Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 130 (2014)

Algebraic Geometric Techniques for Depth-4 PIT & Sylvester-Gallai Conjectures for Varieties

Ankit Gupta[*]
Chennai Mathematical Institute
ankitgupta.iitkanpur@gmail.com

Abstract

We present an algebraic-geometric approach for devising a deterministic polynomial time blackbox identity testing (PIT) algorithm for depth-4 circuits with bounded top fanin. Using our approach, we devise such an algorithm for the case when such circuits have bounded bottom fanin and satisfy a certain non-degeneracy condition. In particular, we present an algorithm that, given blackboxes to $P_1 \cdots P_d$, $Q_{11} \cdots Q_{1d_1}$, . . . , $Q_{k1} \cdots Q_{kd_k}$ where k and the degrees of P_i's and Q_{ij}'s are bounded, determines the membership of $P_1 \cdots P_d$ in the radical of the ideal generated by $Q_{11} \cdots Q_{1d_1}$, . . . , $Q_{k1} \cdots Q_{kd_k}$ in deterministic $\mathsf{poly}(n, d, \max_i(d_i))$-time.

We also give a Dvir-Shpilka [DS06]-like approach to resolve the degenerate case and, in the process, initiate a new direction in *incidence geometry for non-linear varieties.* This approach consists of a series of Sylvester-Gallai type conjectures for bounded-degree varieties and, if true, imply a complete derandomization in the bounded bottom fanin case. To the best of our knowledge, these problems have not been posed before.

[*]Research supported by MSR India PhD Fellowship.

ISSN 1433-8092

1 Introduction

Arithmetic Circuits : The most natural and intuitive way to compute a polynomial is via an arithmetic circuit. An arithmetic circuit on inputs $x_1, \ldots, x_n$ and a field $\mathbb{F}$ computes a polynomial in $\mathbb{F}[x_1, \ldots, x_n]$ using only addition(+) and product(×) gates. The complexity measures associated with circuits are size and depth, which respectively capture the number of operations and the maximal distance between an input and the output.

It is well-known that, over any $\mathbb{F}$, "almost all" degree-d polynomials require circuits of size $2^{\tilde{\Omega}(d)}$ (for $d \leq n$). Shockingly, we don't know of even a single such *explicit* polynomial. In 1979, Valiant formalized the notion of explicitness of a polynomial and conjectured that the permanent of an $n \times n$ matrix of inputs is one such hard polynomial [Val79]. Proving a super-polynomial lower bound on the size of arithmetic circuits computing the permanent is the most important problem in arithmetic complexity and is not only considered to be the arithmetic analogue of $\mathsf{P} =? \mathsf{NP}$ but also a stepping stone towards resolving it (as it must necessarily be resolved before resolving $\mathsf{P} =? \mathsf{NP}$ [SV85]).

Polynomial Identity Testing : In blackbox polynomial identity testing (PIT), given only query access to a hidden circuit, one has to determine if it outputs the zero polynomial. This problem has numerous applications and has appeared in many fundamental results in complexity theory. Although this problem exhibits a trivial randomized algorithm, designing an efficient deterministic algorithm is one of the most challenging open problems. Strong equivalence results between derandomizing PIT and proving super-polynomial circuit lower bounds for explicit polynomials are known (cf. Chapter 4 of [SY10]).

Depth-4 Circuits : In a surprising result, Agrawal-Vinay [AV08] showed that a complete derandomization of PIT for just depth-4 ($\Sigma\Pi\Sigma\Pi$) circuits implies an exponential lower bound for general circuits and a near complete derandomization of PIT for general circuits of poly-degree. In fact, in the $\Sigma\Pi\Sigma\Pi$ circuits which they consider the bottom layer of multiplication gates has just $O(\log n)$ fanin[1]. Hence the problem of derandomizing PIT for such fanin restricted depth-4 circuits is equivalent to the general case. Such bottom-fanin restricted $\Sigma\Pi\Sigma\Pi$ circuits have enjoyed a fair amount of limelight in the past couple of years primarily due to a line of work initiated by Gupta et al. [GKKS13a] on proving lower bounds for such circuits. Such circuits also appear as an intermediate step in the recent construction by Gupta et al. [GKKS13b] of the first $n^{O(\sqrt{n})}$-sized depth-3 circuit for computing the determinant of an $n \times n$ matrix of inputs.

From the PIT side also, there has been an incredibly large number of results for $\Sigma\Pi\Sigma\Pi$ circuits with diverse restrictions. A study for the case in which the bottom fan-in of such depth-4 circuits is at most 1 (known as $\Sigma\Pi\Sigma$ circuits) was initiated by Dvir-Shpilka [DS06] (whitebox) and Karnin-Shpilka [KS11] (blackbox). A different study for the case with the restriction of *read-once* was initiated by Shpilka-Volkovich [SV08], the one with the restriction of *multilinearity* was initiated by Karnin et al. [KMSV13] and the one with the restriction of

[1] fanin of a gate is its in-degree.

bounded *transcendence degree* was initiated by Beecken et al. [BMS13]. Recently, Agrawal et al. [ASSS12] reproved all these diverse results using a single unified technique based on the *Jacobian criterion*. In all most all these results, the fanin of the top + gate is assumed to be $O(1)$. For details see the survey by Shpilka-Yehudayoff [SY10] or the one by Saxena [Sax14].

The Model : In this work we consider the model of $\Sigma\Pi\Sigma\Pi(k, r)$ circuits over $\mathbb{C}$, the field of complex numbers. We first define $\Sigma\Pi\Sigma\Pi(k)$ circuits. These are circuits having four alternating layers of + and × gates where the fanin of the top + gate is $\leq k$. Such a circuit C computes a polynomial of the form

$$C(x_1, \ldots, x_n) = \sum_{i=1}^{k} F_i = \sum_{i=1}^{k} \prod_{j=1}^{d_i} Q_{ij} \tag{1}$$

where d_i's are the fanins of the × gates at the second level. Note that if C has size s then every P_{ij} has at most s non-zero monomials. Such polynomials are said to be s-sparse. Degree of C is defined as $\max\{\deg(F_i) : i \in [k]\}$. Also $\gcd(C) := \gcd(F_1, \ldots, F_k)$ and a circuit is said to be *simple* if $\gcd(C) = 1$. It is said to be *minimal* if for every $\emptyset \subsetneq A \subsetneq [k] : \sum_{i \in A} F_i \not\equiv 0$. The polynomial computed by a $\Sigma\Pi\Sigma\Pi(k, r)$ circuit C has the same form as in Equation (1) with an added restriction that the degree of every Q_{ij} is $\leq r$. As Q_{ij}'s can have at most r irreducible factors, we can factor Q_{ij}'s while incurring a multiplicative factor of r in the d_i's. Hence, the polynomial computed by a $\Sigma\Pi\Sigma\Pi(k, r)$ circuit C is of the form

$$C(x_1, \ldots, x_n) = \sum_{i=1}^{k} F_i = \sum_{i=1}^{k} \prod_{j=1}^{d'_i} Q'_{ij} = \gcd(C) \cdot \text{sim}(C) \tag{2}$$

where $\gcd(C)$ is a product of polynomials of degree $\leq r$ and $\text{sim}(C)$ is a simple $\Sigma\Pi\Sigma\Pi(k, r)$ circuit said to be the simple part of C. Note that although Q'_{ij}'s are irreducible they are not necessarily s-sparse. Such a circuit is said to be *homogenous* if all F_i's are homogenous[2] of the same degree (and therefore Q'_{ij}'s are also homogenous).

