Theory of Computing Systems
https://doi.org/10.1007/s00224-021-10053-w

Univariate Ideal Membership Parameterized by Rank, Degree, and Number of Generators

V. Arvind[1] · Abhranil Chatterjee[1] · Rajit Datta[2] · Partha Mukhopadhyay[2]

Accepted: 28 June 2021Published online: 15 July 2021

Abstract

Let $\mathbb{F}[X]$ be the polynomial ring in the variables $X = \{x_1, x_2, \ldots, x_n\}$ over a field $\mathbb{F}$. An ideal $I = \langle p_1(x_1), \ldots, p_n(x_n)\rangle$ generated by univariate polynomials $\{p_i(x_i)\}_{i=1}^n$ is a *univariate ideal*. Motivated by Alon's Combinatorial Nullstellensatz we study the complexity of *univariate ideal membership*: Given $f \in \mathbb{F}[X]$ by a circuit and polynomials p_i the problem is test if $f \in I$. We obtain the following results.

- Suppose f is a degree-d, rank-r polynomial given by an arithmetic circuit where $\ell_i : 1 \leq i \leq r$ are linear forms in X. We give a deterministic time $d^{O(r)} \cdot \mathrm{poly}(n)$ division algorithm for evaluating the (unique) remainder polynomial $f(X) \bmod I$ at any point $\vec{a} \in \mathbb{F}^n$. This yields a randomized $n^{O(r)}$ algorithm for minimum vertex cover in graphs with rank-r adjacency matrices. It also yields a new $n^{O(r)}$ algorithm for evaluating the permanent of a $n \times n$ matrix of rank r, over any field $\mathbb{F}$.
- Let f be over rationals with $\deg(f) = k$ treated as fixed parameter. When the ideal $I = \left\langle x_1^{e_1}, \ldots, x_n^{e_n}\right\rangle$, we can test ideal membership in randomized $O^*((2e)^k)$. On the other hand, if each p_i has all distinct rational roots we can check if $f \in I$ in randomized $O^*(n^{k/2})$ time, improving on the brute-force $\binom{n+k}{k}$-time search.
- If $I = \langle p_1(x_1), \ldots, p_k(x_k)\rangle$, with k as fixed parameter, then ideal membership testing is W[2]-hard. The problem is MINI[1]-hard in the special case when $I = \left\langle x_1^{e_1}, \ldots, x_k^{e_k}\right\rangle$.

Keywords Ideal membership · Algorithms · Parameterized complexity · Combinatorial Nullstellensatz

An earlier version of this paper was presented at the FSTTCS conference [6].

✉ V. Arvind
arvind@imsc.res.in

Extended author information available on the last page of the article.

1 Introduction

Let $X = \{x_1, x_2, \dots, x_n\}$ be a set of n commuting variables and $\mathbb{F}$ be a field which is either the field $\mathbb{Q}$ of rationals or a finite field throughout this paper. Let $R = \mathbb{F}[X]$ be the ring of multivariate polynomials over the variables in X with coefficients from the field $\mathbb{F}$. A subring $I \subseteq R$ is an *ideal* if I absorbs multiplications by elements of R. That is, $I \cdot R \subseteq I$.

Computationally, an ideal $I \subset R$ is given by a set of generator polynomials : $I = \langle f_1, f_2, \dots, f_\ell \rangle$. In other words, I is the smallest ideal containing the polynomials $f_i, 1 \le i \le \ell$. Given $f \in R$ and $I = \langle f_1, \dots, f_\ell \rangle$, the *Ideal Membership problem* is to decide whether $f \in I$ or not. In general, the problem is notoriously intractable. It is EXPSPACE-complete even if f and the generators $f_i, i \in [\ell]$ are given explicitly as sums of monomials [26]. Nevertheless, special cases of ideal membership problem have played important roles in several results in arithmetic complexity. For example, the polynomial identity testing algorithm for depth three $\Sigma\Pi\Sigma$ circuits with bounded top fan-in; the structure theorem for $\Sigma\Pi\Sigma(k, d)$ identities use ideal membership very crucially [8, 18, 29].

In this paper, our study of ideal membership is motivated by Alon's Combinatorial Nullstellensatz [1], and we recall one of its formulations.

Theorem 1.1 [1] *Let $\mathbb{F}$ be any field, and $f(X) \in \mathbb{F}[X]$. Define polynomials $g_i(x_i) = \prod_{s \in S_i}(x_i - s)$ for non-empty subsets S_i, $1 \le i \le n$ of $\mathbb{F}$. If f vanishes on all the common zeros of $g_1, \dots, g_n$, then there are polynomials $h_1, \dots, h_n$ satisfying $\deg(h_i) \le \deg(f) - \deg(g_i)$ such that $f = \sum_{i=1}^{n} h_i g_i$.*

It can be restated in terms of ideal membership: Let $f(X) \in \mathbb{F}[X]$ be a given polynomial, and $I = \langle g_1(x_1), g_2(x_2), \dots, g_n(x_n) \rangle$ be an ideal generated by univariate polynomials g_i *without repeated roots*. Let $Z(g_i)$ denote the zero set of g_i, $1 \le i \le n$. By Theorem 1.1, if $f \notin I$ then there is a $\vec{\alpha} = (\alpha_1, \dots, \alpha_n) \in Z(g_1) \times \cdots \times Z(g_n)$ such that $f(\vec{\alpha}) \neq 0$. Of course, if $f \in I$ then $f|_{Z(g_1)\times\cdots\times Z(g_n)} = 0$.

Ideals I generated by univariate polynomials are called *univariate ideals*. For any univariate ideal I and any polynomial f, by repeated application of the division algorithm, we can write $f(X) = \sum_{i=1}^{n} h_i(X) g_i(x_i) + R(X)$ where R is unique and for each $i \in [n] : \deg_{x_i}(R) < \deg(g_i(x_i))$. Since the remainder is unique, it is convenient to write $R = f \mod I$. By Alon's theorem, if $f \notin I$ then there is a $\vec{\alpha} \in Z(g_1) \times \cdots \times Z(g_n)$ such that $R(\vec{\alpha}) \neq 0$.

Univariate ideal membership is further motivated by its connection with two well-studied problems. Computing the permanent of a $n \times n$ matrix over any field $\mathbb{F}$ can be cast in terms of univariate ideal membership. Given a matrix $A = (a_{i,j})_{1 \le i,j \le n} \in \mathbb{F}^{n \times n}$, consider the product of linear forms $P_A(X) = \prod_{i=1}^{n} \left(\sum_{j=1}^{n} a_{ij} x_j \right)$. The following observation is well known.

Fact 1.2 *The permanent of the matrix A is given by the coefficient of the monomial $x_1 x_2 \cdots x_n$ in P_A. In other words, the remainder of the polynomial*

$P_A(x_1, x_2, \ldots, x_n)$ modulo the univariate ideal $\langle x_1^2, \ldots, x_n^2 \rangle$ is precisely $Perm(A) \cdot x_1x_2 \cdots x_n$.

It follows immediately that the remainder $P_A \bmod \langle x_1^2, \ldots, x_n^2 \rangle$ evaluates to $\text{Perm}(A)$ at the point $\vec{1} \in \mathbb{F}^n$.

Next, we briefly mention the connection of univariate ideal membership with the multilinear monomial detection problem, a benchmark problem that is useful in designing fast parameterized algorithms for a host of problems [21–23, 33].

Notice that, given an arithmetic circuit C computing a polynomial $f \in \mathbb{F}[X]$ of degree k, checking if f has a non-zero multilinear monomial of degree k is equivalent to checking if $f \bmod \langle x_1^2, \ldots, x_n^2 \rangle$ is non-zero. Moreover, the constrained multilinear detection problem studied in [10, 22] can also be viewed as a problem of deciding membership in a univariate ideal.

However, even for univariate ideals, the ideal membership problem is hard in general. As an application of Theorem 1.1, Alon and Tarsi [1, 2] show that checking k-colorability of a graph G is polynomial-time equivalent to checking if the corresponding graph polynomial $f_G = \prod_{ij \in E, i<j}(x_i - x_j)$ is in the ideal $\langle x_1^k - 1, \ldots, x_n^k - 1 \rangle$. Hence, univariate ideal membership is coNP-hard when the polynomials have distinct roots. We show that Univariate Ideal Membership over $\mathbb{Q}$, in general, is in the third level of the counting hierarchy. For the lower bound, we note that checking if a product of n linear forms is in the ideal $\langle x_1^2, x_2^2, \ldots, x_n^2 \rangle$ is as hard as checking if the integer permanent is zero, which is $\text{C}_=\text{P}$-hard. Univariate Ideal Membership over finite fields of characteristic k is quite tightly classified: the upper bound of $\text{coR} \cdot \text{Mod}_\text{k}\text{P}$ nearly matches with the $\text{Mod}_\text{k}\text{P}$ hardness.

1.1 Our Results

In this paper, we study univariate ideal membership problem for different parameters of the input polynomial f and the univariate ideal I. The first parameter we consider is the rank of f. This notion has found applications, for example, in algorithms for depth-3 polynomial identity testing [29].

Definition 1.3 We say $f \in \mathbb{F}[X]$ is a *rank r* polynomial if $f \in \mathbb{F}[\ell_1, \ell_2, \ldots, \ell_r]$ for linear forms $\ell_j : 1 \leq j \leq r$.

We give two different algorithms for checking if a rank-r polynomial f is in a univariate ideal I. The first one is essentially an iterative division procedure. It evaluates the remainder polynomial $f \bmod I$ at a given point $\vec{\alpha} \in \mathbb{F}^n$ in deterministic time $O^*(d^{O(r)})$. Using this evaluation procedure, we can test if the remainder polynomial $f \bmod I$ is nonzero by evaluating it at a randomly chosen point $\vec{\alpha}$ over $\mathbb{F}$ or a suitable extension field. The second algorithm is structural. It expresses the remainder polynomial $f \bmod I$ as an $O^*(d^{O(r)})$ sum of d-products of linear forms. By the Polynomial Identity Lemma [14, 31, 34], we can check if it is nonzero by evaluation at a randomly chosen point $\vec{\alpha}$. We formally state the theorem.

Theorem 1.4 *Let C be a polynomial-size arithmetic circuit computing a polynomial f in $\mathbb{F}[\ell_1, \ell_2, \ldots, \ell_r]$, where $\ell_1, \ell_2, \ldots, \ell_r$ are given linear forms in $\{x_1, x_2, \ldots, x_n\}$. Let $I = \langle p_1, \ldots, p_n \rangle$ be a univariate ideal generated by $p_i(x_i) \in \mathbb{F}[x_i]$, $1 \le i \le n$.*

1. *Given $\vec{\alpha} \in \mathbb{F}^n$, we can evaluate the remainder $f \bmod I$ at the point $\vec{\alpha}$ in deterministic time $d^{O(r)}\mathrm{poly}(n)$, where $d = \max\{\deg(f), \deg(p_i) : 1 \le i \le n\}$.*
2. *In deterministic time $d^{O(r)}\mathrm{poly}(n)$ we can express the remainder $f \bmod I$ as an $O^*(d^{O(r)})$-sum of d-products of linear forms.*

Using either of these algorithms, we can decide in randomized $O^*(d^{O(r)})$ time if f is in I.

We can check if $f \in I$ by evaluating the remainder $f \bmod I$ at a randomly chosen point $\vec{\alpha}$, which can be done using any of the above algorithms.

We apply the previous result to obtain an efficient algorithm for minimum vertex cover in low rank graphs. A graph G is said to be of rank r if the rank of the adjacency matrix A_G is of rank r. Graphs of low rank were studied by Lovasz and Kotlov [4, 20] in the context of graph coloring.

Theorem 1.5 *Given a graph $G = (V, E)$ on n vertices such that the rank of the adjacency matrix A_G is at most r, and a parameter k, there is a randomized $n^{O(r)}$ algorithm to decide if the graph G has vertex cover of size k or not.*

Theorem 1.4 also yields an $n^{O(r)}$ algorithm to compute the permanent of rank-r matrices over any field. Barvinok had given [9] an algorithm of same running time for the permanent of low rank matrices (over $\mathbb{Q}$) using apolar bilinear forms. By Fact 1.2, if matrix A is rank r then P_A is a rank-r polynomial, and for the univariate ideal $I = \langle x_1^2, \ldots, x_n^2 \rangle$ computing $P_A \bmod I$ at the point $\vec{1}$ yields the permanent. Theorem 1.4 works more generally for all univariate ideals. In particular, the ideal in the proof of Theorem 1.5 is generated by polynomials that are not powers of variables. Thus, Theorem 1.4 can potentially have more algorithmic consequences than the technique in [9].

If k is the degree of the input polynomial and the ideal is given by the powers of variables as generators, we have a randomized FPT algorithm for the problem.

Theorem 1.6 *Given an arithmetic circuit C computing a polynomial $f(X) \in \mathbb{Q}[X]$ of degree k and integers $e_1, e_2, \ldots, e_n$, there is a randomized algorithm to decide whether $f \in \langle x_1^{e_1}, x_2^{e_2}, \ldots, x_n^{e_n} \rangle$ in $O^*((2e)^k)$ time.*

The above result generalizes the algorithm for multilinear monomial detection [23] (there the ideal of interest is $I = \langle x_1^2, x_2^2, \ldots, x_n^2 \rangle$). Brand et al. have given the first FPT algorithm for degree-k multilinear monomial detection in arithmetic circuits [11]. Multilinear monomial detection can also be done, with the same running time, using the Hadamard product [5] of the given polynomial with the elementary symmetric polynomial (and in a different approach using apolar bilinear forms [27]).

When the number of generators in the univariate ideal is treated as fixed parameter, ideal membership is W[2]-hard.

Theorem 1.7 *Given a polynomial $f(X) \in \mathbb{F}[X]$ by an arithmetic circuit C and univariate polynomials $p_1(x_1), p_2(x_2), \ldots, p_k(x_k)$, checking if $f \notin \langle p_1(x_1), p_2(x_2), \ldots, p_k(x_k)\rangle$ is* W[2]*-hard with k as the parameter.*

Theorem 1.7 is shown by an efficient reduction from parameterized the dominating set problem to ideal membership parameterized by number of generators. To find an dominating set of size k, the reduction produces an ideal with k univariates and the polynomial created from the graph has k variables.

Unlike Theorem 1.6, even checking if f is in the ideal $\langle {x_1}^{e_1}, {x_2}^{e_2}, \ldots, {x_k}^{e_k}\rangle$ remains intractable in the parameterized sense.

Theorem 1.8 *Let C be a polynomial-size arithmetic circuit computing a polynomial $f \in \mathbb{F}[X]$. Let $I = \langle {x_1}^{e_1}, {x_2}^{e_2}, \ldots, {x_k}^{e_k}\rangle$ be the given ideal where $e_1, \ldots, e_k$ are given in unary, checking if $f \notin I$ is* MINI[1]*-hard with k as parameter.*

The k−LIN-EQ problem, which asks if there is a $\vec{x} \in \{0, 1\}^n$ satisfying $A\vec{x} = \vec{b}$, where $A \in \mathbb{F}^{k\times n}$ and $\vec{b} \in \mathbb{F}^k$, is reducible to the complement of univariate ideal membership for an ideal of the form $I = \langle {x_1}^{e_1}, {x_2}^{e_2}, \ldots, {x_k}^{e_k}\rangle$. We then show k−LIN-EQ is hard for the parameterized complexity class MINI[1] by reducing the miniature version of 1 − in − 3POSITIVE3 − SAT to it.

