \in R[x_1, x_2, \cdots, x_m]$ be any polynomial of degree at most d. If $g \not\equiv 0$, then for any finite subset A of $\mathbb{F}$ we have*

$$\mathrm{Prob}_{a_1 \in A, \cdots, a_m \in A}[g(a_1, a_2, \cdots, a_m) = 0 \mid g \not\equiv 0] \leq \frac{md}{|A|}.$$

Now we describe our ideal membership test: Choose and fix $S \subseteq F$ of size $2(n-k)d$ and randomly assign values from S to the variables in $\{x_{k+1}, \cdots, x_n\}$. Notice that f, given by a polynomial degree arithmetic circuit C, is in I if and only if $f \equiv 0$ in the ring $R[x_{k+1}, x_{k+2}, \cdots, x_n]$ where $R = \mathbb{F}[x_1, x_2, \cdots, x_k]/I$, since the given generating set for I uses only variables $x_1, \cdots, x_k$. After the random substitution we are left with an arithmetic circuit $C'(x_1, \cdots, x_k)$. Notice that, by Lemma 10 if $f \notin I$ then $C'(x_1, \cdots, x_k) \notin I$ with probability at least $1/2$. We now need to test whether the polynomial computed by C' is in I. As C' is of polynomial degree d and k is a constant, we can explicitly written down the polynomial r that it computes as a $\mathbb{F}$-linear combination of at most d^k monomials. We are now left with the problem of testing if $r \in \langle f_1, \cdots, f_\ell \rangle$ which we can do in polynomial time using Hermann's algorithm as k is a constant. Similarly, Theorem 10 for black-box polynomials can be easily extended to bounded variable Ideal Membership.

Finally, when f is given by a $\Sigma\Pi\Sigma$ circuit with bounded fanin output gate, we can easily argue by following the algorithm in the proof of Theorem 8 that we will end up with the problem of testing if a polynomial g given by a $\Pi\Sigma$ circuit is in an ideal $\langle f_1, \cdots, f_\ell \rangle$, where f_i are all in $\mathbb{F}[x_1, \cdots, x_t]$ for a constant t. It is easy to see that we can apply Hermann's algorithm to check this in time polynomial in $(m+n+d)^{O(t2^t)}$ which is a polynomial time bound as t is constant. We summarize this result in the following theorem.

Theorem 12. *Let $I = \langle f_1, f_2, \cdots, f_m \rangle$ be an ideal in $\mathbb{F}[x_1, x_2, \cdots, x_n]$ where each $f_i \in \mathbb{F}[x_1, x_2, \cdots, x_k]$ for constant k. If f be a polynomial given by an arithmetic circuit of polynomial degree, then in randomized polynomial time we can test if $f \in I$. This result holds even if f is given by a black-box and the degree of f is polynomial in the input size. Further, if f is given by a $\Sigma\Pi\Sigma(\ell, d)$ circuit with ℓ constant, then we can test whether $f \in I$ in deterministic polynomial time.*

7 Identity Testing for a restricted class of $\Sigma\Pi\Sigma\Pi$ circuits

In this section we examine the possibility of extending [KS07] to certain depth 4 circuits. We consider certain restricted $\Sigma\Pi\Sigma\Pi$ circuits with the top Σ gate having bounded fanin.

Any $\Sigma\Pi\Sigma\Pi$ circuit is of the form $C = \sum_{i=1}^{\ell} T_i$, with $T_i = \prod_{j=1}^{d} P_{ij}$, for polynomials P_{ij}. We now define a *restricted subclass* of circuits which we denote by $\Sigma\Pi\Sigma\Pi(\ell, d, c)$. A circuit C is in this class if

(a) The fanin ℓ of the output Σ gate is a constant.
(b) Furthermore, each P_{ij} is the sum of at most c different *univariate* polynomials, where c is also a constant.

We show that the bounded variable Ideal Membership problem for $\Sigma\Pi\Sigma\Pi(\ell, d, c)$ circuits can be solved in polynomial time. As a consequence we obtain a deterministic polynomial-time identity testing algorithm for such circuits. The key observation is the next lemma which generalizes Lemma 8.