Having described the problems of proving circuit lower bounds and PIT in arithmetic complexity, we now describe a problem in computational algebraic geometry.

Radical Membership : Before describing the problem of *radical membership* we state some definitions. The *variety* of a set of polynomials $f_1, \ldots, f_k \in \mathbb{F}[x_1, \ldots, x_n]$ is the set of their common zeros in $\mathbb{F}^n$ and is denoted by $V(f_1, \ldots, f_k)$. Formally, $V(f_1, \ldots, f_k) := \{\mathbf{a} \in \mathbb{F}^n : f_1(\mathbf{a}) = \ldots f_k(\mathbf{a}) = 0\}$. The *ideal* generated by $f_1, \ldots, f_k$ is the set $\{\sum_i h_i \cdot f_i : h_1, \ldots, h_k \in \mathbb{F}[x_1, \ldots, x_n]\}$ and is denoted by $\langle f_1, \ldots, f_k \rangle$. The radical $\sqrt{I}$ of an ideal I is the set $\{g \in \mathbb{F}[x_1, \ldots, x_n] : g^e \in I$ for some integer $e \geq 1\}$. One of the most fundamental problems in computational algebraic geometry is the problem of determining if the variety of a given set of polynomials $V(f_1, \ldots, f_k)$ is contained inside the variety $V(g)$ of a given

[2] in a homogenous polynomial the total degree of all non-zero monomials is same.

polynomial g. For $k = \Omega(n)$, even in the case when f_i's have degree ≤ 2 and $g = 1$, this problem is known to be NP-hard [BSS89] and hence we do not expect to have efficient algorithms for this problem - at least not in the case when k is not bounded. When $\mathbb{F} = \mathbb{C}$, Hilbert's Nullstellensatz states that this problem can be reformulated as the problem of *radical membership*. Formally, $V(f_1, \ldots, f_k) \subseteq V(g)$ if and only if $g \in \sqrt{\langle f_1, \ldots, f_k \rangle}$. Hence the above described problem is equivalent to asking if $g \in_? \sqrt{\langle f_1, \ldots, f_k \rangle}$. Similarly, in the problem of *ideal membership* one has to determine if $g \in_? \langle f_1, \ldots, f_k \rangle$. For a quick overview of basic algebraic-geometric definitions and problems see the lecture notes by Sudan [Sud99] and, for more details, the excellent book by Cox, Little and O'Shea [CLO07].

In this work, we consider radical membership for the case when the involved polynomials are a product of homogenous bounded-degree polynomials and give the first deterministic algorithm for this case. We show that (complete statement in Theorem 25)

Theorem (Blackbox Radical Membership)**.** *Let $P := P_1 \cdots P_d$, and for $i = 1, \ldots, k$ let $Q_i := Q_{i1} \cdots Q_{id_i}$ where P_i's and Q_{ij}'s are homogenous in $\mathbb{C}[x_0, \ldots, x_n]$ and have degree $\leq r$. Let d_i's are $\leq d'$. Given blackboxes to P and Q_i's, $P \in_? \sqrt{\langle Q_1, \ldots, Q_k \rangle}$ can be decided in deterministic $\mathsf{poly}(n, d, d')$ time when $k, r = O(1)$.*

Having stated our main result for radical membership, we now describe a concept from incidence geometry which also we would be needing to state our main result for the problem of $\Sigma\Pi\Sigma\Pi(k, r)$ PIT.

Sylvester-Gallai type problems : A well-known theorem in incidence geometry called the Sylvester-Gallai (SG) theorem states that : if there are n distinct points on the real plane s.t., for every pair of distinct points, the line through them also contains a third point, then they all lie on the same line. Over several decades, various variants of this result have been proved and are in general called Sylvester-Gallai type problems. Informally, in such problems, one is presented with a set of objects (points, hyperplanes, etc.) with a lot of "local" dependencies (e.g. two points are collinear with a third) and the goal is to translate these local restrictions to a global bound (usually on the dimension of the space spanned by the objects). Recently, in an impressive work by Barak et al. [BDWY13] a *robust* variant of SG theorem was proved which among other things says that, even if for every point, the above stated restriction holds for a constant fraction of other points, one can still bound the dimension of the vector space spanned by the point set in $\mathbb{C}^d$ by a constant. Few other lines of study for SG type problems include

- replacing lines by higher dimensional vector spaces (initiated by Hansen),
- having multiple sets of (colored) points (initiated by Motzkin-Rabin),
- robust/fractional versions of the above (initiated by Barak et al.).

For an introduction to the SG theorem and its variants see the survey by Borwein-Moser [BM90]. One interesting feature of [BDWY13] is that the robust variant of SG theorem was motivated by a problem in theoretical computer science, in particular the study of (linear) Locally

Correctable Codes (cf. Chapter 5 of Dvir's survey [Dvi12]). We note here that a common feature of *all* these variants is that they only consider flats/vector spaces/linear varieties. We propose a new line of SG theorems for non-linear varieties and pose several variants in spirit of the ones for linear varieties. These problems arise very naturally in our approach for devising PIT algorithms for $\Sigma\Pi\Sigma\Pi(k,r)$ circuits which is also a fundamental problem in theoretical computer science.

SG theorem can be restated in terms of varieties as follows: let $\ell_1,\ldots,\ell_m$ be distinct homogenous linear polynomials in $\mathbb{R}[x_0,\ldots,x_n]$ s.t. for every pair of distinct $\ell_i,\ell_{i'}$ there is a distinct ℓ_j s.t. $V(\ell_i,\ell_{i'})\subseteq V(\ell_j)$. Then dimension of the vector space spanned by all ℓ_k's is ≤ 2.