As already mentioned, the result of Alon and Tarsi [1, 2] shows that the membership of f_G in $\left\langle x_1^k - 1, \ldots, x_n^k - 1\right\rangle$ is coNP-hard and the proof crucially uses the fact that the roots of the generator polynomials are all distinct. This naturally raises the question if univariate ideal membership is in coNP when each generator polynomial has distinct roots. We show univariate ideal membership is in coNP over rationals when all the generator polynomials have distinct roots. We show that over $\mathbb{Q}$ univariate ideal membership, in general, is in the third level of the counting hierarchy. This upper bound is reasonably tight, as checking if a product of n linear forms is in the ideal $\left\langle x_1^2, x_2^2, \ldots, x_n^2\right\rangle$ is as hard as checking if the integer permanent is zero, which is $\mathrm{C}_{=}\mathrm{P}$-hard.

Theorem 1.9 *Let $f \in \mathbb{Q}[X]$ be a polynomial of degree at most d given by a black-box. Let $I = \langle p_1(x_1), \ldots, p_n(x_n)\rangle$ be an ideal given explicitly by a set of univariate polynomials $p_1, p_2, \ldots, p_n$ as generators of maximum degree bounded by d. Let L be the bit-size upper bound for any coefficient in $f, p_1, p_2, \ldots, p_n$. Moreover, assume that p_is have distinct roots over $\mathbb{C}$. Then there is a non-deterministic algorithm running in time* $\mathrm{poly}(n, d, L)$ *that decides the non-membership of f in the ideal I.*

Remark 1.10 The distinct roots case discussed in Theorem 1.9 is in stark contrast to the complexity of testing membership of $P_A(X)$ in the ideal $\left\langle x_1^2, \ldots, x_n^2\right\rangle$. That problem is equivalent to checking if $\mathrm{Perm}(A)$ is nonzero for a rational matrix A, which is hard for the exact counting class $\mathrm{C}_{=}\mathrm{P}$. Hence it cannot be in coNP unless the polynomial-time hierarchy collapses. We do not have an analogue of Theorem 1.9 over finite fields.

Recall from Alon's Nullstellensatz that if $f \notin I$, then there is always a point $\vec{\alpha} \in Z(p_1) \times \ldots \times Z(p_n)$ such that $f(\vec{\alpha}) \neq 0$. Notice that in general the roots $\alpha_i \in \mathbb{C}$ and in the standard *Turing Machine* model the NP machine can not guess the roots directly with only finite precision. But we are able to prove that the NP machine can guess a corresponding tuple of *root approximations* $\vec{\tilde{\alpha}} \in \mathbb{Q}^n$, using only polynomial bits of precision and still can decide the non-membership. The main technical idea is to compute efficiently a parameter M (only from the input parameters) such that

$$\begin{aligned} |f(\vec{\tilde{\alpha}})| &\leq M \text{ if } f \in I, \text{ and} \\ |f(\vec{\tilde{\alpha}})| &\geq 2M \text{ if } f \notin I. \end{aligned}$$

The NP machine decides the non-membership according to the final value of $|f(\vec{\tilde{\alpha}})|$.

In this connection, we note that Koiran has considered the weak version of Hilbert Nullstellensatz (HN) problem [19]. The input is a set of multivariate polynomials $f_1, f_2, \ldots, f_m \in \mathbb{Z}[X]$ and the problem is to decide whether $1 \in \langle f_1, \ldots, f_m \rangle$. The result of Koiran shows that $\overline{\text{HN}} \in \text{AM}$ (under GRH), and it is an outstanding open problem problem to decide whether $\overline{\text{HN}} \in \text{NP}$.

Organization In Section 2 we present some background material. In Section 3 we show that, in general, univariate ideal membership is in the counting hierarchy. We prove Theorems 1.4 and 1.5 in Section 4. In Section 5, we explore the parameterized complexity of univariate ideal membership. In the first subsection, we prove Theorem 1.6, and in the second subsection we prove Theorems 1.7 and 1.8. Finally, in Section 7, we prove Theorem 1.9.

2 Preliminaries

We recall some basic definitions and results that are background material.

2.1 Basics of Ideal Membership

Let $\mathbb{F}[X]$ be the ring of polynomials $\mathbb{F}[x_1, x_2, \ldots, x_n]$. Let $I \subseteq \mathbb{F}[X]$ be an ideal given by a set of generators $I = \langle g_1, \ldots, g_\ell \rangle$. Then for any polynomial $f \in \mathbb{F}[X]$, it is a member of the ideal if and only if $f = \sum_{i=1}^{\ell} h_i g_i$ where $\forall i : h_i \in \mathbb{F}[X]$. Dividing f by the g_i by applying the standard division algorithm does not work in general to check if $f \in I$. Indeed, the remainder is not even uniquely defined. However, if the leading monomials of the generators are already pairwise relatively prime, then we can apply the division algorithm to compute the unique remainder.

Theorem 2.1 (See [12], Theorem 3, proposition 4, pp.101) *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.*

In particular, if the ideal I is a univariate ideal given by $I = \langle p_1(x_1), \dots, p_n(x_n)\rangle$, we can apply the division algorithm to compute the unique remainder $f \bmod I$. To bound the run time of this procedure we note the following: Let $\bar{p}$ denote the ordered list $\{p_1, p_2, \dots, p_n\}$. Let Divide$(f; \bar{p})$ be the procedure that divides f by p_1 to obtain remainder f_1, then divides f_1 by p_2 to obtain remainder f_2, and so on to obtain the final remainder f_n after dividing by p_n. We note the following time bound for Divide$(f; \bar{p})$.

Fact 2.2 (See [32], Section 6, pp.5-12) *Let $f \in \mathbb{F}[X]$ be given by a size s arithmetic circuit and $p_i(x_i) \in \mathbb{F}[x_i]$ be given univariate polynomials. The running time of Divide$(f; \bar{p})$ is bounded by $O(s \cdot \prod_{i=1}^{n}(d_i + 1)^{O(1)})$, where $d_i =$* $\max\{\deg_{x_i}(f), \deg(p_i(x_i))\}$.

2.2 Some Bounds Concerning Roots of Univariate Polynomials

The following folklore lemma gives a bound on the absolute value of any root of a univariate polynomial in terms of the degree and the coefficients.

Lemma 2.3 *For any root α of a univariate degree-d polynomial $f(x) = \sum_{i=0}^{d} a_i x^i \in \mathbb{Q}[x]$ one of the following bounds hold:*

$$\frac{|a_0|}{\sum_{i=1}^{d} |a_i|} \leq |\alpha| < 1 \text{ or } 1 \leq |\alpha| \leq d \cdot \frac{\max_i |a_i|}{|a_d|}.$$

Proof Since α is a root of f, we have $0 = f(\alpha) = \sum_{i=0}^{d} a_i\alpha^i = 0$. Hence, $\sum_{i=1}^{d} a_i\alpha^i = -a_0$. By triangle inequality

$$\sum_{i=1}^{d} |a_i||\alpha|^i \geq |a_0|.$$

Since f is degree d, $a_d \neq 0$. We consider two cases. First, suppose $|\alpha| < 1$. Then, by the above inequality, $|\alpha| \cdot (\sum_{i=1}^{d} |a_i|) \geq |a_0|$. Hence, $|\alpha| \geq \frac{|a_0|}{\sum_{i=1}^{d} |a_i|}$. Next, suppose $|\alpha| \geq 1$. Since $-a_d\alpha^d = \sum_{i=0}^{d-1} a_i\alpha^i$, by triangle inequality $|a_d||\alpha|^d \leq |\alpha|^{d-1} \cdot (\sum_{i=0}^{d-1} |a_i|)$. Hence, $|\alpha| \leq \frac{\sum_{i=0}^{d-1} |a_i|}{|a_d|} \leq d \cdot \frac{\max_i |a_i|}{|a_d|}$. This completes the proof. □

The next lemma, due to Mahler [25], lower bounds the distance between any two distinct roots of a univariate polynomial in terms of its degree and the size of its coefficients.

Lemma 2.4 (Mahler [25]) *Let $g(x) = \sum_{i=0}^{d} a_i x^i \in \mathbb{Q}[x]$ and $2^{-L} \leq |a_i| \leq 2^L$ (if $a_i \neq 0$). Let α, β are two distinct roots of g. Then $|\alpha - \beta| \geq \frac{1}{2^{O(dL)}}$.*

Given a univariate polynomial f and a point β that is far from the roots of f, the following lemma lower bounds $|f(\beta)|$. The following lemma states that any univariate polynomial can not get a very small value (in absolute sense) on any point which is far from every root.

Lemma 2.5 *Let $f = \sum_{i=1}^{d} a_i x^i$ be a univariate degree-d polynomial with $2^{-L} \leq |a_i| \leq 2^L$ (if $a_i \neq 0$). Let $\tilde{\alpha}$ be a point such that $|\tilde{\alpha} - \beta_i| \geq \delta$ for every root β_i of f. Then*

$$|f(\tilde{\alpha})| \geq 2^{-L}\delta^d.$$

Proof Since $\deg(f) = d$, $a_d \neq 0$. We can write $f(\tilde{\alpha}) = a_d \prod_{i=1}^{d}(\tilde{\alpha} - \beta_i)$. Since $|\tilde{\alpha} - \beta_i| \geq \delta$, $|f(\tilde{\alpha})| = |a_d| \prod_{i=1}^{d} |\tilde{\alpha} - \beta_i| \geq 2^{-L}\delta^d$. □

2.3 Parameterized Complexity Classes

We recall some standard definitions from parameterized complexity [13, ch.1,pp. 7-14]. For a parameterized problem the input instances are pairs (x, k), where x is the actual input and k is a fixed parameter. The parameterized problem is in the class FPT (for fixed parameter tractable) if the problem has an algorithm with run time $f(k)|(x, k)|^{O(1)}$ for some computable function f.

A parameterized reduction [13, def. 13.1] between two parameterized decision problems P_1 and P_2 is a many-one reduction such that on input instance (x, k) of P_1 the reduction maps it to an instance (x', k') of P_2 in time $f(k)|(x, k)|^{O(1)}$, for some computable f, such that (x, k) is a "yes" instance of P_1 if and only if (x', k') is a "yes" instance of P_2, and $k' \leq f(k)$.

A parameterized problem is said to be in the class XP if it has an algorithm with run time $|x|^{f(k)}$ for some computable function f.

For the purpose of this paper, it suffices to note that a parameterized problem L is in the class W[1] if there is a parameterized reduction from L to some standard W[1]-complete problem like, e.g., the k-Independent set problem and L is in the class W[2] if there is a parameterized reduction from L to some standard W[2]-complete problem like, e.g., the k-dominating set problem (more details can be found in, e.g, [13, def. 13.16]).

The complexity class MINI[1] consists of parameterized problems that are miniature versions of NP problems: For $L \in$ NP, its miniature version mini(L) has instances of the form $(0^n, x)$, where $|x| \leq k \log n$, k is the fixed parameter, and x is an instance of L. Showing mini(L) to be MINI[1]-hard under parameterized reductions is evidence of its parameterized intractability, for it cannot be in FPT assuming the Exponential Time Hypothesis [15].

2.4 Multivariate Polynomials

We recall the definition of Hadamard product of two polynomials.

Definition 2.6 Given two polynomials $f, g \in \mathbb{F}[X]$, their Hadamard product is defined as

$$f \circ g = \sum_{m} [m]f \cdot [m]g \cdot m.$$

We will use a scaled variant of the Hadamard Product [7].

Definition 2.7 [7] Given two polynomials $f, g \in \mathbb{F}[X]$, their *scaled Hadamard Product* $f \circ^s g$, is defined as

$$f \circ^s g = \sum mm! \cdot [m]f \cdot [m]g \cdot m,$$

where $m = x_{i_1}^{e_1} x_{i_2}^{e_2} \ldots x_{i_r}^{e_r}$ and $m! = e_1! \cdot e_2! \cdots e_r!$ abusing the notation.

Remark 2.8 If either f or g is multilinear, notice that their scaled Hadamard product coincides with their Hadamard product.

The *elementary symmetric polynomial* of degree k over n variables $\{x_1, x_2, \ldots, x_n\}$ is defined as:

$$S_{n,k}(x_1, x_2, \ldots, x_n) = \sum_{T \subseteq [n], |T|=k} \prod_{i \in T} x_i.$$

Notice that, $S_{n,k}$ contains all the degree k multilinear terms.

3 A Complexity-Theoretic Upper Bound

We show that over $\mathbb{Q}$ univariate ideal membership is in the counting hierarchy. Over finite fields of characteristic k, the problem is in the randomized complexity class $\text{coR} \cdot \text{Mod}_k\text{P}$.

Let Σ be a finite alphabet (of size at least 2). The class #P consists of functions $h : \Sigma^* \to \mathbb{N}$ defined by an NP machine M such that for all $x \in \Sigma^*$

$$h(x) = acc_M(x),$$

where $acc_M(x)$ is the number of accepting paths of M on input x. A language $L \subseteq \Sigma^*$ is in the counting complexity class $\text{C}_{=\text{P}}$ if there is an NP machine M such that for all $x \in \Sigma^*$ $x \in L$ if and only if $acc_M(x) = rej_M(x)$. For $A \subseteq \Sigma^*$ the relativized class $\text{C}^A_{=\text{P}}$ is defined as above for an NP^A (oracle) machine M. For $i \geq 2$, a language L is in the i^{th} level of the exact counting hierarchy, denoted CH_i, if $L \in \text{C}_=\text{P}^A$ for some $A \in \text{CH}_{i-1}$.

Theorem 3.1

1. *Univariate ideal membership over $\mathbb{Q}$ is in the third level of the counting hierarchy.*
2. *Univariate ideal membership over a finite field of characteristic k is in* $\text{coR} \cdot \text{Mod}_\text{k}\text{P}$.

Proof For the first part, let $f \in \mathbb{Q}[X]$ be given as input by a degree d arithmetic circuit and $p_i(x_i) \in \mathbb{Q}[x_i], i \in [n]$ be the generators of the ideal I. By clearing denominators, we can assume that both f and the p_i have integer coefficients. Writing f as an integer linear combination of monomials we have

$$f = \sum_{m:\deg(m)\leq d} \alpha_m m,$$

where $\alpha_m \in \mathbb{Z}$ is the integer coefficient of monomial m (note that each α_m is polynomial size in binary). As the generators p_i are univariate we can express the remainder polynomial

$$f \bmod I = \sum_{m:\deg(m)\leq d} \alpha_m (m \bmod I).$$

In particular, let $m = x_1^{e_1} \cdot x_2^{e_2} \cdots x_n^{e_n}$ and $r_{m,i}(x_i) = x_i^{e_i} \mathrm{mod} p_i(x_i)$. Then, we have $m \bmod I = \prod_{i=1}^n r_{m,i}(x_i)$, where $\deg(r_{m,i}) < \deg(p_i)$ for each i. Thus, the remainder polynomial

$$f \bmod I = \sum_{m:\deg(m)\leq d} \alpha_m \prod_{i=1}^{n} r_{m,i}(x_i).$$

In order to check if $f \bmod I$ is nonzero, noting that the degree of the remainder also is bounded by d, by Alon's Nullstellensatz it suffices to check if there is a point $\vec{a} = (a_1, a_2, \ldots, a_n)$ in the n-dimensional grid $[d+1]^n$ where $f \bmod I$ does not vanish.