Lemma 11. *Let $I = \langle f_1, f_2, \cdots, f_\ell \rangle$ be an ideal of $\mathbb{F}[x_1, x_2, \cdots, x_n]$, where f_i are polynomials in $\mathbb{F}[x_1, \cdots, x_k]$. Suppose g_1 and g_2 are the polynomials such that:*

1. *$LM(g_1) = x_i^{d_i}$, where $i \in \{k+1, k+2, \cdots, n\}$.*
2. *$LM(g_2) < LM(g_1)$ and $LM(g_2), LM(g_1)$ are relatively prime.*

Then $f \in \langle I, g_1 \rangle$ and $f \in \langle I, g_2 \rangle$ if and only if $f \in \langle I, g_1 g_2 \rangle$.

Proof. The reverse implication is obvious. We prove the forward direction. As $LM(g_2) < LM(g_1)$ and $LM(g_2), LM(g_1)$ are relatively prime, it follows that $g_2 \in \mathbb{F}[x_1, x_2, \cdots, x_{i-1}]$.

As $f \in \langle I, g_2 \rangle$, we can write $f = a + bg_2$, where $a \in I$ and b is an arbitrary polynomial. Furthermore, by Lemma 6 we can write $bg_2 = \alpha g_1 + \beta$, with $\beta \in I$ such that no monomial of β is divisible by $LT(g_1)$. Thus g_2 divides $\alpha g_1 + \beta$. Let p be any irreducible factor of g_2. As the ideal $\langle p \rangle$ generated by the polynomial p is a prime ideal of $R = \mathbb{F}[x_1, x_2, \cdots, x_{i-1}]$, the quotient ring $D = R/\langle p \rangle$ is an integral domain. As p divides $\alpha g_1 + \beta$, it follows that $\alpha g_1 = -\beta$ in $D[x_i]$. We will now argue that β and α must be both zero in $D[x_i]$, which will imply that p divides both α and β. Note that $LM_D(\beta) = -LM_D(\alpha) \cdot LM_D(g_1)$ (by comparing their x_i degrees in the ring $D[x_i]$). But $LM_D(g_1) = LM(g_1) = x_i^{d_i}$ from the statement of the lemma. Considering β as a polynomial of $R[x_i]$, notice that β has degree strictly less than d_i since $LM(g_1) = x_i^{d_i}$ does not divide any monomial of β. Since $p \in R = \mathbb{F}[x_1, x_2, \cdots, x_{i-1}]$, it follows that β as a polynomial of $D[x_i]$ also has degree strictly less than d_i. Thus, $LM_D(g_1)$ can not divide $LM_D(\beta)$. The only possibility left is that $\alpha = \beta = 0$ in $D[x_i]$, which implies that p divides α and β.

This leads us to the following similar identity: $bg_2' = \alpha_1 g_1 + \beta_1$, where $\alpha_1 = \alpha/p$ and $\beta_1 = \beta/p$. Clearly, by the same argument applied to each irreducible factor of g_2 (with repetition) we finally get $b = \alpha' g_1 + \beta'$, for polynomials α' and β' where $\alpha = \alpha' g_2$ and $\beta = \beta' g_2$. Putting it together, $bg_2 = \alpha' g_1 \cdot g_2 + \beta' g_2 = \alpha' g_1 \cdot g_2 + \beta$. As $\beta \in I$, it follows that bg_2 is in the ideal $\langle I, g_1 g_2 \rangle$. This completes the proof. ∎

Now we present the polynomial time algorithm for bounded variable ideal membership instances (f, I), where the polynomial f is given by a $\Sigma\Pi\Sigma\Pi(\ell, d, c)$ circuit. The polynomial-time identity test for $\Sigma\Pi\Sigma\Pi(\ell, d, c)$ circuits is a corollary.

Theorem 13. *Let C be a given $\Sigma\Pi\Sigma\Pi(\ell, d, c)$ circuit and $I = \langle f_1, f_2, \cdots, f_m \rangle$ be an ideal in $\mathbb{F}[x_1, \cdots, x_n]$ such that each $f_i \in \mathbb{F}[x_1, x_2, \cdots, x_k]$ where k is a constant. Then testing if $C \in I$ can be done deterministically in time* $\mathrm{poly}(n, d)$.

Proof. We first write $C = T_1 + T_2 + \cdots + T_\ell$, where each $T_i = \prod_{j=1}^{d} P_{ij}$ such that each P_{ij} is the sum of at most c many univariate polynomials. The case $\ell = 1$ and the case when each T_i is only over indeterminates $x_1, \cdots, x_k$ can be directly handled using Hermann's algorithm (Theorem 11), in time $\mathrm{poly}(d^{2^k})$.