Dimension of vector space spanned by a set of linear polynomials is a special case of the general concept of transcendence degree of a set of polynomials (denoted as trdeg). For $f_1,\ldots,f_m \in \mathbb{F}[x_1,\ldots,x_n]$, where characteristic of $\mathbb{F}$ is 0, $\mathrm{trdeg}_{\mathbb{F}}\{f_1,\ldots,f_m\}$ equals the rank (over $\mathbb{F}(x_1,\ldots,x_n)$) of their *Jacobian matrix* which is the $m\times n$ matrix whose (i,j)-th entry is $\frac{\partial f_i}{\partial x_j}$.

Having stated the definitions of varieties and the SG theorem, we now define SG-$\Sigma\Pi\Sigma\Pi(k,r)$ circuits and state our main conjecture.

Definition 1 (SG-$\Sigma\Pi\Sigma\Pi(k,r)$ circuit)**.** A simple, minimal, homogenous $\Sigma\Pi\Sigma\Pi(k)$ circuit $C := \sum_{i=1}^k F_i$ as stated in Equation (1) is SG if

$$\forall i \in [k] \;:\; \bigcap_{j\in[k]\setminus\{i\}} V(F_j) \quad\subseteq\quad V(F_i).^{3}$$

Let $C := \sum_{i=1}^k F_i$ be a simple, minimal $\Sigma\Pi\Sigma\Pi(k)$ circuit of degree d. C is SG if its homogenization w.r.t. a new variable x_0 i.e. the circuit $H(C) := \sum_{i=1}^k x_0^d \cdot F_i$ is SG. Note that $H(C)$ is simple and minimal. In general, a $\Sigma\Pi\Sigma\Pi(k,r)$ circuit C is SG if the simple part $\mathrm{sim}(C_{min})$ of its minimal part C_{min} is SG.

Our motivation behind terming such circuits as SG comes from Dvir-Shpilka's idea of using variants of SG theorem for bounding the dimension of the vector space spanned by the linear forms occurring (at the third layer) in such circuits in the case when when the bottom fanin is at most 1 i.e. it is a $\Sigma\Pi\Sigma\Pi(k,1)$ circuit. They also conjectured that, if $\mathbb{F}$ has characteristic 0 then, this dimension is bounded by a function of only k. Indeed later, Kayal-Saraf [KS09] used a colored higher-dimensional variant of SG theorem to prove this conjecture for $\mathbb{R}$. In spirit of Dvir-Shpilka [DS06] we conjecture that in such SG-$\Sigma\Pi\Sigma\Pi(k,r)$ circuits the transcendence degree of the set of Q_{ij}'s is bounded by a function of k,r. This also implies a similar conjecture made in [BMS13]. But in contrast we state a completely geometric conjecture

Conjecture 1. *Let $F_1,\ldots,F_k$ be finite sets of irreducible homogenous polynomials in $\mathbb{C}[x_0,\ldots,x_n]$ of degree $\leq r$ s.t. $\cap_i F_i = \emptyset$ and for every $k-1$ $Q_1,\ldots,Q_{k-1}$, each from a distinct set, there*

[3] varieties are viewed in the projective space.

are $P_1, \ldots, P_c$ in the remaining set s.t. $V(Q_1, \ldots, Q_{k-1}) \subseteq \cup_i V(P_i)$. Then $\mathrm{trdeg}_{\mathbb{C}}(\cup_i F_i) \leq \lambda(k, r, c)$ *for some function λ.*

Over $\mathbb{C}$, by Nullstellensatz, the above condition can be restated as $P_1 \cdots P_c \in \sqrt{\langle Q_1, \ldots, Q_{k-1} \rangle}$. For the case $r = 1$ this conjecture reduces to the case $c = 1$ by the irreducibility of vector spaces and was first proved over $\mathbb{R}$ in [KS09].

We are now ready to state our main result for PIT.

Theorem ($\Sigma\Pi\Sigma\Pi(k, r)$ PIT)**.** *Given blackbox access to the output $f \in \mathbb{C}[x_1, \ldots, x_n]$ of a $\Sigma\Pi\Sigma\Pi(k, r)$ circuit C of degree $\leq d$, $f \equiv_? 0$ can be decided deterministically in time*

1. *$T := d^{O(k)} \cdot (nkD(M''' + 2d))^{O(D)}$ if C is not* SG.
2. *$T + (dn\lambda')^{O(r\lambda')}$ if Conjecture 1 is true ($\lambda' := \lambda(k, r, r^{k-1})$).*

where $\tilde{d} := r^k$, $E := \binom{2(k-1)+1+\tilde{d}\cdot 13r^{2(k-1)+2}}{2(k-1)+1}$, $V := (k-1)\binom{2(k-1)+1+\tilde{d}\cdot 13r^{2(k-1)+2}-r}{2(k-1)+1}$, $D := E \cdot \tilde{d} \cdot 13r^{2(k-1)+2}$ and $M''' := \binom{d}{r^{k-1}} \cdot 2^{E+V}$.

1.1 Comparison with previous work on PIT

As we have already mentioned before, most of the work on $\Sigma\Pi\Sigma\Pi(k, r)$ PIT has been done for the case $r = 1$ ($\Sigma\Pi\Sigma(k)$) and hence here we will focus on the sub-models of $\Sigma\Pi\Sigma\Pi(k)$ circuits which can have $r > 1$. For these, unconditional results are known for very few sub-models. For $k = O(1)$, [KMSV13, SV11] gave $\mathsf{poly}(n, s)$ PIT with the assumptions of multilinearity i.e. F_i's in Equation (1) are such that every variable in every monomial has degree ≤ 1. There are results known for constant-read formulas i.e. every variable appears at most $O(1)$ times (cf. [ASSS12]). In [BMS13], a $\mathsf{poly}(n, s)$ time algorithm was given for $\Sigma\Pi\Sigma\Pi(k)$ circuits with the assumption that the set of Q_{ij}'s in Equation (1) has $O(1)$ transcendence degree. We very gently note here that if one samples $m \leq n$ polynomials of any given degree from a large enough subset of $\mathbb{F}$, w.h.p. they will have transcendence degree exactly m.

As one of our results, we present an unconditional blackbox PIT algorithm for non-SG $\Sigma\Pi\Sigma\Pi(k, r)$ circuits which runs in $\mathsf{poly}(n)$ time when $k, r = O(1)$. In contrast to [BMS13], our algorithm works unconditionally for "most" $\Sigma\Pi\Sigma\Pi(k, r)$ circuits. By this we mean that if one fixes the parameters k, r, d_i's in Equation (1) and samples Q_{ij}'s randomly over any large enough subset of $\mathbb{F}$, one can show that w.h.p., the circuit C will *not* be SG. This can be easily deduced from our proof techniques. Hence, being SG is a degenerate case and our algorithm works unconditionally modulo this degenerate case. This makes our algorithm the best known unconditional result for $\Sigma\Pi\Sigma\Pi(k, r)$ PIT. Moreover our approach goes via radical membership something that has not been studied for devising PIT algorithms before our work. As expected, we introduce new techniques which are build on the concepts used in computational algebraic geometry.