We will be using the simple fact that we can compute in $\mathrm{P}^{\#\mathrm{P}}$ the coefficient of any monomial of degree at most d in f.

Let $L = \{(f, \{p_i\}_{i\in[n]}, \vec{a}) \mid f \in \mathbb{Z}[X], p_i(x_i) \in \mathbb{Z}[X], \vec{a} \in [d+1]^n\ f \bmod I(\vec{a}) \neq 0\}$. Checking if $f \notin I$ is clearly in NP^L: we guess the point $\vec{a}$ and verify that $(f, I, \vec{a}) \in L$ by querying the oracle. We now show that $\overline{L}$ is in CH_2 and that completes the proof of the first part. To do so, we define an oracle NP machine M as follows:

- M guesses the monomials of degree at most d along its computation paths (each path corresponds to a unique monomial).
- On the computational path that guesses monomial m, M uses a #P oracle to compute its (integer) coefficient α_m in the polynomial f.
- Compute the remainder polynomial $m \bmod I = \prod_{i=1}^n r_{m,i}(x_i)$. This computation path contributes $\alpha_m \prod_{i=1}^n r_{m,i}(x_i)$ to the overall remainder.
- Compute $val(m) = \alpha_m \prod_{i=1}^n r_{m,i}(a_i)$. If $val(m)$ is negative then M produces $|val(m)|$ many rejecting paths. Otherwise, M produces $|val(m)|$ many accepting paths.

Notice that the overall remainder is $f \bmod I = \sum_m \alpha_m \prod_{i=1}^n r_{m,i}(x_i)$. Clearly, $f \bmod I(\vec{a}) = 0$ if and only if the number of accepting paths equals the number of rejecting paths. Hence, $\overline{L} \in \mathrm{C_{=}P}^{\#\mathrm{P}}$. Since $\mathrm{P}^{\#\mathrm{P}} \subseteq \mathrm{coNP}^{\mathrm{C_{=}P}}$, it follows that $\overline{L} \in \mathrm{CH}_2$.

For the second part, the proof is along the same lines using the additional facts that $\mathrm{Mod}_k\mathrm{P}^{\mathrm{Mod}_k\mathrm{P}} = \mathrm{Mod}_k\mathrm{P}$ for prime k, and $\mathrm{NP} \subseteq \mathrm{coR} \cdot \mathrm{Mod}_k\mathrm{P}$ by the Valiant-Vazirani lemma. □

Remark 3.2 It is interesting to note that we have the lower bound (of $\mathrm{C_{=}P}$ for $\mathbb{F} = \mathbb{Q}$ and $\mathrm{Mod}_k\mathrm{P}$ for $\mathrm{char}(\mathbb{F}) = k, k > 2$) for the simple case of checking if a product of linear forms is in the ideal $\langle x_1^2, x_2^2, \ldots, x_n^2 \rangle$, by virtue of the hardness of checking if the permanent is zero (over $\mathbb{Q}$ and $\mathrm{char}(\mathbb{F}) \neq 2$). We now observe a hardness result over $\mathrm{char}(\mathbb{F}) = 2$ for the same ideal. Consider a graph $G = (V, E)$. For each vertex $v \in V$ define the monomial $star(v) = y_v \prod_{v \in e} x_e$, where x_e and y_v are edge and vertex variables. Now, we define the polynomial

$$P = \prod_{u=1}^{n} (1 + t \cdot star(u)),$$

where t is a new variable. Writing $P = \sum_{d=0}^{n} P_d \cdot t^d$, consider the polynomial $P_{n/2}$ (for which we can find a small circuit from P). Then $P_{n/2} \mathrm{mod} \langle \{x_e^2 \mid e \in E\} \rangle$ is nonzero if and only if G has an independent set of size $n/2$. This holds over all fields $\mathbb{F}$ including $\mathbb{F}_2$.

4 Ideal Membership for Low Rank Polynomials

We first recall the notion *rank* of a polynomial in $\mathbb{F}[X]$.

Definition 4.1 A polynomial $f(X) \in \mathbb{F}[X]$ is a *rank-r* polynomial if there are linear forms $\ell_1, \ell_2, \ldots, \ell_r$ in the variables X and an r-variate polynomial $g(z_1, z_2, \ldots, z_r) \in \mathbb{F}[z_1, z_2 \ldots, z_r]$ such that

$$f(X) = g(\ell_1, \ell_2, \ldots, \ell_r).$$

For an (unspecified) fixed parameter r, we refer to rank-r polynomials as *low rank polynomials.*

In this section we prove Theorem 1.4: Let $f(X)\mathbb{F}[X]$ be a rank-r degree d polynomial given by an r-variate arithmetic circuit C and linear forms $\ell_i, i \in [r]$ such that $f = C(\ell_1, \ell_2, \ldots, \ell_r)$, along with a univariate ideal I, and a point $\vec{\alpha} \in \mathbb{F}^n$ as inputs. We give a deterministic $O^*(d^{O(r)})$ time algorithm to evaluate the remainder polynomial $f \bmod I$ at $\vec{\alpha}$ where d is the degree of the polynomial f. As corollary, this yields an $O^*(d^{O(r)})$-time randomized algorithm for testing if f is in the ideal I.

Remark 4.2 Kayal [17] has shown a *randomized* polynomial-time algorithm for testing if a given polynomial $f(X) \in \mathbb{F}[X]$ is of a given rank r and, if so, to compute the linear forms $\ell_1, \ell_2, \ldots, \ell_r$ and the polynomial g such that $f(X) = g(\ell_1, \ell_2, \ldots, \ell_r)$. Combined with Theorem 1.4, we can obtain a randomized $O^*(d^{O(r)})$ time algorithm with f and I given as input, with the promise that f has rank r.

We present two different algorithms as proofs for Theorem 1.4. The first is essentially a division algorithm. The second gives a circuit construction for the remainder polynomial $f \bmod I$. Both algorithms have $O^*(d^{O(r)})$ running time.

4.1 A Division Algorithm

Given $\vec{\alpha} \in \mathbb{F}^n$, a univariate ideal $I = \langle p_1(x_1), \ldots, p_n(x_n)\rangle$, and a rank r polynomial $f(\ell_1, \ldots, \ell_r)$ we show how to efficiently evaluate the remainder polynomial $f(\ell_1, \ldots, \ell_r) \bmod I$ at $\vec{\alpha}$ using a recursive procedure $\mathrm{REM}(f(\ell_1, \ldots, \ell_r), I, \vec{\alpha})$. We introduce the following notation. For $S \subseteq [n]$, let I_S denote the ideal $\langle p_i(x_i) : i \in [S]\rangle$ generated by the polynomials $p_i(x_i), i \in S$.

Let $g \in \mathbb{F}[X]$ be an n-variate polynomial. For an $n \times n$ invertible matrix T over $\mathbb{F}$, we define the polynomial

$$T(g(X)) = g(T(x_1), T(x_2), \ldots, T(x_n)),$$

where $T(x_i) = \sum_{j=1}^{n} T_{ij}x_j, i \in [n]$.

The following lemma shows how to remove the redundant variables from a low rank polynomial. Let $\ell_1, \ell_2, \ldots, \ell_r$ be homogeneous linear forms in $X = \{x_1, x_2, \ldots, x_n\}$, f be an r-variate degree-d polynomial over $\mathbb{F}$, and consider $f(\ell_1, \ell_2, \ldots, \ell_r)$. For an $n \times n$ invertible matrix T over $\mathbb{F}$, let $T(f)$ denote the polynomial

$$T(f)(X) = f(T(\ell_1), T(\ell_2), \ldots, T(\ell_r)),$$

where $T(x_i) = \sum_{j=1}^{n} T_{ij}x_j, i \in [n]$, and each $T(\ell_j), j \in [r]$ is defined by linearity.

Lemma 4.3 *Given as input a polynomial $f(\ell_1, \ldots, \ell_r)$ where $\ell_1, \ldots, \ell_r$ are given homogeneous linear forms in $\mathbb{F}[X]$, there is an invertible matrix $T \in \mathbb{F}^{n\times n}$ such that $T(x_i) = x_i, 1 \le i \le r$ and $T(f)$ is defined on the $2r$ variables $x_1, x_2, \ldots, x_{2r}$.*

Proof Write each linear form ℓ_i in two parts: $\ell_i = \ell_{i,1} + \ell_{i,2}$, where $\ell_{i,1}$ is the part over variables $x_1, \ldots, x_r$ and $\ell_{i,2}$ is over variables $x_{r+1}, \ldots, x_n$. W.l.o.g, assume that $\{\ell_{i,2}\}_{i=1}^{r'}$ is a maximum linearly independent subset of linear forms in $\{\ell_{i,2}\}_{i=1}^{r}$. Let T be the invertible linear map that fixes $x_1, \ldots, x_r$, maps the independent linear forms $\{\ell_{i,2}\}_{i=1}^{r'}$ to variables $x_{r+1}, \ldots, x_{r+r'}$, and suitably extended to the remaining variables to form an invertible map. Clearly, T can be computed in polynomial time, given the ℓ_i. This completes the proof. □

The following lemma shows that evaluating the remainder of a polynomial f modulo a univariate ideal $I = \langle p_1(x_1), \ldots, p_n(x_n)\rangle$ at a point in $\mathbb{F}^n$ can be done incrementally, by computing and evaluating the remainder modulo the smaller ideals $I_{[\ell]}, 1 \le \ell \le n$.

Lemma 4.4 *Let $f(X) \in \mathbb{F}[X]$ and $I = \langle p_1(x_1), \ldots, p_n(x_n)\rangle$ be a univariate ideal. Let $R(X)$ be the unique remainder $f \bmod I$. Let $\vec{\alpha} \in \mathbb{F}^r, r \le n$ and $R_r(X) = f \bmod I_{[r]}$. Then $R(\alpha_1, \ldots, \alpha_r, x_{r+1}, \ldots, x_n) = R_r(\alpha_1, \ldots, \alpha_r, x_{r+1}, \ldots, x_n) \bmod I_{[n]\setminus[r]}$.*

Proof By uniqueness of remainders modulo univariate ideals, it follows that $R(X) = R_r(X) \bmod I_{[n]\setminus[r]}$. Since the ideal $I_{[n]\setminus[r]}$ does not involve $x_1, x_2, \ldots, x_r$, substituting $x_i = \alpha_i$, $1 \le i \le r$ we have

$$R(\alpha_1, \alpha_2, \ldots, \alpha_r, x_{r+1}, \ldots, x_n) = R_r(\alpha_1, \alpha_2, \ldots, \alpha_r, x_{r+1}, \ldots, x_n) \bmod I_{[n]\setminus[r]}.$$

□

The next lemma is crucial for the proof of Theorem 1.4.

Lemma 4.5 *Let $f \in \mathbb{F}[X]$, and $T : \mathbb{F}^n \to \mathbb{F}^n$ be an invertible linear transformation fixing $x_1, \ldots, x_r$ and mapping $x_{r+1}, \ldots, x_n$ to linearly independent linear forms over $x_{r+1}, \ldots, x_n$. Write $R = f \bmod I_{[r]}$ and $R' = T(f) \bmod I_{[r]}$. Then $R' = T(R)$.*

Proof Let $f = \sum_{i=1}^{r} h_i(X) \cdot p_i(x_i) + R(X)$ and $T(f) = \sum_{i=1}^{r} h'_i(X) \cdot p_i(x_i) + R'(X)$. Note that for both remainder polynomials R and R', we have $\deg_{x_i} R < \deg_{x_i}(p_i)$ and $\deg_{x_i} R' < \deg(p_i)$ for $1 \le i \le r$. Now, as T is invertible and it fixes $x_1, \ldots, x_r$, we can write $f = \sum_{i=1}^{r} T^{-1}(h'_i(X)) \cdot p_i(x_i) + T^{-1}(R'(X))$. As T fixes each x_i, $i \in [r]$ it follows that $\deg_{x_i}(T^{-1}(R'(X))) < \deg(p_i(x_i))$ for $1 \le i \le r$. Combining the two expressions for f, we obtain that

$$(R - T^{-1}(R')) = 0 \bmod I_{[r]}$$

which forces $R = T^{-1}(R')$ by the degree bounds on x_i, $i \in [r]$. □

Proof of Theorem 1.4 We now describe the algorithm, prove its correctness and analyze its running time. The input to the algorithm is an arithmetic circuit computing the r-variate degree-d polynomial f, the linear forms $\ell_1, \ell_2, \ldots, \ell_r$, and the univariate polynomials $p_i(x_i)$, $i \in [n]$. Let the positive integer L bound the encoding lengths of the coefficients of the linear forms and polynomials p_i as well as any scalar inputs to the circuit defining f. □

The algorithm can be seen as a recursive procedure REM: the initial call to it is REM($f(\ell_1, \ldots, \ell_r)$, $I_{[n]}$, $\vec{\alpha}$).

Step 1. As the first step, we apply the invertible linear transformation obtained in Lemma 4.3 to f and obtain the polynomial $T(f)$ over the variables $x_1, \ldots, x_r, x_{r+1}, \ldots, x_{r+r'}$ where $r' \le r$.[1]

Step 2. The polynomial $T(f)$ can be explicitly computed as a linear combination of degree d monomials in variables $x_1, x_2, \ldots, x_{r+r'}$ in time poly$(L, s, n, d^{O(r)})$.

Step 3. Then we compute the remainder polynomial $f'(x_1, \ldots, x_{r+r'}) = T(f) \bmod I_{[r]}$ by applying the division algorithm: it essentially amounts to replacing x_i^e by $x_i^e \bmod p_i(x_i)$ when $e \ge \deg(p_i(x_i))$ for any x_i^e occurring in a monomial of $T(f)$.

[1] We use f to denote $f(\ell_1, \ldots, \ell_r)$.

Step 4. Next we compute the polynomial $g(x_{r+1},\dots,x_{r+r'}) = f'(\alpha_1,\dots,\alpha_r,x_{r+1},\dots,x_{r+r'})$. By Lemma 4.3, we have $T^{-1}(x_{r+i}) = \ell_{i,2}$ for $1 \le i \le r'$. Hence, $T^{-1}(f') = g(\ell_{1,2},\ell_{2,2},\dots,\ell_{r',2})$.

Step 5. We next consider the polynomial $g(\ell_{1,2},\ell_{2,2},\dots,\ell_{r',2})$ and recursively compute $\mathrm{REM}(g(\ell_{1,2},\dots,\ell_{r',2}), I_{[n]\setminus[r]}, \vec{\alpha}')$ where $\vec{\alpha}' = (\alpha_{r+1},\dots,\alpha_n)$.