We describe the general case. Let $R = \mathbb{F}[x_1, x_2, \cdots, x_k]$. We can write $C = \beta_1 T_1' + \beta_2 T_2' + \cdots + \beta_m T_m'$ for some $m \leq \ell$, where $\beta_i \in R$ and $\beta_i \notin I$, and T_i' are nontrivial polynomials in $R[x_{k+1}, \cdots, x_n]$. We can easily determine $LT_R(T_i')$ for each T_i' from the polynomials P_{ij}, and rearrange the T_i' so that $LM_R(T_1') \geq LM_R(T_2') \geq \cdots \geq LM_R(T_m')$. Thus, $LM_R(T_1') \geq LM_R(C)$. The coefficient r of $LM_R(T_1')$ in C is also easily computable in polynomial time: we find the coefficient γ_i of $LM_R(T_1')$ in T_i' for $i = 1, 2, \cdots, m$. Note that $r = \sum_{i=1}^{m} \beta_i \gamma_i$. If $r \neq 0$ then notice that $r \notin I$ implies $C \notin I$. We check if $r \in I$ using Hermann's algorithm (Theorem 11) in time $\mathrm{poly}(d^{2^k})$. We need to continue the test if $r \in I$. That means either $LM_R(T_1') > LM_R(C)$ or $LM_R(T_1') = LM_R(C)$ and $r \in I$. By Lemma 7, $C \in I$ if and only if $\sum_{i=2}^{m} \beta_i T_i' \in \langle I, T_1' \rangle$.

Next, we group the factors P_{ij} occurring in T_1' according to the leading monomials. Let T_{1r} be the product of all factors P_{1j} of T_1' such that $LM(P_{1j})$ is a power of x_r, for $r = k+1, k+2, \cdots, x_n$. For an index r if there are no such factors P_{1j} then set $T_{1r} = 1$. Thus we have $T_1' = \prod_{r=k+1}^{n} T_{1r}$, where some of the factors T_{1r} are 1 and can be ignored. Clearly, for all $T_{1r} \neq 1$ and $T_{1s} \neq 1$ we have $LM(T_{1r}) > LM(T_{1s})$ if $r > s$.

Let $C_1 = \sum_{i=2}^{m} \beta_i T_i'$. For each r such that $T_{1r} \neq 1$, let I_{1r} denote the ideal $\langle I, T_{1r} \rangle$. The algorithm recursively checks if C_1 is in the ideal I_{1r} for each ideal I_{1r} and declares $C \in I$ if and only if $C_1 \in I_{1i}$

for each i. Notice that C_1 is a $\Sigma\Pi\Sigma\Pi(\ell-1,d,c)$ circuit and the generators of I_{1i}'s are now over $k+c$ indeterminates which is still a constant.

Claim. $C_1 = \sum_{i=2}^{m} \beta_i T_i' \in \langle I, T_1' \rangle$ if and only if $C_1 \in I_{1r}$ for each r such that $T_{1r} \neq 1$.

Proof of Claim: We first write T_1' as $T_1' = T_{1i_1} T_{1i_2} \cdots T_{1i_t}$, where all $T_{1i_j} \neq 1$. Letting $g_2 = T_{1i_1} T_{1i_2} \cdots T_{1i_{t-1}}$ and $g_1 = T_{1i_t}$ in Lemma 11, we get that $C_1 \in \langle I, T_1' \rangle = \langle I, g_2 g_1 \rangle$ if and only if $C_1 \in I_{1i_t}$ and $C_1 \in \langle I, T_{1i_1} T_{1i_2} \cdots T_{1i_{t-1}} \rangle$. A similar repeated application of Lemma 11 yields $C_1 \in \langle I, T_1' \rangle$ if and only if $C_1 \in \langle I, T_{1i_j} \rangle$ for each $j = 1, \cdots, t$. This completes the correctness proof of the algorithm.