We also pose a geometric conjecture and resolve the SG case conditioned on it. This is a higher-degree colored variant of the SG theorem and is true over $\mathbb{R}$ for the case $r = 1$ [KS09].

Although it is not immediately clear and will be made clear in the forthcoming sections, our conjecture also implies a conjecture made in [BMS13] conditioned on which they too derandomized $\Sigma\Pi\Sigma\Pi(k,r)$ PIT. They conjectured that the transcendence degree of the set of Q_{ij}'s occurring in simple, minimal $\Sigma\Pi\Sigma\Pi(k,r)$ identities is bounded. But, before our work, there wasn't any approach, geometric or algebraic, for resolving the conjecture on simple, minimal $\Sigma\Pi\Sigma\Pi(k,r)$ identities. In contrast to [BMS13], besides posing a conjecture, we also give a geometric approach (in Section 6) for resolving it, the simplest of the conjectures being

Conjecture 2. *Let $Q_1, \ldots, Q_m \in \mathbb{C}[x_0, \ldots, x_n]$ be irreducible and homogenous of degree $\leq r$ s.t. for every pair of distinct Q_i, Q_j there is a distinct Q_k s.t. $V(Q_i, Q_j) \subseteq V(Q_k)$. Then $\mathrm{trdeg}_{\mathbb{C}}\{Q_1, \ldots, Q_m\} \leq \lambda(r)$.*

For the case $r = 1$ the above conjecture is true and is called Kelly's Theorem (as an easier goal one can also start by bounding the co-dimension of $V(Q_1, \ldots, Q_m)$). This conjecture itself proposes a new line of work in incidence geometry viz. SG theorems for non-linear varieties.

1.2 Overview of Techniques

We now give a high level picture of our proof techniques. Suppose we are given blackbox access to a simple, minimal, homogenous $\Sigma\Pi\Sigma\Pi(3,2)$ circuit C of degree $\leq d$ computing a non-zero polynomial $F \in \mathbb{C}[x_0, \ldots, x_n]$:

$$F = F_1 + F_2 + F_3 = \sum_{i=1}^{3} \prod_{j=1}^{d_i} Q_{ij}$$

where degrees of Q_{ij}'s is ≤ 2. Our goal is to efficiently construct a set of points s.t. on at least one of them F doesn't evaluate to 0. If C is not SG then w.l.o.g. say $V(F_1, F_2) \nsubseteq V(F_3)$. As $V(F_i) = \cup_j V(Q_{ij})$ we have that $\cup_{j_1, j_2} V(Q_{1j_1}, Q_{2j_2}) \nsubseteq V(F_3)$. This implies that w.l.o.g. say $V(Q_{11}, Q_{21}) \nsubseteq V(F_3)$. Hence $F_3 \notin \sqrt{\langle Q_{11}, Q_{21} \rangle}$. If we could somehow come up with a linear transformation Φ that maps the variables x_i's to linear polynomials $A_i(y_0, \ldots, y_5)$ respectively but at the same time preserves the non-membership of F_3 in $\sqrt{\langle Q_{11}, Q_{21} \rangle}$, then we claim that $F(A_0, \ldots, A_n) \not\equiv 0$. This is because $F(A_0, \ldots, A_n) \equiv 0$ implies that $F_3(A_0, \ldots, A_n) = -F_1(A_0, \ldots, A_n) - F_2(A_0, \ldots, A_n)$ which, by definition, further implies that $F_3(A_0, \ldots, A_n) \in \sqrt{\langle Q_{11}(A_0, \ldots, A_n), Q_{21}(A_0, \ldots, A_n) \rangle}$, a contradiction. As $F(A_0, \ldots, A_n)$ is a degree $\leq d$ polynomial on 6 variables, its non-zeroness can easily be tested by Schwartz-Zippel lemma.

Hence we are essentially reduced to the problem of coming up with a set of linear transformations that preserves $P_1 \cdots P_d \notin \sqrt{\langle Q_1, Q_2 \rangle}$ where P_i's and Q_i's have degree ≤ 2. By Hilbert's Nullstellensatz, this is equivalent to $V(Q_1, Q_2) \nsubseteq \cup_i V(P_i)$. Now although Q_1 and Q_2 have bounded degree, same is not true for P_i. We claim that this non-membership can be re-written as a set of non-memberships each involving only bounded degree polynomials.

This is because, by Bézout's Theorem, it can be shown that if $V(Q_1, Q_2) \subseteq \cup_i V(P_i)$ then $\exists P_{i_1}, \ldots, P_{i_4}$ among the P_i's s.t. $V(Q_1, Q_2) \subseteq \cup_{j=1}^4 V(P_{i_j})$ (see Claim 11). This would further imply that $P_{i_1} \cdots P_{i_4} \in \sqrt{\langle Q_1, Q_2 \rangle}$. As linear transformation doesn't increase the degree, to preserve $P_1 \cdots P_d \notin \sqrt{\langle Q_1, Q_2 \rangle}$, we just have to preserve it for all size-4 subsets $S \subseteq [d]$. I.e., under Φ, we want to preserve $\prod_{i \in S} P_i \notin \sqrt{\langle Q_1, Q_2 \rangle}$ for all size 4 subsets $S \subseteq [d]$. Now as P_i's themselves have degree ≤ 2 we have that each $\prod_{i \in S} P_i$ has degree ≤ 8.

We are now reduced to a problem of coming up with a set of linear transformations that preserves $Q_3 \notin \sqrt{\langle Q_1, Q_2 \rangle}$ where Q_i's have degree ≤ 8. As Q_1, Q_2 are homogenous, we have that *every* component of $V(Q_1, Q_2)$ has co-dimension ≤ 2. Using this fact, we first show that if one makes a random projection to 6 variables $y_0, \ldots, y_5$ then indeed the non-membership is preserved. This is the most technically challenging part of our proof and requires intricate use of the so called Bertini's (second) Theorem, which is a generalization of Hilbert's Irreducibility Theorem to arbitrary varieties. We then derive an *effective* version of this random radical non-membership-preserving projection by first reducing it to Ideal Membership using a slightly different version of Kollár's effective Nullstellensatz and then using the fact that Ideal Membership is a linear algebraic problem. This allows us to derive degree bounds on the polynomials which must evaluate to a non-zero quantity in our choice of Φ.

Organization : In Section 2 we state our notations, the required preliminaries from identity testing and algebraic geometry. In Section 3 we prove that radical non-membership is preserved under random projections. In Section 4 we give an effective version of the previous statement and present our algorithm for testing radical membership. In Section 5 we prove our main theorem for $\Sigma\Pi\Sigma\Pi(k, r)$ PIT. In Section 6 we present our approach for resolving Conjecture 1. Finally in Section 7 we present our overall program for $\Sigma\Pi\Sigma\Pi(k)$ PIT and conclude.