Correctness Let $R(X) = f \bmod I_{[n]}$ be the unique remainder polynomial. Let $R_r(X) = f \bmod I_{[r]}$. Then, by Lemma 4.4, we know that $R_r \bmod I_{[n]\setminus[r]} = R$, and that it suffices to show $g(\ell_{1,2},\dots,\ell_{r',2}) = R_r(\alpha_1,\dots,\alpha_r,x_{r+1},\dots,x_n)$ as that would imply

$$\mathrm{REM}(g(\ell_{1,2},\dots,\ell_{r',2}), I_{[n]\setminus[r]}, \vec{\alpha}') = \mathrm{REM}(f(\ell_1,\dots,\ell_r, I_{[n]}, \vec{\alpha}) = R(\alpha_1,\alpha_2,\dots,\alpha_n),$$

showing the correctness of the recursion.

Let $R'(x_1,\dots,x_r,x_{r+1},\dots,x_n) = T(f) \bmod I_{[r]}$. By Lemma 4.5 we have $R' = T(R_r)$ and hence $R_r = T^{-1}(R')(x_1,\dots,x_r,T^{-1}(x_{r+1}),\dots,T^{-1}(x_n))$. By definition of the linear map T, and substituting $x_i = \alpha_i$, $i \in [r]$, we have

$$\begin{aligned} g(\ell_{1,2},\dots,\ell_{r',2}) &= T^{-1}(R')(\alpha_1,\dots,\alpha_r,T^{-1}(x_{r+1}),\dots,T^{-1}(x_{r+r'})) \\ &= R_r(\alpha_1,\dots,\alpha_r,x_{r+1},\dots,x_n). \end{aligned}$$

Running Time In order to bound the running time of the above algorithm, we need to bound the total number of scalar arithmetic operations and the size of the scalars involved in the computations. We will bound the total number of arithmetic operations by $\mathrm{poly}(L,s,n,d^{O(r)})$, where L bounds the encoding lengths of the scalars in the input and s is the size the input circuit for f.

First consider the case when $\mathbb{F}$ is a finite field. In that case, we can let L bound encodings of all elements of $\mathbb{F}$. We only need to bound the size of the polynomial $g(\ell_{1,2},\dots,\ell_{r',2})$ and analyze the total number of operations.

Firstly, the polynomial $T(f)$ can be explicitly computed from the input arithmetic circuit deterministically in time $\mathrm{poly}(L,s,n,d^{O(r)})$, because it has at most $\binom{d+2r}{2r}$ many monomials (as the number of variables is $r + r' \le 2r$).

Next, notice that the polynomial $g(x_{r+1},\dots,x_{r+r'})$ can also be written as a linear combination of at most $\binom{d+2r}{2r}$ many degree-d monomials in $x_{r+1},\dots,x_{r+r'}$. Thus, the polynomial $g(\ell_{1,2},\ell_{2,2},\dots,\ell_{r',2})$ can be seen as a $\Sigma\Pi\Sigma$ circuit. In other words, it is a sum of at most $\binom{d+2r}{2r}$ products of the linear forms $\ell_{i,2}$, and the products are at most d-fold.

Further, notice that the number of divisions (by the univariate polynomials $p_i(x_i)$, $i \in [r]$) performed in Step 3 is r per monomial of $T(f)$. Since $T(f)$ has at most $\binom{d+2r}{2r}$ monomials the number of univariate polynomial divisions, and hence number of scalar operations, is bounded by $\mathrm{poly}(L,s,n,d^{O(r)})$. All other steps require $\mathrm{poly}(s,n,d,L)$ operations.

Now, in each recursive application the number of generators in the ideal is reduced by at least one, and there is only one recursive call made.

Thus, the overall number of scalar (i.e., $\mathbb{F}$) operations involved in the algorithm is bounded by $\text{poly}(L, s, n, d^{O(r)})$.

The above analysis bounding the total number of operations also applies for $\mathbb{F} = \mathbb{Q}$. For $\mathbb{Q}$, we additionally need to bound the sizes of the numbers during the computation.

Bit-size Growth Over $\mathbb{Q}$ It suffices to argue that the size of coefficients in the polynomial $g(\ell_{1,2}, \ell_{2,2}, \ldots, \ell_{r',2})$ increase by a fixed additive value bounded by $\text{poly}(n, d, L)$. As the total number of recursive calls is at most n, this would polynomially bound all scalars involved in the entire computation.

Let $\tilde{L}$ bound the coefficients of polynomial $f(z_1, z_2, \ldots, z_r)$. As $2^{\tilde{L}} \leq 2^{Ld} \cdot \binom{d+r}{r}$, we have $\tilde{L} \leq dL + r\log(r+d)$.

We will show that the $\sum\prod\sum$ circuit that we use for g in the next recursive step has coefficients of bit size at most $\tilde{L} + \text{poly}(n, d, L)$.

For $h \in \mathbb{Q}[X]$, let $c(h)$ denote the maximum coefficient (in absolute value) of a nonzero monomial of h. By direct expansion

$$|c(f(\ell_1, \ldots, \ell_r))| \leq 2^{\tilde{L}+\text{poly}(n,d,L)}.$$

Also the matrix T of Lemma 4.3, and its inverse, require $\text{poly}(n, L)$ size entries.

Therefore, $c(T(f(\ell_1, \ldots, \ell_r)) \leq 2^{\tilde{L}+\text{poly}(n,d,L)}$. Next, the algorithm expands $T(f)$ explicitly as a sum of $d^{O(r)}$ monomials. Dividing $T(f)$ by the polynomials $p_1(x_1), \ldots, p_r(x_r)$ one by one, and substituting $x_1 = \alpha_1, \ldots, x_r = \alpha_r$ giving us the remainder polynomial $g(x_{r+1}, \ldots, x_{r+r'})$. Each such division involves computing a remainder polynomial of the form $x_i^e \text{mod} p_i(x_i)$ for some $e \leq d$, which does not involve intermediate computations. Each such remainder $x_i^e \text{mod} p_i(x_i)$ obtained has $\text{poly}(n, d, L)$ size coefficients and degree at most $\deg(p_i) - 1$. Putting it together, it follows that $|c(g)| \leq 2^{\tilde{L}+\text{poly}(n,d,L)}$.

Now the algorithm passes the $d^{O(r)}$ size $\Sigma\Pi\Sigma$ circuit $g(\ell_{1,2}, \ldots, \ell_{r',2})$ (We note that $T^{-1}(x_{r+1}) = \ell_{1,2}, \ldots, T^{-1}(x_{r+r'}) = \ell_{r',2}$), univariates $p_{r+1}(x_{r+1}), \ldots, p_n(x_n)$ and the point $(\alpha_{r+1}, \ldots, \alpha_n)$ for the next recursive call.

In the recursive call $\text{REM}(g(\ell_{1,2}, \ldots, \ell_{r',2}), I_{[n]\setminus[r]}, \vec{\alpha}')$, notice that the only change in the input size is in the size of g (which, as shown above, is of $O^*(d^{O(r)})$ size with $L + \text{poly}(n, d, L)$ size coefficients).

As there are at most n recursive calls overall, all coefficients involved at intermediate stages are bounded by $\text{poly}(n, d, L)$ for a fixed polynomial p.

Remark 4.6 Given a rank r polynomial $f(\ell_1, \ldots, \ell_r)$ and a univariate ideal $I = \langle p_1(x_1), \ldots, p_n(x_n)\rangle$, we can decide the membership of f in I by testing if the remainder polynomial $f \bmod I$ is identically zero by evaluating it at a randomly chosen α over $\mathbb{F}$ or a suitable extension field [14, 31, 34]. Hence, univariate ideal membership of degree-d rank-r polynomials can be decided in randomized $d^{O(r)} \cdot \text{poly}(n)$ time where $d = \max\{\deg(f), \deg(p_i) : 1 \leq i \leq n\}$ by Theorem 1.4.

As mentioned in Section 1, an application of our result yields an $n^{O(r)}$ time algorithm for computing the permanent of rank-r matrices over $\mathbb{Q}$ or any finite field. Barvinok [9], via a different method, had obtained an $n^{O(r)}$ time algorithm for this problem over $\mathbb{Q}$.

Corollary 4.7

- *There is an $n^{O(r)}$ time algorithm to compute the permanent of $n \times n$ matrices of rank at most r over the field of rationals or any finite field.*
- *For finite fields $\mathbb{F}$ the algorithm has running time bounded by $O^*(|\mathbb{F}|^{O(r^2)})$. In particular, over constant size fields this is an FPT algorithm for computing* $\mathrm{Perm}(A)$ *(with r as fixed parameter).*

Proof The $n^{O(r)}$ time algorithm is a direct application of the algorithm of Theorem 1.4 to the product of linear forms polynomial and univariate ideal described in Fact 1.2.

For the second part, suppose $\mathbb{F}$ is a finite field of size p^s, where $\mathrm{char}(\mathbb{F}) = p$ (a prime). Let $A \in \mathbb{F}^{n\times n}$ be a rank r matrix and let $\ell_i = \sum_{j=1}^n a_{ij}x_j$, $1 \le i \le n$. Then there are exactly $N = |\mathbb{F}|^r - 1$ many distinct nonzero $\mathbb{F}$-linear forms spanned by $\ell_i, i \in [n]$. We denote them by $\ell'_1, \ell'_2, \ldots, \ell'_N$. Then the product $\prod_{i=1}^n \ell_i$ can be expressed as

$$\prod_{i=1}^{n} \ell_i = \prod_{j=1}^{N} \ell'^{d_j}_j,$$

where $d_1 + d_2 + \cdots + d_N = n$ is the degree of the product. Therefore, by Fact 1.2 we have

$$\mathrm{Perm}(A) = \prod_{j=1}^{N} \ell'^{d_j}_j \bmod \left\langle x_1^2, x_2^2, \ldots, x_n^2 \right\rangle.$$

Now, suppose $d_j \ge p$ for some j. Let $\ell'_j = \sum_{k=1}^n \alpha_{jk}x_k$. Then writing $d_j = pq_j + r_j, r_j < p$ we have

$$\begin{aligned}
\ell'^{d_j}_j &= \left(\sum_{k=1}^{n} \alpha_{jk}x_k\right)^{pq_j+r_j} \\
&= (\sum_{k=1}^{n} \alpha_{jk}^p x_k^p)^{q_j} \dot{(}\sum_{k=1}^{n} \alpha_{jk}x_k)^{r_j} \\
&= 0 \bmod \left\langle x_1^2, x_2^2, \ldots, x_n^2 \right\rangle.
\end{aligned}$$

The last equality holds because $x_k^p = 0 \bmod x_k^2$ for any $p \ge 2$. Consequently, if $n > (p-1)\dot{(}|\mathbb{F}|^r - 1)$ then $d_j \ge p$ for some j, and by Fact 1.2 we have $\mathrm{Perm}(A) = 0$. For $n \le (p-1)\dot{|}\mathbb{F}|^r$ the $n^{O(r)}$-time algorithm is an $O^*(p^r \dot{|}\mathbb{F}|^{O(r^2)})$ time algorithm, which completes the proof. □

4.2 Small Circuit for the Remainder Polynomial

The first algorithm is based on repeated division and partial evaluation. As such, it does not directly yield a small circuit for $f \bmod I$.

We now show that $f \bmod I$ has an arithmetic circuit of size $O^*(d^{O(r)})$, where $d = \deg(f)$. The circuit has a nice form: it is a $d^{O(r)}$-sum of products of univariate polynomials, each of degree at most d. Moreover, this circuit can be constructed in time $O^*(d^{O(r)})$ from the input f and I. This also yields another proof of Theorem 1.4, since evaluation of the circuit obtained at a given scalar point can be done in $O^*(d^{O(r)})$ time.

Some notation for the sequel: For $q \in \mathbb{F}[t_1, t_2, \ldots, t_r, X]$, let $[t_1^{d_1} t_2^{d_2} \cdots t_r^{d_r}](q)$ denote the coefficient of $t_1^{d_1} t_2^{d_2} \cdots t_r^{d_r}$ in q, noting that $[t_1^{d_1} t_2^{d_2} \cdots t_r^{d_r}](f) \in \mathbb{F}[X]$.

Now, we can write $f = g(\ell_1, \ell_2, \ldots, \ell_r)$ as a sum of $d^{O(r)}$ d-products of the r linear forms. Thus, it suffices to give a small circuit, of the above form, for a remainder $\ell_1^{d_1} \ell_2^{d_2} \cdots \ell_r^{d_r} \bmod I$, where $I = \langle p_1(x_1), p_2(x_2), \ldots, p_n(x_n)\rangle$. A $+$-gate summing up all these remainder circuits would be a circuit of the claimed form for $f \bmod I$.

We first consider a single power $\ell^d \bmod I$, where $\ell = \sum_{i=1}^n a_i x_i$ is a homogeneous linear form in $\mathbb{F}[X]$. By the multinomial theorem

$$\left(\sum_{i=1}^{n} a_i x_i t\right)^d = \sum_{j_1+j_2+\cdots+j_n=d} \binom{d}{j_1, j_2, \ldots, j_n} \prod_{i=1}^{n} (a_i x_i t)^{j_i}.$$

For fields $\mathbb{F}$ of characteristic zero, we can write:

$$\left(\sum_{i=1}^{n} a_i x_i\right)^d = d![t^d]\left(\prod_{i=1}^{n}\left(\sum_{j=0}^{d} \frac{1}{j!}(a_i x_i t)^j\right)\right). \qquad (1)$$

Equation 1 is combinatorially verified by noting that the term $\prod_{i=1}^n (a_i x_i t)^{j_i}$, for $j_1 + j_2 + \ldots j_n = d$ occurs precisely $\binom{d}{j_1, j_2, \ldots, j_n}$ times on the right side, matching the multinomial expansion of the left side. This identity was first used in arithmetic circuit complexity by Saxena [28],[2] and has found many applications.

Remark 4.8 Observe that, the right hand side expression of (1) can be viewed as a univariate polynomial in t of degree nd. Therefore, by interpolation, we can find $\alpha_1, \ldots, \alpha_{nd+1} \in \mathbb{F}$ (or a suitable extension field of $\mathbb{F}$) and $\beta_1, \ldots, \beta_{nd+1} \in \mathbb{F}$ such that,

$$\left(\sum_{i=1}^{n} a_i x_i\right)^d = \sum_{\ell=1}^{nd+1} \beta_\ell \left(\prod_{i=1}^{n}\left(\sum_{j=0}^{d} \frac{1}{j!}(a_i x_i \alpha_\ell)^j\right)\right). \qquad (2)$$

Therefore, a power of a linear form can be expressed as a small sum of product of univariates.

[2] Shown [28] using the identity $e^{\sum_i y_i} = \prod_i e^{y_i}$, and taylor series expansion for e^{y_i}.