We now show that the time bound is poly$(n, d^{max\{\ell, 2^k\}})$. Let $T(\ell,d,n)$ denote the time taken to test if $C \in I$. The algorithm description implies the following recurrence relation for T from which the running time bound is immediate.

$$T(\ell,d,n) \leq \begin{cases} dT(\ell,d,n) + \text{poly}(n, d^{2^k}) & \text{if } \ell > 1; \\ \text{poly}(n, d^{2^k}) & \text{if } \ell = 1. \end{cases}$$

■

References

[AB03] M. AGRAWAL AND S. BISWAS. Primality and identity testing via Chinese remaindering. *J. ACM.,* 50(4):429-443, 2003.

[AKS04] M. AGRAWAL, N. KAYAL AND N. SAXENA. Primes is in P. *Annals of Mathematics.,* 160(2):781-793, 2004.

[ALMSS92] S. ARORA, C. LUND, R. MOTWANI, M. SUDAN AND M. SZEGEDY. Proof verification and hardness of approximation problems. *In Proc. of the 33rd Annual IEEE Symposium on Foundations of Computer Science.,* pages 14-23, 1992.

[AS92] S. ARORA AND S. SAFRA. Probabilistic checking of proofs: A new characterization of NP. *In Proc. of the 33rd Annual IEEE FOCS.,* pages 2-13, 1992.

[COX92] D. COX, J. LITTLE AND D. O'SHEA. Ideals, Varieties and Algorithms. *Undergraduate Text in Mathematics.,* Springer, 1992.

[DS05] Z. DVIR AND A. SHPILKA. Locally Decodable Codes with 2 queries and Polynomial Identity Testing for depth 3 circuits. *In Proc. of the 37th annual ACM Sym. on Theory of computing.,* 2005.

[He26] G. HERMANN. Die Frage der endlich viel Schritte in der Theorie der Polynomideale. *Math. Annalen,* 95: 736-788, 1926.

[KI03] V. KABANETS AND R. IMPAGLIAZZO. Derandomization of polynomial identity tests means proving circuit lower bounds. *In Proc. of the thirty-fifth annual ACM Sym. on Theory of computing.,* pages 355-364, 2003.

[KS07] N. KAYAL AND N. SAXENA. Polynomial Identity Testing for Depth 3 Circuits. *Computational Complexity.,* 16(2):115-138, 2007.

[LFKN92] C. LUND, L. FORTNOW, H. KARLOFF AND N. NISAN. Algebraic methods for interactive proof systems. *Journal of the ACM.,* 39(4):859-868, 1992.

[Lov79] L. LOVASZ. On determinants, matchings, and random algorithms. *In Fundamentals of Computation Theory : Proc. of the Conference on Algebraic, Arithmetic, and Categorical Methods in Computation Theory,* Vol.2, pages 565-574. Akademic-Verlag, 1979.

[Mayr89] E. MAYR. Membership in polynomial ideals over $\mathbb{Q}$ is exponential space complete. *In Proc. of STACS.,* 1989.

[MM82] E. MAYR AND A. MEYER. The complexity of word problem for commutative semigroups and polynomial ideals. *Adv. Math.,* 46, 305-329, 1982.

[MR01] R. MOTWANI AND P. RAGHAVAN. Randomized Algorithm. Cambridge, 2001.

[MVV87] K. MULMULEY, U. VAZIRANI AND V. VAZIRANI. Matching is as easy as matrix inversion. *In Proc. of the nineteenth annual ACM conference on Theory of Computing.,* pages 345-354. ACM Press, 1987.

[OT88] M. BEN-OR AND P. TIWARI. A Deterministic Algorithm For Sparse Multivariate Polynomial Interpolation. *In Proc. of the 20th annual ACM Sym. on Theory of computing.,* pages 301-309, 1988.

[Sch80] JACOB T. SCHWARTZ. Fast Probabilistic algorithm for verification of polynomial identities. *J. ACM.,* 27(4), pages 701-717, 1980.

[Sha92] A. SHAMIR. IP=PSPACE. *J. ACM.,* 39(4), pages 869-877, 1992.

[Su98] MADHU SUDAN. Lectures on Algebra and Computation (6.966), Lecture 12,13,14, 1998.

[TZ06] T. TAO AND T. ZEIGLER. The primes contain arbitrarily long polynomial progressions. *To appear in Acta Mathematica.* In arxiv:math/0305172v2, June 2006.

[Zip79] R. ZIPPEL. Probabilistic algorithms for sparse polynomials. *In Proc. of the Int. Sym. on Symbolic and Algebraic Computation.,* pages 216-226, 1979.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de/