2 Preliminaries

Notations : $[n] := \{1, 2, \ldots, n\}$, $[0 : n] := \{0, 1, \ldots, n\}$ and, for a finite set S, $\binom{S}{t}$ denotes the set of all subsets of S of size t. Boldfaced letters such as $\mathbf{y}$ shall stand for tuples of variables or field elements. "w.h.p." denotes *with high probability* (with probability $(1 - o(1))$), "s.t." denotes *such that* and "w.l.o.g." denotes *without loss of generality.*

$\mathbb{F}$-irreducibility and absolute irreducibility : A polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$ is said to be $\mathbb{F}$-reducible if there exist nonconstant polynomials $g, h \in \mathbb{F}[x_1, \ldots, x_n]$ such that $f = g \cdot h$. Otherwise f is said to be $\mathbb{F}$-irreducible. If f is $\bar{\mathbb{F}}$-irreducible then it is said to be absolutely irreducible where $\bar{\mathbb{F}}$ is the algebraic closure of $\mathbb{F}$.

Homogeneous Components : A polynomial is *homogeneous* of degree d if every monomial with a non-zero coefficient is of degree d. By collecting together all monomials of the same degree it can be seen that any polynomial f of degree d can be uniquely written as $f = f^{[d]} + f^{[d-1]} + \ldots + f^{[0]}$ where each $f^{[i]}$ is homogeneous of degree i. We call $f^{[i]}$ the *homogeneous component of degree i* of f. A polynomial of degree less than 0 is 0.

2.1 Hitting Sets and Generators

Here we state the notion of generators and hitting sets for a given circuit class. A detailed discussion can be found in [SY10].

Hitting Set : $\mathcal{H} \subseteq \mathbb{C}^N$ is said to be a *hitting set* for a class $\mathcal{C}$ of N-variate polynomials if for every non-zero $f \in \mathcal{C}$, $\exists \hat{a} \in \mathcal{H}$ such that $f(\hat{a}) \neq 0$. We will call $\mathcal{H}$ *explicit* if there is a deterministic algorithm to construct $\mathcal{H}$ in time $\mathsf{poly}(|\mathcal{H}|, N)$.

Generator : A polynomial mapping $\mathcal{G} = (\mathcal{G}_1, \dots, \mathcal{G}_N) : \mathbb{C}^t \mapsto \mathbb{C}^N$ is called a *generator* for a class of polynomials $\mathcal{C}$ if for every non-zero $f \in \mathcal{C}$, $F(\mathcal{G}) \not\equiv 0$.

In PIT both these objects play the same role. The following lemma shows how to interconvert them easily.

Lemma 3 ([SY10] pg. 294)**.** *Given a hitting set $\mathcal{H} \subseteq \mathbb{C}^N$ for a circuit class $\mathcal{C}$, there is a deterministic algorithm that, in time $\mathsf{poly}(|\mathcal{H}|, N)$, constructs a map $\mathcal{G} : \mathbb{C}^t \mapsto \mathbb{C}^N$ with $t = \lceil \log_N |\mathcal{H}| \rceil$ that is a generator for $\mathcal{C}$. Moreover, degrees of $\mathcal{G}_i$'s are $\leq N - 1$.*

In the other direction, let $\mathcal{G} : \mathbb{C}^t \mapsto \mathbb{C}^N$ be a generator for $\mathcal{C}$ and degrees of $\mathcal{G}_i$'s be $\leq r$. If degrees of polynomials in $\mathcal{C}$ is $\leq D$ then for every set $S \subseteq \mathbb{C}$ of size $|S| > rD$ we have that $\mathcal{H} = \mathcal{G}(S^t)$ is a hitting set for $\mathcal{C}$.

In particular, we will be needing hitting sets and generators for the class of polynomials that can be expressed as a product of bounded-degree polynomials .

Low-Degree Polynomials: Let $\mathcal{C}_D$ be the class of all polynomials in $\mathbb{C}[x_1, \dots, x_N]$ of degree $\leq D$. It is well-known that there is an explicit hitting set $\mathcal{H}_D$ for $\mathcal{C}_D$ of size $N^{O(D)}$ (Thm. 10 in [KS01]). From Lemma 3 it follows that there is a generator $\mathcal{G}_D = (\mathcal{G}_1, \dots, \mathcal{G}_n)$ for $\mathcal{C}_D$ with $t = O(D)$ and $\mathcal{G}_i$'s of degree $\leq N - 1$.

Proposition 4. *Let $\mathcal{C}_{D,M}$ be the class of all polynomials in $\mathbb{C}[x_1, \dots, x_N]$ which can be written as a product of at most M polynomials each of degree $\leq D$. There is an explicit hitting set $\mathcal{H}_{D,M}$ for $\mathcal{C}_{D,M}$ of size $(D(N-1)M + 1)^{O(D)}$.*

Proof. Let $f \in \mathcal{C}_{D,M}$ be non-zero and let $f = g_1 \cdots g_l$ for $l \leq M$ where degree of each g_i is $\leq D$. By definition of $\mathcal{G}_D = (\mathcal{G}_1, \dots, \mathcal{G}_n)$, we have that $\forall i \in [r] : g_i(\mathcal{G}_D) \not\equiv 0$. So, $f(\mathcal{G}_D) \not\equiv 0$. As degree of g_i is $\leq D$ and degree of each $\mathcal{G}_j$ is $\leq N - 1$ we have that degree of $g_i(\mathcal{G}_D)$ is $\leq D(N-1)$. Degree of $f(\mathcal{G}_D)$ is at most $D(N-1)l$ and hence at most $D(N-1)M$.

As $f(\mathcal{G}_D)$ is a t-variate polynomial of degree $\leq D(N-1)M$, by a variant of Schwartz-Zippel Lemma (cf. [SY10] pg. 296), $\exists \hat{a} \in [D(N-1)M + 1]^t$ such that $f(\mathcal{G}_D)(\hat{a}) \neq 0$, Hence, $\mathcal{H}_{D,M} := \mathcal{G}_D([D(N-1)M + 1]^t)$ is a hitting set for $\mathcal{C}_{D,M}$. Bound follows from using the fact that $t = O(D)$. □

2.2 Preliminaries from Algebraic Geometry

We now state the definitions and concepts from algebraic geometry that we would be needing in our proofs. A good reference for most of these is [CLO07].