This can be generalized to the finite fields setting [16]. We give a self-contained description of this, as it is required for the circuit construction for $f \bmod I$. First, for $\mathrm{char}(\mathbb{F}) = p$, (1) only holds for $d < p$, as each $k!$ occurring in it is invertible in $\mathbb{F}_p$ precisely if $d < p$. To obtain a suitable form of the equation for $d \geq p$, we first write $d = \sum_{k=0}^{s} e_k p^k$, for $s \leq \log_p(d) - 1$ and each $e_k < p$. Since $\mathrm{char}(\mathbb{F}) = p$ for each $k \leq s$, letting $a_i^{p^k} = a_{k,i} \in \mathbb{F}$ we have:

$$\left(\sum_{i=1}^{n} a_i x_i t\right)^{e_k p^k} = \left(\sum_{i=1}^{n} a_{k,i} x_i^{p^k} t^{p^k}\right)^{e_k}.$$

Combined with (1) we get for $0 \leq k \leq s$:

$$\ell^{e_k p^k} = \left[t^{e_k p^k}\right]\left(\sum_{i=1}^{n} a_{k,i} x_i^{p^k} t^{p^k}\right)^{e_k} = (e_k)!\left[t^{e_k p^k}\right]\left(\prod_{i=1}^{n}\left(\sum_{j=0}^{e_k} \frac{1}{j!}\left(a_{k,i} x_i^{p^k} t^{p^k}\right)^j\right)\right).$$

As $d = \sum_{k=0}^{s} e_k p^k$, multiplying over all k gives

$$\begin{aligned}\ell^d &= \prod_{k=0}^{s}\left[t^{e_k p^k}\right]\left(\sum_{i=1}^{n} a_{k,i} x_i^{p^k} t^{p^k}\right)^{e_k}\\ &= \prod_{k=0}^{s}(e_k)!\left[t^{e_k p^k}\right]\left(\prod_{i=1}^{n}\left(\sum_{j=0}^{e_k} \frac{1}{j!}\left(a_{k,i} x_i^{p^k} t^{p^k}\right)^j\right)\right)\end{aligned}$$

Let $t_0, t_1, \ldots, t_s$ be new variables. Replacing t^{p^k} by t_k for each $0 \leq k \leq s$ in the above equations we get:

$$\ell^d = \left[t_0^{e_0} t_1^{e_1} \ldots t_s^{e_s}\right]\prod_{k=0}^{s}(e_k)!\left(\prod_{i=1}^{n}\left(\sum_{j=0}^{e_k} \frac{1}{j!}\left(a_{k,i} x_i^{p^k} t_k\right)^j\right)\right). \tag{3}$$

Thus, $\ell^d = [t_0^{e_0} t_1^{e_1} \ldots t_s^{e_s}] Q_{\ell,d}$, where $Q_{\ell,d}$ is a product of the sn many polynomials as above (each of which is a bivariate polynomial in x_i, t_k, $i \in [n]$, $k \in [s]$). This equation generalizes to express the product $\ell_1^{d_1} \cdot \ell_2^{d_2} \cdots \ell_r^{d_r}$ in the following form:

$$\ell_1^{d_1} \cdot \ell_2^{d_2} \cdots \ell_r^{d_r} = \left[t_1^{\nu_1} t_2^{\nu_2} \ldots t_D^{\nu_D}\right]\prod_{k=1}^{D}\prod_{i=1}^{n} q_{k,i}, \tag{4}$$

where $D = (s+1)r$, and $\nu_k < p$ for each $k \in [D]$ such that $d_j = \sum_{k=(s+1)(j-1)+1} (s+1)j\nu_k p^{k-(s+1)(j-1)-1}$, $j \in [r]$. It is obtained simply by applying (3) to each $\ell_j^{d_j}$ with a different set of $s+1$ many variables t_i and multiplying these equations for $1 \leq j \leq r$. We note that each $q_{k,i} \in \mathbb{F}[x_i, t_k]$ is a polynomial of individual variable degree at most $d = \sum_{j=1}^{r} d_j$, as is clear from (3). The next claim will complete the proof of Theorem 1.4.

Claim 4.9 $\ell_1^{d_1} \cdot \ell_2^{d_2} \cdots \ell_r^{d_r} \bmod I$ has an arithmetic circuit which is a $d^{O(r)}$-sum of products of univariate polynomials, where each univariate polynomial in x_i involved in a product has degree at most $\deg(p_i(x_i)) - 1$.

For the proof, we first consider the following subexpression in (4)

$$[t_1^{\nu_1} t_2^{\nu_2} \ldots t_D^{\nu_D}] \prod_{k=1}^{D} q_{k,i},$$

which we will evaluate modulo $p_i(x_i)$. Note that the number of monomials of the form $\prod_{k=1}^{D} t_k^{\mu_k}$, $\mu_k \le \nu_k < p$ is bounded by $p^D = (p^{s+1})^r = d^{O(r)}$. Thus, in $O^*(d^{O(r)})$ time we can expand the product $\prod_{k=1}^{D} q_{k,i}$ by multiplying out the polynomials, one by one, from left to right. After each multiplication, we replace x_i^a by its remainder $x_i^a \bmod p_i$ and drop any term with a factor t_k^p, $k \in [D]$. This will result in a polynomial expression of the form

$$Q_i = \sum_{\bar{\mu}} r_{\bar{\mu}}(x_i) \prod_{k=1}^{D} t_k^{\mu_k},$$

where the sum runs over the $d^{O(r)}$ many tuples $\bar{\mu} = (\mu_1, \mu_2, \ldots, \mu_k)$ such that $\mu_k \le \nu_k$ for each k. Thus, each $r_{\bar{\mu}}(x_i)$ is a univariate in x_i of degree at most $\deg(p_i) - 1$. We can now evaluate the product $Q_1 Q_2 \cdots Q_n$ modulo the ideal $\langle t_1^p, t_2^p, \ldots, t_D^p \rangle$ by multiplying out adjacent pairs and dropping any terms with a factor t_k^p, $k \in [D]$. This will given an expression for $Q_1 Q_2 \cdots Q_n$ modulo $\langle t_1^p, t_2^p, \ldots, t_D^p \rangle$ of the form $\sum_{\bar{\mu}} R_{\bar{\mu}} \prod_{k=1}^{D} t_k^{\mu_k}$, where each $R_{\bar{\mu}}$ is a $d^{O(r)}$-sum of products of n univariate polynomials (and in each product the i^{th} is a polynomial in x_i of degree $\deg(p_i) - 1$). Finally, we note that $R_{\bar{\nu}}$ is the desired polynomial expression for $\prod_{j=1}^{r} \ell_j^{d_j} \bmod I$, completing the proof of the claim.

4.3 Vertex Cover Detection in Low Rank Graphs

In the Vertex Cover problem, the input instances are pairs (G, k), where $G = (V, E)$ is a graph and k is an integer. The problem is to decide whether or not G has a vertex cover of size k. This is a classical NP-complete problem.

A graph G is said to be of rank r if the rank of the adjacency matrix A_G is of rank r. Graphs of low rank were studied by Lovasz and Kotlov [4, 20]. As an application of Theorem 1.4, we obtain an $n^{O(r)}$ time algorithm to compute a minimum vertex cover in an n-vertex graph of rank r.

Remark 4.10 A pair of vertices x, y in a graph G are *twins* if they have identical neighborhoods in G. Lovasz and Kotlov [4] have shown that a rank r graph G that is twin-free has at most $O(2^{r/2})$ vertices. Clearly, a minimal vertex cover S of G does not contain twins. Therefore, in order to search for a minimum vertex cover for G, it suffices to search for it in a maximal twin-free subgraph H of G, which is easy to find in poly(n) time. Now, H will have at most $O(2^{r/2})$ vertices as its rank is also bounded by r. A brute-force search for the minimum vertex cover in $V(H)$ yields an $O^*(2^{2^{r/2}})$ algorithm. For n that is double exponential in r, this brute-force search is faster than the $n^{O(r)}$ algorithm of this section.

Proof of Theorem 1.5 We give a polynomial-time reduction from Vertex Cover to Univariate Ideal Membership. Let (G, k) be a Vertex Cover instance. Let $I = \langle x_1^2 - x_1, x_2^2 - x_2, \ldots, x_n^2 - x_n \rangle$ and

$$f = \prod_{s=1}^{\binom{n}{2}} (\vec{x} A_G \vec{x}^T - s) \cdot \prod_{t=0}^{n-k-1} \left(\sum_{i=1}^{n} x_i - t \right),$$

where A_G is the adjacency matrix of the graph G and $\vec{x} = (x_1, x_2, \ldots, x_n)$ is row-vector.

Claim 4.11 The rank of the polynomial f is at most $r + 1$.

Proof We note that A_G is symmetric since it encodes an undirected graph. Let Q be an invertible $n \times n$ matrix that diagonalizes A_G. So we have $Q A_G Q^T = D$ where D is a diagonal matrix with only the first r diagonal elements being non-zero. Let $\vec{y} = (y_1, y_2, \ldots, y_n)$ be another row-vector of variables. Now, we show the effect of the transform $\vec{x} \mapsto \vec{y} Q$ on the polynomial $\vec{x} A_G \vec{x}^T$. Clearly, $\vec{y} Q A_G Q^T \vec{y}^T = \vec{y} D \vec{y}^T$ and since there are only r non-zero entries on the diagonal, the polynomial $\vec{y} D \vec{y}^T$ is over the variables $y_1, y_2, \ldots, y_r$. Thus $g = \prod_{s=1}^{\binom{n}{2}} (\vec{x} A_G \vec{x}^T - s)$ is a rank r polynomial. Also $h = \prod_{t=0}^{n-k-1} (\sum_{i=1}^{n} x_i - t)$ is a rank 1 polynomial as there is only one linear form $\sum_{i=1}^{n} x_i$. Since $f = gh$, we conclude that f is a rank $r + 1$ polynomial. □

Now the proof of Theorem 1.5 follows from the next claim.

Claim 4.12 The graph G has a Vertex Cover of size k if and only if $f \notin I$.

Proof First, observe that the set of common zeroes of the generators of the ideal I is the set $\{0, 1\}^n$. Let S be a vertex cover in G such that $|S| \leq k$. We will exhibit a point $\vec{\alpha} \in \{0, 1\}^n$ such that $f(\vec{\alpha}) \neq 0$. This will imply that $f \notin I$. Identify the vertices of G with $\{1, 2, \ldots, n\}$. Define $\vec{\alpha}(i) = 0$ if and only if $i \in S$. Since $\vec{x} A_G \vec{x}^T = \sum_{(i,j) \in E_G} x_i x_j$ and S is a vertex cover for G, it is clear that $\vec{x} A_G \vec{x}^T(\vec{\alpha}) = 0$. Also $(\sum_{i=1}^{n} x_i)(\vec{\alpha}) \geq n - k$. Then clearly $f(\vec{\alpha}) \neq 0$.

For the other direction, suppose that $f \notin I$. Then by Theorem 1.1, there exists $\vec{\alpha} \in \{0, 1\}^n$ such that $f(\vec{\alpha}) \neq 0$. Define the set $S \subseteq [n]$ as follows. Include $i \in S$ if and only if $\vec{\alpha}(i) = 0$. Since $f(\vec{\alpha}) \neq 0$, and the range of values that $\vec{x} A_G \vec{x}^T$ can take is $\{0, 1, \ldots, |E|\}$, it must be the case that $\vec{x} A_G \vec{x}^T(\vec{\alpha}) = 0$. It implies that the set S is a vertex cover for G. Moreover, $\prod_{t=0}^{n-k-1} (\sum_{i=1}^{n} x_i - t)(\vec{\alpha}) \neq 0$ implies that $|S| \leq k$. □

The degree of the polynomial f is bounded by $n^2 + n$ and from Claim 4.12 we know that $f \bmod I$ is a non-zero polynomial if and only if G has a vertex cover of size k. By the Polynomial Identity lemma [14, 31, 34], $(f \bmod I)(\vec{\beta})$ is non-zero with high probability when $\vec{\beta}$ is chosen randomly from a small domain. Now, we need to just compute $(f \bmod I)(\vec{\beta})$ where f is a rank $r + 1$ polynomial with $\ell_i = (\vec{x} Q^{-1})_i$ for each $1 \le i \le r$ and $\ell_{r+1} = \sum_{i=1}^{n} x_i$ which can be performed in $(n, k)^{O(r)}$ time using Theorem 1.4. □

5 Univariate Ideal Membership Parameterized by Degree

In this section, we consider the degree of the input polynomial as the fixed parameter. Consider $I = \langle \{p_i(x_i)\}_{i=1}^n \rangle$ be a univariate ideal and $f \in \mathbb{F}[X]$ be a degree k polynomial given by an arithmetic circuit. Clearly, there is a simple $O^*(n^{O(k)})$ algorithm for it: we can write $f = \sum_m \alpha_m m$ as a linear combination of $\binom{n+k}{k}$ many monomials m. We can then compute the remainder $f \bmod I = \sum_m \alpha_m (m \bmod I)$ as a linear combination of monomials.

We first prove Theorem 1.6 showing a randomized $O^*((2e)^k)$ time algorithm for the special case where $\mathbb{F} = \mathbb{Q}$ and the ideal $I = \langle x_1^{e_1}, x_2^{e_2}, \ldots, x_n^{e_n} \rangle$.

5.1 Proof of Theorem 1.6

Proof The main step is the following reduction of checking if $f \in I$ (where f is degree-k and $I = \langle x_1^{e_1}, x_2^{e_2}, \ldots, x_n^{e_n} \rangle$) to the problem of checking if the polynomial $f \circ^s g$ is identically zero, where g is chosen as a polynomial weakly equivalent[3] to the elementary symmetric polynomial. The claimed algorithm then follows by applying a recent result of [7].

Recall that $S_{m,\ell}$ denotes the elementary symmetric polynomial of degree ℓ over m variables. Set $m = \sum_{i=1}^{n} (e_i - 1)$ and define $S_{m,\ell}$ on the m variables $z_{1,1}, \ldots, z_{1,e_1-1}, \ldots, z_{n,1}, \ldots, z_{n,e_n-1}$. Now, for $0 \le \ell \le k$ define $g_\ell(X)$ as the polynomial obtained from $S_{m,\ell}$ by replacing each $z_{i,j}$ by x_i, $1 \le i \le n$.

Claim 5.1 Given integers $e_1, e_2, \ldots, e_n$, and a homogeneous polynomial $f(X)$ of degree k, $f \in \langle x_1^{e_1}, x_2^{e_2}, \ldots, x_n^{e_n} \rangle$ if and only if $f \circ^s g_\ell \equiv 0$ for $0 \le \ell \le k$.

Proof Clearly $f \notin \langle x_1^{e_1}, x_2^{e_2}, \ldots, x_n^{e_n} \rangle$ if and only if f has a nonzero degree ℓ monomial $M = x_1^{f_1} x_2^{f_2} \ldots x_n^{f_n}$, for some $\ell \le k$, such that $f_i < e_i$ for each $1 \le i \le n$. Hence, the scaled Hadamard product polynomial $f \circ^s g_\ell$ is not identically zero for some $\ell \le k$ if and only if $f \notin \langle x_1^{e_1}, x_2^{e_2}, \ldots, x_n^{e_n} \rangle$. □

[3] Polynomials $f, g \in \mathbb{F}[X]$ are *weakly equivalent* if for each monomial m, $[m]f = 0$ if and only if $[m]g = 0$.