Projective Varieties : A variety is the set of common zeroes of a system of polynomial equations $f_1 = f_2 = \ldots = f_k = 0$ for some f_i's in $\mathbb{F}[x_0, \ldots, x_n]$. If all the f_i's are homogeneous then such a system also corresponds to a *projective variety* wherein two points $\mathbf{x}, \mathbf{y} \in \mathbb{F}^{n+1}$ are considered to be equivalent, denoted $\mathbf{x} \sim \mathbf{y}$, if one is a non-zero scalar multiple of the other. $\mathbb{P}^n(\mathbb{F})$ (simply $\mathbb{P}^n$ for short), called the projective space of dimension n, is the set of all points in $(\mathbb{F}^{n+1} \setminus \{\mathbf{0}\})$ modulo this equivalence relation $\sim$. Unless mentioned otherwise, we will always be dealing with projective varieties over $\mathbb{C}$.

Irreducible Varieties and Minimal Decomposition : If for a variety V, $V = V_1 \cup V_2$ implies $V = V_1$ or $V = V_2$, it is said to be *irreducible*. It is known that any variety $V \subseteq \mathbb{P}^n$ can be decomposed into a union of finite number of irreducible varieties $V_1, V_2, \ldots, V_t$ s.t. $V_i \nsubseteq V_j$ for $i \neq j$, with the varieties V_i's (called the irreducible components of V) being uniquely determined. This is called the *minimal decomposition* of V and t is called the *number of components* of V.

Ideal-Variety Correspondence : Let I be an ideal in $\mathbb{F}[x_1, \ldots, x_n]$. We say I is *radical* if $\sqrt{I} = I$. *Hilbert's Nullstellensatz* shows the correspondence between varieties and radical ideals over $\mathbb{C}$. It states that, over $\mathbb{C}$, $V(f_1, \ldots, f_k) \subseteq V(f)$ if and only if $f \in \sqrt{\langle f_1, \ldots, f_k \rangle}$. It can be easily deduced from this that two distinct radical ideals cannot have the same variety. As every variety is associated to some radical ideal this implies that every variety corresponds to a unique radical ideal (and vice versa). This correspondence will be used implicitly in our proofs.

In particular, there is a one-to-one correspondence between irreducible varieties and *prime* ideals. An ideal I is prime if, $f \cdot g \in I$ implies $f \in I$ or $g \in I$. Over $\mathbb{C}$, by Nullstellensatz it follows that $\sqrt{\langle f_1, \ldots, f_k \rangle}$ is prime if and only if $V(f_1, \ldots, f_k)$ is irreducible. Thus, one can write any radical ideal as an intersection of prime ideals corresponding to the irreducible components of the variety of the radical ideal.

Dimension of a variety : We now examine the dimension of a variety. We shall use the following definition of dimension from the text by Harris [Har92].

Proposition 5 ([Har92], Prop. 11.4)**.** *Dimension of $V \subseteq \mathbb{P}^n$ is the largest k s.t. for every linear subspace Λ of dimension $\geq n - k$ we have $V \cap \Lambda \neq \emptyset$.*

Co-dimension of a variety $V \subseteq \mathbb{P}^n$ (denoted by $\operatorname{codim}(V)$) is defined as $n - \dim(V)$. We collect certain well-known facts about the dimension of projective varieties.

Fact 1. *Let V, W be projective varieties in $\mathbb{P}^n$.*

1. *If $V \subseteq W$ then* $\dim(V) \leq \dim(W)$.
2. $\dim(V \cup W) = \max\{\dim(V), \dim(W)\}$.

3. $\mathrm{codim}(V \cap W) \leq \mathrm{codim}(V) + \mathrm{codim}(W)$ *or equivalently,* $\dim(V \cap W) \geq \dim(V) + \dim(W) - n$.

The following can easily be deduced from Exercise 11.6 in [Har92].

Proposition 6. *For a variety $V \subseteq \mathbb{P}^n$ of co-dimension c and a generic linear subspace*[4] *Λ of co-dimension $\leq n - c - 1$,*

$$\mathrm{codim}(V \cap \Lambda) = \mathrm{codim}(V) + \mathrm{codim}(\Lambda).$$

2.3 Some Algebraic Geometric Facts

Having stated the above definitions, we now state some of their important properties and results on maneuvering these geometric objects.

Proposition 7 (Proposition 9.4.2 in [CLO07])**.** *Let $F \in \mathbb{C}[x_0, \ldots, x_n]$ be non-zero and homogenous. Then in $\mathbb{P}^n$, $\mathrm{codim}(V(F)) = 1$.*

Theorem 8 (Projective Dimension Theorem, Theorem 7.2 in [Har77])**.** *For varieties $V, W \subseteq \mathbb{P}^n$, every irreducible component of $V \cap W$ has co-dimension $\leq \mathrm{codim}(V) + \mathrm{codim}(W)$.*

It is easy to see from the above two properties that, for homogenous F_i's, every component of $V(F_1, \ldots, F_k)$ has co-dimension $\leq k$. This is not true if F_i's are not homogenous as $\mathrm{codim}(V(f, 1-f)) \geq n$. The following decomposition property will be used frequently.

Proposition 9. *Let for each $i \in [k]$, $Q_i := Q_{i1} \cdots Q_{id_i}$ where Q_{ij}'s and $P \in \mathbb{C}[x_0, \ldots, x_n]$.*

$$P \in \sqrt{\langle Q_1, \ldots, Q_k \rangle} \quad \iff \quad \forall (i_1, \ldots, i_k) \in [d_1] \times \ldots \times [d_k] : \ P \in \sqrt{\langle Q_{1i_1}, \ldots, Q_{ki_k} \rangle}.$$

The proof is immediate from the definition of radical of an ideal and the ideal-variety correspondence. The following proposition will be used crucially in our proofs and is one of our main observations.

Proposition 10. *Let $Q_1, \ldots, Q_k \in \mathbb{C}[x_0, \ldots, x_n]$ be homogenous of degree at most r. Then $V(Q_1, \ldots, Q_k)$ has at most r^k irreducible components.*

Proof. The number of irreducible components of a variety is bounded by its *cumulative* degree which is the sum of degrees of all its irreducible components. By Bézout's Theorem, cumulative degree of $V(Q_1, \ldots, Q_k)$ is at most $\prod_i \deg(Q_i)$ (cf. Section 1.1.5 in [Sch07]). □

One can also state the above observation in terms of radical ideals.

Claim 11. *Let $P_1, \ldots, P_d, Q_1, \ldots, Q_k \in \mathbb{C}[x_0, \ldots, x_n]$ be homogenous and degree of each Q_i is at most r. Then,*

$$P_1 \cdots P_d \in \sqrt{\langle Q_1, \ldots, Q_k \rangle} \quad \iff \quad \exists \{i_1, \ldots, i_{r^k}\} \subseteq [d] : \ P_{i_1} \cdots P_{i_{r^k}} \in \sqrt{\langle Q_1, \ldots, Q_k \rangle}.$$

[4] Informally, by a *generic* subspace of co-dimension t one means $V(\ell_1, \ldots, \ell_t)$ where ℓ_i's are linear polynomials with their coefficients chosen randomly from a "sufficiently large" subset of $\mathbb{C}$.

Proof. Let $P_1 \cdots P_d \in \sqrt{\langle Q_1, \ldots, Q_k \rangle}$ and $V_1 \cup \cdots \cup V_t$ be the minimal decomposition of $V(Q_1, \ldots, Q_k)$ where V_i's are irreducible. Then,

$$V_1 \cup \cdots \cup V_t \subseteq V(P_1) \cup \cdots \cup V(P_d).$$

As V_i's are irreducible, we have that for each i there is an $i_j \in [d]$ such that $V_i \subseteq V(P_{i_j})$. Therefore,

$$V(Q_1, \ldots, Q_k) = V_1 \cup \cdots \cup V_t \subseteq V(P_{i_1}) \cup \cdots \cup V(P_{i_t}).$$

By Nullstellensatz, $P_{i_1} \cdots P_{i_t} \in \sqrt{\langle Q_1, \ldots, Q_k \rangle}$. By Proposition 10, $t \leq r^k$ and the claim follows. □

The following corollary follows immediately from Proposition 9 and Claim 11.

Corollary 12. *Let $P_1, \ldots, P_d, Q_{11}, \ldots, Q_{1d_1}, \ldots, Q_{k1}, \ldots, Q_{kd_k} \in \mathbb{C}[x_0, \ldots, x_n]$ be homogenous and degree of each Q_{ij} is at most r. Then, $P_1 \cdots P_d \in \sqrt{\langle Q_{11} \cdots Q_{1d_1}, \ldots, Q_{k1} \cdots Q_{kd_k} \rangle}$ if and only if*

$$\forall \mathbf{i} = (i_1, \ldots, i_k) \in [d_1] \times \ldots \times [d_k] \; \exists S_{\mathbf{i}} \in \binom{[d]}{r^k} \; : \; \prod_{j \in S_{\mathbf{i}}} P_j \in \sqrt{\langle Q_{1i_1}, \ldots, Q_{ki_k} \rangle}.$$

3 Radical Non-membership is preserved under random linear projections

In this section we study the problem of testing membership in the radical of an ideal generated by bounded number of homogenous polynomials and show that radical non-membership is preserved under a random linear transformation of the variable set to a bounded number of variables. We will using the following theorem crucially in our proof.

Theorem 13 (Bertini's (second) Theorem, Corollary 4.18 in [Mum76])**.** *Intersection of an irreducible variety $V \subseteq \mathbb{P}^n$ of dimension c and a generic linear subspace Λ of co-dimension $\leq c - 1$ is irreducible.*

We now prove our main lemma for this section which essentially a geometric version of our above assertion on random linear projections.

Lemma 14. *Let $F, F_1, \ldots, F_k \in \mathbb{C}[x_0, \ldots, x_n]$ be homogenous. Then,*

$$V(F_1, \ldots, F_k) \subseteq V(F) \iff V(F_1, \ldots, F_k) \cap \Lambda \subseteq V(F) \cap \Lambda$$

where Λ is a generic linear subspace of dimension $2k + 1$.

Proof. Let $V := V(F_1, \ldots, F_k)$ and $V_1 \cup \cdots \cup V_t$ be its minimal decomposition. Let $F = P_1^{e_1} \cdots P_d^{e_d}$ where P_i's are distinct irreducible homogenous polynomials over $\mathbb{C}$ and let $H_i := V(P_i)$. Let $V \nsubseteq V(F)$. Then,

$$V_1 \cup \cdots \cup V_t \nsubseteq H_1 \cup \cdots \cup H_d.$$

As V_i's are irreducible, $\exists l \in [t]$ such that $\forall j \in [d] : V_l \nsubseteq H_j$. Using the following proposition we will restate this condition in a quantitative way.

Proposition 15 ([CLO07], Proposition 9.4.10)**.** *For an irreducible variety $V \subseteq \mathbb{P}^n$ and a homogenous $F \in \mathbb{C}[x_1, \ldots, x_n]$,*

1. $V \nsubseteq V(F) \implies \mathrm{codim}(V \cap V(F)) = \mathrm{codim}(V) + 1$
2. *if $W \subset V$ is a variety such that $W \neq V$, then* $\mathrm{codim}(W) > \mathrm{codim}(V)$.

Using Proposition 15, we have that $\forall j \in [d] : \mathrm{codim}(V_l \cap H_j) = \mathrm{codim}(V_l) + 1$. Now, as V is an intersection of k hypersurfaces, from Proposition 7 and Theorem 8, we have that $\mathrm{codim}(V_i) \leq k$ for all i. Moreover, from Proposition 7, $\mathrm{codim}(H_j) = 1$ for all j. From Theorem 8, we have that $\mathrm{codim}(V_i \cap H_j) \leq k + 1$ and $\mathrm{codim}(V_i \cap V_{i'}) \leq 2k$ for all i, j, i'.

Let Λ be a generic linear subspace of dimension $\geq 2k + 1$. From Theorem 13, we have that $V_i \cap \Lambda$ and $H_j \cap \Lambda$ are irreducible for all i, j. We now show that they also satisfy other non-containment conditions. As $V_1 \cup \cdots \cup V_t$ is a minimal decomposition, for any $i \neq i'$, we have that $V_i \nsubseteq V_{i'}$ or, equivalently, $V_i \cap V_{i'} \neq V_i$. From Proposition 15, $\mathrm{codim}(V_i \cap V_{i'}) > \mathrm{codim}(V_i)$. Now as $\mathrm{codim}(V_i \cap V_{i'}) \leq 2k$ and Λ is a generic subspace of co-dimension $\leq n - 2k - 1$, by Proposition 6 we have

$$\mathrm{codim}((V_i \cap \Lambda) \cap (V_{i'} \cap \Lambda)) = \mathrm{codim}((V_i \cap V_{i'}) \cap \Lambda) = \mathrm{codim}(V_i \cap V_{i'}) + \mathrm{codim}(\Lambda).$$