The proof now follows from the recent work of [7] as explained below:

For checking if $f \circ^s g_\ell$ (as defined in Lemma 5.1) is identically zero, it suffices to check for some polynomial $\tilde{g_\ell}$ weakly equivalent to g_ℓ that $f \circ^s \tilde{g_\ell}$ is identically zero. By color coding [3], we can construct a homogeneous depth-three circuit of size $e^k\text{poly}(n)$ that computes a polynomial weakly equivalent to $S_{n,k}$ with high probability (see [7] for details). Replacing each $z_{i,j}$ by x_i, $1 \le i \le n$, we obtain a homogeneous depth-three circuit of the same size for a polynomial $\tilde{g_\ell}$ weakly equivalent to g defined in Lemma 5.1.

Now, it is shown in [7] that we can compute the scaled Hadamard product of a circuit of size s_1 with a degree-k homogeneous depth three circuit of size s_2 in deterministic $O^*(2^k \cdot s_1 s_2)$ time. Therefore, $f \circ^s g_\ell$ can be computed in $O^*((2e)^k)$ time. We can check if $f \circ^s g_\ell$ is identically zero by evaluating at a randomly chosen point [14, 31, 34]. Overall, this gives a randomized $O^*((2e)^k)$ time algorithm. □

Remark 5.2

1. The above proof fails for $\text{char}(\mathbb{F}) < k$ because $f \circ^s g$ might vanish because the scaling factor $m!$ for each monomial might be divisible by $\text{char}(\mathbb{F})$.
2. Over rationals, we can apply a recent work [27] to obtain an $O^*(4.08^k)$ time algorithm to test identity of scaled Hadamard product with elementary symmetric polynomial. This improves the algorithm of Theorem 1.6 to a randomized $O^*(4.08^k)$ algorithm.

We now consider deciding the membership for the general case of univariate ideal. We first make the following observation.

Observation 5.3 *Let $I = \left\langle \{p_i(x_i)\}_{i=1}^n \right\rangle$ be a univariate ideal and $f \in \mathbb{F}[X]$ be a degree k polynomial of Waring rank r. Then f can be expressed as an r-sum of k^{th} powers of linear forms i.e. $f = \sum_{i=1}^r \ell^k$ for some affine linear forms ℓ_i. Then, there is a deterministic* poly(r, k, n) *algorithm to decide whether $f \in I$.*

The proof follows easily from (2) that allows us to write f as a small sum of product of univariates.

Remark 5.4 As an application, motivated by the permanent lemma [1, Lemma 8.1], consider the following constrained linear *inequations* problem: given $A \in \mathbb{F}^{k\times n}$, $(b_1, b_2, \ldots, b_k)^T \in \mathbb{F}^k$, and a family of subsets $S_1, S_2, \ldots, S_n$ of the field $\mathbb{F}$ the problem is to find an assignment $\vec{x} = \vec{a} \in S_1 \times S_2 \times \cdots \times S_n$ such that $\sum_j a_{ij}x_j \neq b_i$, $1 \le i \le k$. We define the degree-k polynomial

$$f = \prod_{i=1}^{k} \left(\sum_{j=1}^{n} a_{ij}x_j - b_j \right).$$

Clearly, a solution to the above inequation system exists if and only if there exists $\vec{a} \in S_1 \times \cdots S_n$ such that $f(\vec{a})$ is non-zero. By the Combinatorial Nullstellensatz [1] (Theorem 1.1), it can be expressed as a univariate ideal membership problem. As

f is a product of k linear forms, its the Waring rank is bounded by $O^*(2^k)$. By Observation 5.3, we obtain a deterministic $O^*(2^k)$ algorithm to solve this constrained inequation system.

For degree-k, n-variate polynomials f, we do not have an algorithm with running time better than $O^*\left(\binom{n+k}{k}\right)$ for univariate ideal membership in general. However, if each generator polynomial p_i has distinct roots we obtain a faster algorithm.

Theorem 5.5 *Let $I = \langle p_1(x_1), \ldots, p_n(x_n)\rangle$ be a univariate ideal given explicitly by a set of univariate polynomials $p_1, \ldots, p_n$ such that for each $i \in [n]$, $p_i(x_i)$ has distinct roots over $\mathbb{Q}$. Given a polynomial $f(X) \in \mathbb{C}[X]$ of degree k and I as input, we can decide whether $f \in I$ or not in randomized $O^*(n^{k/2})$ time.*

Proof W.l.o.g. we can assume the degree of each p_i is at most k. Otherwise, we can drop p_i from I. For $i \in [n]$, let $S_i \subset \mathbb{Q}$ be the set of all roots of p_i. By Alon's Combinatorial Nullstellensatz (Theorem 1.1), Theorem 5.4 can be restated as the following.

Claim 5.6 Given a polynomial $f(X) \in \mathbb{C}[X]$ of degree k and $S_1, \ldots, S_n$ such that for each $i \in [n]$, $S_i \subset \mathbb{C}$ as inputs, we can decide whether $S_1 \times \cdots \times S_n$ contains a nonzero of f in in randomized $O^*(n^{k/2})$ time.

For a degree-k polynomial $f \in \mathbb{F}[X]$ let

$$\tilde{f} = x_{n+1}^k \cdot f\left(\frac{x_1}{x_{n+1}}, \frac{x_2}{x_{n+1}}, \ldots, \frac{x_n}{x_{n+1}}\right),$$

be its homogenization. Thus, $\tilde{f}$ is homogeneous of degree k and $\tilde{f}(x_1, x_2, \ldots, x_n, 1) = f(x_1, \ldots, x_n)$. Clearly, f is nonzero on the n-dimensional grid $S_1 \times \cdots \times S_n$ if and only if $\tilde{f}$ is nonzero on the $n+1$ -dimensional grid $S_1 \times \cdots \times S_n \times \{1\}$. Hence, without loss of generality we can assume f is homogeneous degree k.

Observation 5.7 *For a homogeneous polynomial f of degree k,*

$$f \circ^s (a_1x_1 + \ldots + a_nx_n)^k \mid_{\vec{1}} = k! \cdot f(a_1, \ldots, a_n).$$

We need to decide whether there exists a point $\vec{a} \in S_1 \times \cdots \times S_n$ such that $f(\vec{a}) \neq 0$.

For each $(a_1, \ldots, a_n) \in S_1 \times \ldots \times S_n$, by (2) we can write,

$$\frac{1}{k!} \cdot (a_1x_1 + \ldots + a_nx_n)^k = \sum_{\ell=1}^{nk+1} \beta_\ell \cdot \prod_{i=1}^{n} p_i(a_i\alpha_\ell x_i).$$

where $\alpha_1, \ldots, \alpha_n \in \mathbb{Q}$ are some distinct points, $\beta_\ell \in \mathbb{Q}$, and each p_i is univariate.

Now, we define the "grid" polynomial

$$g = \sum_{\ell=1}^{nk+1} \beta_\ell \cdot \prod_{i=1}^{n} \left(\sum_{a_i \in S_i} \xi_{i,a_i} p_i(a_i \alpha_\ell x_i) \right) \tag{5}$$

$$= \sum_{(a_1,\ldots,a_n)\in S_1\times\ldots\times S_n} \prod_{i=1}^{n} \xi_{i,a_i} \left(\sum_{\ell=1}^{nk+1} \beta_\ell \cdot \prod_{i=1}^{n} p_i(a_i\alpha_\ell x_i) \right), \tag{6}$$

where ξ_{i,a_i}, $i \in [n]$, $a_i \in S_i$ are new variables. Hence,

$$f \circ^s g \mid_{\vec{1}} = \sum_{(a_1,\ldots,a_n)\in S_1\times\ldots\times S_n} \prod_{i=1}^{n} \xi_{i,a_i} f \circ^s \left(\sum_{\ell=1}^{nk+1} \beta_\ell \cdot \prod_{i=1}^{n} p_i(a_i\alpha_\ell x_i) \right) \mid_{\vec{1}} \tag{7}$$

$$= \sum_{(a_1,\ldots,a_n)\in S_1\times\ldots\times S_n} \prod_{i=1}^{n} \xi_{i,a_i} f(a_1, a_2, \ldots, a_n) \tag{8}$$

Thus, $f \circ^s g \mid_{\vec{1}}$ is a nonzero polynomial (in the ξ_{i,a_i} variables) of degree n iff $f \circ^s (a_1x_1 + \cdots a_nx_n)^k$ is nonzero for some $(a_1,\ldots,a_n) \in S_1 \times \ldots S_n$. By the Polynomial Identity Lemma [14, 31, 34], we can independently randomly assign values for the ξ_{i,a_i} variables from $[n^2]$, and the evaluation is nonzero with probability at least $1 - 1/n$ iff f nonzero on a grid point in $S_1 \times \cdots \times S_n$. Furthermore, from (7) we note that we can clear the denominators of all the β_ℓ and the polynomials $p_i(a_i\alpha_i x_i)$ and the polynomial f (given by input circuit) and take out a common factor $\frac{1}{D}$ (where D is a polynomially many bits long integer) to write (7) as

$$f \circ^s g \mid_{\vec{1}} = \frac{1}{D} \sum_{(a_1,\ldots,a_n)\in S_1\times\ldots\times S_n} \prod_{i=1}^{n} \xi_{i,a_i} \hat{f} \circ^s \left(\sum_{\ell=1}^{nk+1} \gamma_\ell \cdot \prod_{i=1}^{n} \hat{p}_i(a_i\alpha_\ell x_i) \right) \mid_{\vec{1}},$$

where $\hat{f}$ and $\hat{p}_i(a_i\alpha_\ell x_i)$ have integer coefficients. Thus, when $f \circ^s g \mid_{\vec{1}}$ is nonzero at a choice of the ξ_{i,a_i} then it is of absolute value at least $1/D$.

Therefore, after randomly choosing $\xi_{i,a_i} \in_R [n^2]$, it is clear from (5) that the problem reduces to efficiently computing the scaled Hadamard product $f \circ^s h \mid_{\vec{1}}$ evaluated at $\vec{1}$, where $h = \prod_{i=1}^{n} q_i(x_i)$ and each q_i is of degree k. We now show that $f \circ^s h \mid_{\vec{1}}$ can be computed in $O^*(n^{k/2})$ time which suffices to detect if $f \circ^s g \mid_{\vec{1}}$ is nonzero in $O^*(n^{k/2})$ time.

Claim 5.8 $f \circ^s \prod_{i=1}^{n} q_i(x_i) \mid_{\vec{1}}$ can be computed in $O^*(n^{k/2})$ time.

Notice that the above claim completes the proof, because the summation over ℓ has $nk + 1$ terms. Let $\beta = \max_\ell\{|\beta_\ell|\}$. Then the overall error in $f \circ^s g \mid_{\vec{1}}$ is bounded by the precision error of the claim multiplied by $(nk+1)\beta$ which can be made smaller than $1/D$ by choosing the precision error of the claim.

We now prove the claim. We need approximations because we will need to approximately compute the roots of the univariate polynomials q_i. Let R_i denote the nonzero roots of q_i. Then we can write

$$\prod_i q_i = \prod_{i=1}^{n} x_i^{\mu_i} \prod_{i=1}^{n} \prod_{-\beta \in R_i} (x_i + \beta)^{\nu_{i,\beta}},$$

where $\nu_{i,\beta}$ is the multiplicity of root $-\beta$ in q_i. If $\sum_i \mu_i > k$ then clearly $f \circ^s \prod_i q_i = 0$. Otherwise, let $\sum_i \mu_i = s$ and let $r = k - s$. Let $\prod_i \prod_{\beta \in R_i} \beta^{\nu_{i,\beta}} = \Gamma$. Write $\prod_{i=1}^{n} \prod_{-\beta \in R_i} (x_i + \beta)^{\nu_{i,\beta}}$ as $\Gamma \prod_{i=1}^{n} \prod_{-\beta \in R_i} (x_i/\beta + 1)^{\nu_{i,\beta}}$. Let $m = \sum_i \deg(q_i) - s$ and consider the elementary symmetric polynomial $S_{m,r}$ in variables $y_1, y_2, \ldots, y_m$. By Lee's result [24], $S_{m,r}$ can be expressed as $O^*(m^{r/2})$ sum of powers of linear forms. In the polynomial $S_{m,r}$ we replace the m variables $y_1, y_2, \ldots, y_m$ by the m nonzero roots (of the form x_i/β, as explained above) of $\prod_j q_j$. Let the product of the resulting polynomial (which is still a $O^*(m^{r/2})$-sum of r-power of linear forms) with $\Gamma \cdot \prod_{i=1}^{n} x_i^{\mu_i}$ be denoted by Q. Clearly, $f \circ^s \prod_i q_i = f \circ^s Q$. Since Q is a sum of power of linear forms using Observation 5.7, we can evaluate $f \circ^s Q \mid_{\bar{1}}$ with $O^*(n^{k/2})$ arithmetic operations.

Now, replacing each root β by a rational approximation β' such that $|\beta - \beta'| \leq 1/2^L$ for a suitably chosen polynomial bit number L, the overall error in the approximation to $f \circ^s Q \mid_{\bar{1}}$ will be bounded. It can be made smaller than ε by choosing L suitably large. We can use any efficient root approximation algorithm for univariate polynomials to find all such root approximations β'.

This completes the proof of the claim and the theorem. □

Remark 5.9 Observe that Claim 5.8 can be restated as follows: given univariate polynomials $p_i(x_i)$, $1 \leq i \leq n$, the Waring rank of the degree-k part of their product $\prod_{i=1}^{n} p_i(x_i)$ is bounded by $O^*(n^{k/2})$. Then the proof of Theorem 5.4 follows as an application of Observation 5.3.

6 Univariate Ideal Membership Parameterized by Number of Generators

In this section, we consider the univariate ideal membership parameterized on the number of generators of the univariate ideal. More precisely, we consider univariate ideal membership for input $f(X)$ by a circuit of size s and univariate ideal $I = \langle p_1(x_1), \ldots, p_k(x_k) \rangle$ (with k as fixed parameter).

We show that the *nonmembership* problem is W[2]-hard by giving an efficient reduction from the k-dominating set problem which is W[2]-complete [13].

Moreover, in contrast to the problem parameterized by $\deg(f)$, even for the special case of the ideal $I = \left\langle x_1^{e_1}, x_2^{e_2}, \ldots, x_k^{e_k} \right\rangle$ we show the problem remains hard. We are able to show it is MINI[1]-hard. Hence, even in this special case the problem cannot have an algorithm of run time $O^*(s^{o(k)})$ assuming the exponential time hypothesis. On the other hand, the problem has an easy $O^*(s^k)$ time randomized algorithm.

Proof of Theorem 1.7 Let (G, k) be an instance of the k-dominating set problem, where $G = (V, E)$ is an n-vertex graph and the fixed parameter k is the size of the independent set. Let $V(G) = \{1, 2, \ldots, n\}$. For $1 \leq i \leq k$, we define polynomials

$$p_i(x_i) = \prod_{j=1}^{n}(x_i - j).$$

The W[2]-hardness proof is an application of Alon's Combinatorial Nullstellensatz (Theorem 1.1): By definition, for each p_i its zero set is $Z(p_i) = [n]$. Therefore, a polynomial $g \in \mathbb{Q}[x_1, x_2, \ldots, x_k]$ is in the ideal $\langle p_1, p_2, \ldots, p_k\rangle$ if and only if g is zero on every point in the k-dimensional grid $[n] \times [n] \times \cdots \times [n]$.

For each $u \in V$, let $N_u = \{u\} \cup \{v \in V \mid uv \in E\}$ denote its closed neighborhood in G. Define polynomials q_u, $u \in V$

$$q_u = \sum_{i=1}^{k} \prod_{v \in \overline{N_u}} (x_i - v)^2.$$

Notice that q_u is nonzero at a grid point $x_i = v_i$, $1 \leq i \leq k$ if and only if there is a $v_i \in N_u$. That is, q_u is nonzero at $(v_1, v_2, \ldots, v_k)$ if and only if some v_i dominates u. Now, letting

$$q_G(x_1, x_2, \ldots, x_k) = \prod_{u=1}^{n} q_u,$$

it follows that q_G is nonzero at a grid point $x_i = v_i$, $1 \leq i \leq k$ if and only if $\{v_1, v_2, \ldots, v_k\}$ is a dominating set for G.

Hence, by Theorem 1.1 we have the following claim which completes the proof. □

Claim 6.1 The polynomial q_G is *not in* the univariate ideal $\langle p_1, p_2, \ldots, p_n\rangle$ if and only if the graph G has a dominating set of size k.

6.1 Proof of Theorem 1.8

We first relate our univariate ideal membership problem with a linear algebraic problem k−LIN-EQ. It turns that k−LIN-EQ problem is more amenable to the MINI[1]-hardness proof. Finally we show a reduction from MINI − 1 − in − 3POSITIVE3 − SAT to k−LIN-EQ to complete the proof.

Definition 6.2 (k-LIN-EQ) *Input:* Integers k, n in unary, a $k \times n$ matrix A with all the entries given in unary and a k dimensional vector $\vec{b}$ with all entries in unary.

Parameter: k.

Question: Does there exist an $\vec{x} \in \{0, 1\}^n$ such that $A\vec{x} = \vec{b}$?

Lemma 6.3 *There is a parameterized reduction from* $k-$Lin-Eq *to the univariate ideal membership problem when the ideal is given by the powers of variables as generators.*

Proof We introduce $2k$ variables $x_1, x_2, \ldots, x_k, y_1, y_2, \ldots, y_k$ where two variables will be used for each row. For each $i \in [n]$, let $\mu_i = \sum_{j=1}^{n} a_{ij}$. For each column $c_i = (a_{1i}, a_{2i}, \ldots, a_{ki})$ we construct the polynomial $P_i = ({y_1}^{a_{1i}} {y_2}^{a_{2i}} \ldots {y_k}^{a_{ki}} + {x_1}^{a_{1i}} {x_2}^{a_{2i}} \ldots {x_k}^{a_{ki}})$. We let $P_A = \prod_{i=1}^{n} P_i$ and we choose the ideal to be $\langle x_1^{b_1+1}, y_1^{\mu_1-b_1+1}, \ldots, x_k^{b_k+1}, y_1^{\mu_k-b_k+1} \rangle$. Notice that P_A has a small arithmetic circuit which is polynomial time computable. □

Claim 6.4 An instance $(A, \vec{b})$ is an YES instance for $k-$Lin-Eq iff $P_A \notin \left\langle x_1^{b_1+1}, y_1^{\mu_1-b_1+1}, \ldots, x_k^{b_k+1}, y_k^{\mu_k-b_k+1} \right\rangle$.

Proof of Claim Suppose $(A, \vec{b})$ is an YES instance. Then there is an $\vec{x} \in \{0,1\}^n$ such that $A\vec{x} = \vec{b}$. Define $S := \{i \in [n] : \vec{x}_i = 1\}$ where $\mathbf{x}_i$ is the ith coordinate of $\vec{x}$. Think of the monomial where ${x_1}^{a_{1i}} {x_2}^{a_{2i}} \ldots {x_k}^{a_{ki}}$ is picked from P_i for each $i \in S$ and ${y_1}^{a_{1i}} {y_2}^{a_{2i}} \ldots {y_k}^{a_{ki}}$ is picked from reaming P_j's where $j \in \bar{S}$. This gives us the monomial $x_1^{b_1} y_1^{\mu_1-b_1} \ldots x_k^{b_k} y_1^{\mu_k-b_k}$ in the polynomial P_A. Thus $P_A \notin \left\langle x_1^{b_1+1}, y_1^{\mu_1-b_1+1}, \ldots, x_k^{b_k+1}, y_k^{\mu_k-b_k+1} \right\rangle$.

Now we show the other direction. Now suppose $P_A \notin \left\langle x_1^{b_1+1}, y_1^{\mu_1-b_1+1}, \ldots, x_k^{b_k+1}, y_k^{\mu_k-b_k+1} \right\rangle$. Let $S := \{i \in [n] : {x_1}^{a_{1i}} {x_2}^{a_{2i}} \ldots {x_k}^{a_{ki}}$ is picked from $P_i\}$. There must be a monomial ${x_1}^{c_1} {x_2}^{c_2} \ldots {x_k}^{c_k} {y_1}^{d_1} {y_2}^{d_2} \ldots {y_k}^{d_k}$ in P_A such that for each i, $\sum_{j \in S} a_{ij} = c_i \leq b_i$, $\sum_{j \notin S} a_{ij} = d_i \leq (\mu_i - b_i)$. As, $\mu_i = \sum_{j \in S} a_{ij} + \sum_{i \notin S} a_{ij}$, we get $b_i \leq \sum_{j \in S} a_{ij}$. Hence, $\sum_{j \in S} a_{ij} = b_i$ for each i. Define $\vec{x} \in \{0,1\}^n$ where $\vec{x}_i = 1$ if $i \in S$ else $\vec{x}_i = 0$. This shows $(A, \vec{b})$ is an YES instance. □

Before we prove the MINI[1]-hardness of $k-$Lin-Eq, we show that the following problem is MINI[1]-hard.

Definition 6.5 MINI $-$ 1 $-$ in $-$ 3POSITIVE3 $-$ SAT

Input: Integers k, n in unary, a 3-SAT instance $\mathcal{E}$ consisting of only positive literals where $\mathcal{E}$ has at most $k \log n$ variables and at most $k \log n$ clauses.

Parameter: k.

Question: Does there exist a satisfiable assignment for $\mathcal{E}$ such that every clause has exactly one iteral?

Claim 6.6 MINI $-$ 1 $-$ in $-$ 3POSITIVE3 $-$ SAT is MINI[1]-hard.

To prove the claim we only need to observe that the standard *Schaefer Reduction* [30] from 3-SAT to 1 $-$ in $-$ 3POSITIVE3 $-$ SAT is in fact a linear size reduction, that directly gives us an FPT reduction from MINI$-$3SAT to MINI $-$ 1 $-$ in $-$ 3POSITIVE3 $-$ SAT.

Proof of Theorem 1.8 Given a $\mathrm{MINI}-1-\mathrm{in}-3\mathrm{POSITIVE}3-\mathrm{SAT}$ instance $\mathcal{E}$, order the variables $v_1, \ldots, v_{k\log n}$ and the clauses $C_1, \ldots, C_{k\log n}$. Construct the following $k\log n \times k\log n$ matrix M where the rows are indexed by the clauses and the columns are indexed by the variables. $M[i][j]$ is set to 1 if v_j appears in C_i, otherwise set it to 0. Make M a $2k\log n \times n$ matrix by adding an all zero row between every rows and appending all zero columns at the end. Now, define $\vec{e}$ as a $2k\log n$ dimensional vector where ith co-ordinate of e, $e_i = 1$ when i is odd and $e_i = 0$ when i is even. We want to find $\vec{y} \in \{0,1\}^n$ such that $M\vec{y} = \vec{e}$.

However this is not an instance of k–LIN-EQ. To make it so, we observe that M is a bit matrix and $\vec{e}$ is a bit vector, hence we can modify them to a $k \times n$ matrix A and k dimensional vector $\vec{b}$ in the following way. For each column j, think of the ith consecutive $2\log n$ bits as the binary expansion of a single entry, call it N and set $A[i][j]$ to N. Similarly, we modify $\vec{e}$ to a k dimensional vector $\vec{b}$ by considering $2\log n$ bits as a binary expansion of a single entry. Now the proof follows from the following claim. □

Claim 6.7 $\mathcal{E}$ is an YES instance for $\mathrm{MINI}-1-\mathrm{in}-3\mathrm{POSITIVE}3-\mathrm{SAT}$ if and only if there exists an $\vec{x} \in \{0,1\}^n$ such that $A\vec{x} = \vec{b}$.

Proof Suppose there is such a satisfiable assignment for $\mathcal{E}$. Define $S := \{j \in [k\log n] \mid v_j = \mathrm{TRUE}\}$. Define $\vec{z} \in \{0,1\}^n$ such that $z_j = 1$ where $j \in S$ else $z_j = 0$. For each i, as C_i contains exactly one iteral, hence $e_{2i+1} = \sum_{j=1}^{n} M[i][j] \cdot z_j = 1$ and $e_{2i} = 0$. Therefore $\vec{z}$ is a solution for $M\vec{y} = \vec{e}$. As every integer has a unique binary expansion, hence $\vec{z}$ is also a solution for $A\vec{x} = \vec{b}$.

Now we prove the other direction. Suppose $A\vec{z} = \vec{b}$ for some $\vec{z} \in \{0,1\}^n$. From the construction of the matrix M, it is sufficient to show that $\vec{z}$ is a satisfying assignment for $M\vec{y} = \vec{e}$. First we note that the numbers $A[i][j], b[i]$ in their binary expansion have bits 1 in the odd location and 0 in the even locations. Let $A[i][j] = \sum_{t=1}^{2\log n} a_{ijt}2^{t-1}$ and $b[i] = \sum_{t=1}^{2\log n} e_t 2^{t-1}$. Since $A\vec{z} = \vec{b}$ we have $\sum_{j=1}^{n} A[i][j] \cdot z_j = b[i]$. This shows that

$$\sum_{j=1}^{n} A[i][j] \cdot z_j = \sum_{j=1}^{n} \left(\sum_{t=1}^{2\log n} a_{ijt} 2^{t-1} \right) \cdot z_j = \sum_{t=1}^{2\log n} \left(\sum_{j=1}^{n} a_{ijt} \cdot z_j \right) 2^{t-1}.$$

Since $\mathcal{E}$ is a 3-CNF formula we have $(\sum_{j=1}^{n} a_{ijt} \cdot z_j) \in \{0,1,2,3\}$. Now we compare $(\sum_{j=1}^{n} a_{ijt} \cdot z_j)$ with the binary expansion of $b[i]$. When t is odd the bit e_t is 1 and so there must be a 1 in the corresponding bit of $(\sum_{j=1}^{n} a_{ijt} \cdot z_j)$. This shows that $(\sum_{j=1}^{n} a_{ijt} \cdot z_j) \neq 0$ when t is odd. Now if $(\sum_{j=1}^{n} a_{ijt} \cdot z_j) \in \{2,3\}$ for any odd t then the term 2^{t+1} will be produced and this will not match the expansion of $b[i]$ as the $e_{t+1} = 0$. Thus by the uniqueness of binary expansion we conclude that $(\sum_{j=1}^{n} a_{ijt} \cdot z_j) = 1$ if t is odd and 0 otherwise. Thus $M\vec{y} = \vec{e}$ has a solution with $y_i = z_i$. □

7 Non-deterministic Algorithm for Univariate Ideal Membership

In this section we prove Theorem 1.9. Given a polynomial $f(X) \in \mathbb{Q}[X]$ and a univariate ideal $I = \langle p_1(x_1), \ldots, p_n(x_n)\rangle$ where the generators are $p_1, \ldots, p_n$ have no repeated roots, we show that deciding nonmembership of f in I is in NP. By Theorem 1.1, it suffices to check in NP if there is a grid point $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ in the n-dimensional grid $Z(p_1) \times Z(p_2) \times \cdots \times Z(p_n)$ where f does not vanish. Since the roots of p_i could be irrational (even complex), it is not immediately clear how to guess a polynomial size witness for such a grid point and efficiently verify. However, we show that for the NP machine it suffices to guess a grid point $\vec{\alpha}$ approximately, upto polynomially many bits of precision. Recall that

$$f(X) = \sum_{i=1}^{n} h_i(X)\; p_i(x_i) + R(X),$$

where the remainder R is unique and $\deg_{x_i}(R) < \deg(p_i)$ for all i. For a polynomial $g \in \mathbb{F}[X]$, let $|c(g)|$ denote be the maximum coefficient (in absolute value) of a monomial in g. We obtain simple estimates for the coefficients of the polynomials $h_1, \ldots, h_n, R$ in terms of n, $\deg(f)$, and the coefficients of f and the p_i.

Lemma 7.1 *Let* $2^{-L} \leq |c(f)|, |c(p_i)| \leq 2^L$. *Then* $2^{-\mathrm{poly}(L,n,d)} \leq |c(h_i)|, |c(R)| \leq 2^{\mathrm{poly}(L,n,d)}$ *where d is the degree upper bound for f, and* $\{p_i : 1 \leq i \leq n\}$.

Proof Write f as a linear combination of at most $\binom{d+n}{n}$ many monomials $f = \sum_m \alpha_m m$. Each monomial m occurring in it is of the form $m = x_1^{e_1} x_2^{e_2} \ldots x_n^{e_n}$, $\sum_i e_i \leq d$. By univariate division, we can write each m as:

$$m = \prod_{i=1}^{n} (h_{m,i}\, p_i + r_{m,i}),$$

where $h_{m,i}, r_{m,i} \in \mathbb{Q}[x_i]$ such that $x^{e_i} = h_{m,i} p_i + r_{m,i}$, and $\deg(r_{m,i}) < \deg(p_i)$. Moreover, by the properties of univariate polynomial division, the absolute value of the coefficients of each $h_{m,i}$ and $r_{m,i}$ lie in an interval of the form $[2^{-\mathrm{poly}(L,n,d)}, 2^{\mathrm{poly}(L,n,d)}]$. We note that $R = \sum_m \prod_{i=1}^n r_{m,i}$, and each h_i is a $2^{\mathrm{poly}(n,d)}$ sum of n-fold products of the $h_{m,i}$ and the p_i. Therefore, the coefficients of R and of each h_i, in absolute value, also lie in an interval of the form $[2^{-\mathrm{poly}(L,n,d)}, 2^{\mathrm{poly}(L,n,d)}]$, as claimed. □

Let $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{C}^n$ be such that $p_i(\alpha_i) = 0$, $1 \leq i \leq n$. By Lemma 2.3, $2^{-\hat{L}} \leq |\alpha_i| \leq 2^{\hat{L}}$ where $\hat{L} = \mathrm{poly}(L, d)$. For each i, let $\tilde{\alpha}_i \in \mathbb{Q}[i]$ be an ϵ-approximation of α_i. That is, $|\alpha_i - \tilde{\alpha}_i| \leq \epsilon$. Let $\tilde{\alpha} = (\tilde{\alpha}_1, \ldots, \tilde{\alpha}_n)$. Then we can bound the absolute value of $p_i(\tilde{\alpha}_i)$ and $\sum_{i=1}^n h_i(\tilde{\alpha}) p_i(\tilde{\alpha})$.

Observation 7.2

- *For* $1 \leq i \leq n$ *we have that* $|p_i(\tilde{\alpha}_i)| \leq \epsilon \cdot 2^{(dL)^c}$.

- $|\sum_{i=1}^n h_i(\tilde{\alpha}) p_i(\tilde{\alpha})| \le \epsilon 2^{(ndL)^c}$.

Here $c > 0$ is a constant that is independent of ϵ.

Proof Let $p_i(x_i) = c \cdot \prod_{j=1}^d (x_i - \beta_{i,j})$. Without loss of generality, suppose $\tilde{\alpha}_i$ ϵ-approximates $\beta_{i,1}$ for each i. Then

$$\begin{aligned} |p_i(\tilde{\alpha}_i)| &\le \epsilon \cdot |c| \cdot \prod_{j=2}^d |\tilde{\alpha}_i - \beta_{i,j}| \\ &\le \epsilon \cdot |c| \cdot \prod_{j=2}^d (|\beta_{i,1} - \beta_{i,j}| + \epsilon) \\ &\le \epsilon \cdot 2^{\text{poly}(d,L)}, \end{aligned}$$

where the last inequality follows from the bound on the distance between the roots of a univariate polynomial shown in Lemma 2.3. For the second part, note that $|\tilde{\alpha}_i| \le |\alpha_i| + 1 \le 2^{\tilde{L}+1}$ by Lemma 2.3. Each h_i has at most $\binom{n+d}{d}$ monomials, and, by Lemma 7.1, the coefficients of each h_i is bounded by $2^{\text{poly}(n,d,L)}$. Putting it together, $|h_i(\tilde{\alpha})| \le 2^{\text{poly}(n,d,L)}$ for all i. Hence, by the first part, $|\sum_{i=1}^n h_i(\tilde{\alpha}) p_i(\tilde{\alpha})| \le \epsilon 2^{(ndL)^{O(1)}}$. □

We now prove Theorem 1.9.

Proof If f is not in the ideal I then, by Theorem 1.1, there exists a grid point $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n) \in Z(p_1) \times \ldots \times Z(p_n)$ such that $R(\vec{\alpha}) \neq 0$.

The NP Machine guesses an ϵ-approximation $\vec{\tilde{\alpha}} = (\tilde{\alpha}_1, \ldots, \tilde{\alpha}_n)$ of $\vec{\alpha}$, where ϵ will be chosen later in the analysis. Using the circuit (or black-box) for f, we obtain the value for $f(\vec{\tilde{\alpha}})$.

Next, we show that the value $|f(\vec{\tilde{\alpha}})|$ distinguishes between the cases $f \in I$ and $f \notin I$.

Case 1 $f \in I$ $|f(\tilde{\alpha})| = |\sum_{i=1}^n h_i(\vec{\tilde{\alpha}}) p_i(\tilde{\alpha_i})| \le \epsilon \cdot 2^{(ndL)^c}$ by Observation 7.2. We can verify this from the value returned by the circuit (or black-box) for f. Note: the inequality may be satisfied even for a $\tilde{\alpha}$ that is not an ϵ-approximation of $\vec{\alpha}$. However, the analysis and choice of ϵ will guarantee correctness.

Case 2 $f \notin I$ We have $f(\tilde{\alpha}) = \sum_{i=1}^n h_i(\tilde{\alpha}) p_i(\tilde{\alpha}) + R(\tilde{\alpha})$. Hence,

$$|f(\tilde{\alpha}) - R(\tilde{\alpha})| \le \epsilon 2^{(ndL)^c}.$$

Our aim is to show that $|f(\tilde{\alpha})| \ge 2\epsilon 2^{(ndL)^c}$. We have from above that $|f(\tilde{\alpha})| \ge R(\tilde{\alpha}) - \epsilon 2^{(ndL)^c}$.

By triangle inequality, $|R(\tilde{\alpha})| \ge |R(\vec{\alpha})| - |R(\tilde{\alpha}) - R(\vec{\alpha})|$. We now show a lower bound on $|R(\vec{\alpha})|$ and an upper bound for $|R(\tilde{\alpha}) - R(\vec{\alpha})|$.

Claim 7.3 $|R(\vec{\alpha})| \ge \frac{1}{2^{(ndL)^{c_1}}}$ for some constant c_1.

Proof Let $\hat{R}(x_n) = R(\alpha_1, \ldots, \alpha_{n-1}, x_n) = a \cdot \prod_{j=1}^{d'}(x_n - \beta_j)$, where a is some nonzero scalar and $d' \leq d$. Note that α_n is not a zero for $\hat{R}(x_n)$. Consider the polynomial $Q(x_n) = p_n(x_n)\hat{R}(x_n)$. The set $\{\alpha_n, \beta_1, \ldots, \beta_{d'}\}$ are roots of $Q(x_n)$ and $\alpha_n \neq \beta_j : 1 \leq j \leq d'$. By the root separation bound of Lemma 2.4 for $|\alpha_n - \beta_j|$, it follows that $|\hat{R}(\alpha_n)| \geq \frac{1}{2^{(ndL)^{c_1}}}$ for some $c_1 > 0$. □

Claim 7.4 $|R(\vec{\tilde{\alpha}}) - R(\vec{\alpha})| \leq \epsilon 2^{(ndL)^{c_2}}$ for some constant c_2.

Proof Define $R^0(\vec{\tilde{\alpha}}) = R(\vec{\alpha})$ and $R^i(\vec{\tilde{\alpha}}) = R(\tilde{\alpha}_1, \ldots, \tilde{\alpha}_i, \alpha_{i+1}, \ldots, \alpha_n)$. By triangle inequality, $|R(\vec{\alpha}) - R(\vec{\tilde{\alpha}})| \leq \sum_{i=1}^{n} |R^{i-1}(\vec{\tilde{\alpha}}) - R^i(\vec{\tilde{\alpha}})|$. Writing explicitly, we have $R^{i-1}(\vec{\tilde{\alpha}}) - R^i(\vec{\tilde{\alpha}}) = \sum_{\vec{e}} c_{\vec{e}} \tilde{\alpha}_1^{e_1} \ldots \tilde{\alpha}_{i-1}^{e_{i-1}}(\alpha_i^{e_i} - \tilde{\alpha}_i^{e_i})\alpha_i^{e_{i+1}} \ldots \alpha_n^{e_n}$. Now, the bounds $|\alpha_i| \leq 2^{(ndL)^{O(1)}}$, and $|\alpha_i - \tilde{\alpha}_i| \leq \epsilon$, combined with the number of summands being bounded by $\binom{d+n}{d}$ implies by triangle inequality that $|R(\vec{\tilde{\alpha}}) - R(\vec{\alpha})| \leq \epsilon \cdot 2^{(ndL)^{c_2}}$ for some constant $c_2 > 0$ (independent of ϵ). □

Combined with the inequalities in Claims 7.3 and 7.4, we have $|f(\vec{\tilde{\alpha}})| \geq \frac{1}{2^{(ndL)^{c_1}}} - \epsilon \cdot \left(2^{(ndL)^{c_2}} + 2^{(ndL)^{c}}\right)$.

To make the calculation precise, let $3M = \frac{1}{2^{(ndL)^{c_1}}}$ and choose ϵ such that $\epsilon \cdot (2^{(ndL)^{c_2}} + 2^{(ndL)^{c}}) \leq M$. We note that the number M can be efficiently pre-computed from the input.

Summarizing the test, notice that $f \in I$ implies that there is a guessed point $\tilde{\alpha}$ of polynomial size such that $|f(\tilde{\alpha})| \leq M$. On the other hand, as argued in Case 2 above, if $f \notin I$ then for any guessed point $\tilde{\alpha}$ we have $|f(\tilde{\alpha})| \geq 2M$. □

Acknowledgements We thank the anonymous reviewers for their useful comments. The third author acknowledges partial support from Infosys Foundation. The fourth author acknowledges partial support from Infosys Foundation and Tata Trust.

References

1. Alon, N.: Combinatorial nullstellensatz. Comb. Probab. Comput. **8**(1–2), 7–29 (1999). http://dl.acm.org/citation.cfm?id=971651.971653
2. Alon, N., Tarsi, M.: A note on graph colorings and graph polynomials. J. Comb. Theory Ser. B. **70**(1), 197–201 (1997). https://doi.org/10.1006/jctb.1997.1753
3. Alon, N., Yuster, R., Zwick, U.: Color-coding. J. ACM **42**(4), 844–856 (1995). https://doi.org/10.1145/210332.210337
4. Kotlov, A., Lovász, L.: The rank and size of graphs. J. Graph Theory **23**(2), 185–189 (1996)
5. Arvind, V., Chatterjee, A., Datta, R., Mukhopadhyay, P.: Fast exact algorithms using Hadamard product of polynomials. arXiv:1807.04496 (2018)
6. Arvind, V., Chatterjee, A., Datta, R., Mukhopadhyay, P.: Univariate ideal membership parameterized by rank degree, and number of generators. In: 38th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science, FSTTCS 2018, December 11-13, 2018, Ahmedabad, India, pp. 7:1–7:18 (2018). https://doi.org/10.4230/LIPIcs.FSTTCS.2018.7
7. Arvind, V., Chatterjee, A., Datta, R., Mukhopadhyay, P.: Efficient black-box identity testing over free group algebra (accepted in RANDOM 2019). arXiv:1904.12337 (2019)
8. Arvind, V., Mukhopadhyay, P.: The ideal membership problem and polynomial identity testing. Inf. Comput. **208**(4), 351–363 (2010). https://doi.org/10.1016/j.ic.2009.06.003

9. Barvinok, A.I.: Two algorithmic results for the traveling salesman problem. Math. Oper. Res. **21**(1), 65–84 (1996). https://doi.org/10.1287/moor.21.1.65
10. Björklund, A., Kaski, P., Kowalik, L.: Constrained multilinear detection and generalized graph motifs. Algorithmica **74**(2), 947–967 (2016). https://doi.org/10.1007/s00453-015-9981-1
11. Brand, C., Dell, H., Husfeldt, T.: Extensor-coding. In: Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA June 25-29, 2018, pp. 151–164 (2018). https://doi.org/10.1145/3188745.3188902
12. Cox, D.A., Little, J., O'Shea, D.: Ideals Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, 3/e (Undergraduate Texts in Mathematics). Springer-Verlag, New York, Inc., Secaucus, NJ USA (2007)
13. Cygan, M., Fomin, FV., Kowalik, L., Lokshtanov, D., Marx, D., Pilipczuk, M., Pilipczuk, M., Saurabh, S.: Parameterized Algorithms. Springer, New York (2015). https://doi.org/10.1007/978-3-319-21275-3
14. Demillo, RA., Lipton, RJ.: A probabilistic remark on algebraic program testing. Inf. Process. Lett. **7**(4), 193–195 (1978). http://www.sciencedirect.com/science/article/pii/0020019078900674, https://doi.org/10.1016/0020-0190(78)90067-4
15. Downey, RG., Estivill-Castro, V., Fellows, M.R., Prieto-Rodriguez, E., Rosamond, FA.: Cutting up is hard to do: the parameterized complexity of k-cut and related problems. Electr. Notes Theor. Comput. Sci. **78**, 209–222 (2003). https://doi.org/10.1016/S1571-0661(04)81014-4
16. Forbes, M., Shpilka, A.: Quasipolynomial-time identity testing of non-commutative and read-once oblivious algebraic branching programs. In: 16th Annual Symposium on Foundations of Computer Science, 09 2012 (1975). https://doi.org/10.1109/FOCS.2013.34
17. Kayal, N.: Algorithms for arithmetic circuits. Electron. Colloq. Comput. Complex. (ECCC) **17**, 73 (2010)
18. Kayal, N., Saxena, N.: Polynomial identity testing for depth 3 circuits. Comput. Complex. **16**(2), 115–138 (2007). https://doi.org/10.1007/s00037-007-0226-9
19. Koiran, P.: Hilbert's nullstellensatz is in the polynomial hierarchy. J. Complex. **12**(4), 273–286 (1996). https://doi.org/10.1006/jcom.1996.0019
20. Kotlov, A.: Rank and chromatic number of a graph. J. Graph Theory **26**(1), 1–8 (1997)
21. Koutis, I.: Faster algebraic algorithms for path and packing problems. In: Automata, Languages and Programming, 35th International Colloquium, ICALP 2008, Reykjavik, Iceland, July 7-11, 2008, Proceedings, Part I: Tack A: Algorithms, Automata, Complexity, and Games, pp. 575–586 (2008). https://doi.org/10.1007/978-3-540-70575-8_47
22. Koutis, I.: Constrained multilinear detection for faster functional motif discovery. Inf. Process. Lett. **112**(22), 889–892 (2012). https://doi.org/10.1016/j.ipl.2012.08.008
23. Koutis, I., Williams, R.: LIMITS and applications of group algebras for parameterized problems. ACM Trans. Algorithm. **12**(3), 31:1–31:18 (2016). https://doi.org/10.1145/2885499
24. Lee, H.: Power sum decompositions of elementary symmetric polynomials. Linear Algebra Appl. **492**(08) (2015)
25. Mahler, K.: An inequality for the discriminant of a polynomial. Mich. Math. J. **09**(3), 257–262 (1964). https://doi.org/10.1307/mmj/1028999140
26. Mayr, E., Meyer, A.: The complexity of word problem for commutative semigroups and polynomial ideals. Adv. Math **46**, 305–329 (1982)
27. Pratt, K.: Faster algorithms via waring decompositions. arXiv:1807.06194 (2018)
28. Saxena, N.: Diagonal circuit identity testing and lower bounds. In: Automata, Languages and Programming, 35th International Colloquium, ICALP 2008, Reykjavik, Iceland, July 7-11, 2008, Proceedings, Part I: Tack A: Algorithms, Automata, Complexity, and Games, pp. 60–71 (2008). https://doi.org/10.1007/978-3-540-70575-8_6
29. Saxena, N., Seshadhri, C.: From sylvester-gallai configurations to rank bounds: Improved blackbox identity test for depth-3 circuits. J. ACM **60**(5), 33:1–33:33 (2013). https://doi.org/10.1145/2528403
30. Schaefer, T.J.: The complexity of satisfiability problems. In: Proceedings of the Tenth Annual ACM Symposium on Theory of Computing, STOC '78, pp. 216–226. ACM, New York, NY USA (1978)
31. Schwartz, J.T.: Fast probabilistic algorithm for verification of polynomial identities. J. ACM. **27**(4), 701–717 (1980)
32. Sudan, M.: Lectures on algebra and computation. Lecture notes 6,12,13,14 (1998)
33. Williams, R.: Finding paths of length k in O*(2^k) time. Inf. Process. Lett. **109**(6), 315–318 (2009). https://doi.org/10.1016/j.ipl.2008.11.004

34. Zippel, R.: Probabilistic algorithms for sparse polynomials. In: Proc. of the Int. Sym. on Symbolic and Algebraic Computation, pp. 216–226 (1979)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Affiliations

V. Arvind[1] · Abhranil Chatterjee[1] · Rajit Datta[2] · Partha Mukhopadhyay[2]

Abhranil Chatterjee
abhranilc@imsc.res.in

Rajit Datta
rajit@cmi.ac.in

Partha Mukhopadhyay
partham@cmi.ac.in

[1] Institute of Mathematical Sciences (HBNI), Chennai, India

[2] Chennai Mathematical Institute, Chennai, India