Similarly, $\mathrm{codim}(V_i \cap \Lambda) = \mathrm{codim}(V_i) + \mathrm{codim}(\Lambda)$. As $\mathrm{codim}(V_i \cap V_{i'}) > \mathrm{codim}(V_i)$,

$$\mathrm{codim}((V_i \cap \Lambda) \cap (V_{i'} \cap \Lambda)) > \mathrm{codim}(V_i \cap \Lambda),$$

which implies that $V_i \cap \Lambda \nsubseteq V_{i'} \cap \Lambda$. Similarly, $V_{i'} \cap \Lambda \nsubseteq V_i \cap \Lambda$. Hence, $(V_1 \cap \Lambda) \cup \cdots \cup (V_t \cap \Lambda)$ is the minimal decomposition of $V \cap \Lambda$. Using the same argument, we can also show that $(H_1 \cap \Lambda) \cup \cdots \cup (H_d \cap \Lambda)$ is the minimal decomposition of $V(F) \cap \Lambda$ and that $\mathrm{codim}((V_l \cap \Lambda) \cap (H_j \cap \Lambda)) = \mathrm{codim}(V_l \cap \Lambda) + 1$ for all j. This implies that, for all j,

$$V_l \cap \Lambda \nsubseteq H_j \cap \Lambda,$$

and hence $V \cap \Lambda \nsubseteq V(F) \cap \Lambda$. □

Till now, a generic linear subspace Λ of co-dimension c was defined as $V(L_1, \ldots, L_c)$ where $L_i = \sum_{j \in [0:n]} a_{ij} x_j$ and a_{ij}'s are generic over $\mathbb{C}$. Note that as L_i's are generic, they are also linearly independent, and hence one can always solve $x_0, \ldots, x_{c-1}$ as linear forms in the remaining variables over $\mathbb{C}$ after applying Gaussian elimination. Hence, another sufficient way to define a generic linear subspace Λ of co-dimension c is $V(x_0 - \sum_{j \in [n]} a_{0,j} x_j, \ldots, x_{c-1} - \sum_{j \in [c:n]} a_{c-1,j} x_j)$.

To make this argument more rigorous, we use a slightly different version of Bertini's Theorem by Heintz-Sieveking [HS81], in which a generic linear subspace Λ of co-dimension c is defined as

$$V(x_0 - \sum_{j\in[n]} a_{0,j}x_j, \dots, x_{c-1} - \sum_{j\in[c:n]} a_{c-1,j}x_j)$$

where a_{ij}'s are generic over $\mathbb{C}$. More formally,

Lemma 16 (Heintz-Sieveking, [HS81])**.** *Let I be a prime ideal in $\mathbb{C}[x_0, \dots, x_n]$ and $\dim(V(I)) = c + 1$ (≥ 2). Let a_{ij}'s be transcendental over $\mathbb{C}$ and $\mathbb{K}$ be an algebraically closed field containing $\mathbb{C}$ and a_{ij}'s. Then, the ideal $I + \left\langle x_0 - \sum_{j\in[n]} a_{0,j}x_j, \ \dots \ , x_{c-1} - \sum_{j\in[c:n]} a_{c-1,j}x_j \right\rangle$ is prime in $\mathbb{K}[x_0, \dots, x_n]$.*

Note that in Lemma 16 one can solve $x_0, \dots, x_{c-1}$ as linear forms in the remaining variables where the coefficients are polynomials in a_{ij}'s. An immediate corollary is that

Corollary 17. *Let I be a prime ideal in $\mathbb{C}[x_0, \dots, x_n]$ and $\dim(V(I)) = c + 1$ (≥ 2). Let a_{ij}'s be transcendental over $\mathbb{C}$ and $\mathbb{K}$ be an algebraically closed field containing $\mathbb{C}$ and a_{ij}'s. Then, the ideal $I + \left\langle x_0 - \sum_{j\in[0:n-c]} a_{0,j}y_j, \ \dots \ , x_n - \sum_{j\in[0:n-c]} a_{n,j}y_j \right\rangle$ is prime in $\mathbb{K}[x_0, \dots, x_n, y_0, \dots, y_{n-c}]$.*

For a detailed discussion on Bertini's Theorem and its variants see Section 9.1.3 in [DE05]. Using Corollary 17 we can restate Lemma 14 in form of radical membership.

Lemma 18. *Let $F, F_1, \dots, F_k \in \mathbb{C}[x_0, \dots, x_n]$ be homogenous. Then,*

$$F \in \sqrt{\langle F_1, \dots, F_k\rangle} \quad \iff \quad F(A\mathbf{y}) \in \sqrt{\langle F_1(A\mathbf{y}), \dots, F_k(A\mathbf{y})\rangle}$$

where $F(A\mathbf{y}) := F\left(\sum_{j=0}^{2k+1} a_{0j}y_j, \ \dots \ , \sum_{j=0}^{2k+1} a_{nj}y_j\right)$ and a_{ij}'s are generic in $\mathbb{C}$.[5]

Proof. If $F \notin \sqrt{\langle F_1, \dots, F_k\rangle}$ then, by Nullstellensatz, $V(F_1, \dots, F_k) \not\subseteq V(F)$. From Lemma 14,

$$V(F_1, \dots, F_k) \cap \Lambda \quad \not\subseteq \quad V(F) \cap \Lambda$$

where Λ is a generic linear subspace of dimension $2k+1$. From Corollary 17 (and using the irreducible variety-prime ideal correspondence), one can observe that in Lemma 14 Λ can be defined as $V\left(x_0 - \sum_{j\in[0:2k+1]} a_{0,j}y_j, \ \dots \ , x_n - \sum_{j\in[0:2k+1]} a_{n,j}y_j\right)$ for generic a_{ij}'s. After substituting x_i's in F_i's and F, we get $V(F_1(A\mathbf{y}), \dots, F_k(A\mathbf{y})) \not\subseteq V(F(A\mathbf{y}))$ which implies that $F(A\mathbf{y}) \notin \sqrt{\langle F_1(A\mathbf{y}), \dots, F_k(A\mathbf{y})\rangle}$. □

4 Deterministic Radical Membership Testing

Lemma 18 gives us a very good indication that we are on the right track and that there should be a system of polynomial equations that captures all the "bad" choices of the transforma-

[5] alternatively, a_{ij}'s are transcendental over $\mathbb{C}$.

tions. In this section we indeed derive an effective version of Lemma 18 by characterizing these "bad" transformations. In particular, we prove the following lemma.

Lemma 19 (Non-membership preserving projections)**.** *Let $\tilde{P}, \tilde{Q}_1, \ldots, \tilde{Q}_k \in \mathbb{C}[x_0, \ldots, x_n]$ be homogenous of degrees $\tilde{d}, d_1, \ldots, d_k$ respectively with d_i's $\leq r$. Let $E := \binom{2k+1+\tilde{d}\cdot 13r^{2k+2}}{2k+1}$, $V := k\binom{2k+1+\tilde{d}\cdot 13r^{2k+2}-r}{2k+1}$, $M' := 2^{E+V}$, $D := E \cdot \tilde{d} \cdot 13r^{2k+2}$ and $\mathcal{H}_{D,M'}$ be a hitting set for all polynomials in $\mathbb{C}[a_{0,0}, \ldots, a_{n,2k+1}]$ which are a product of at most M' polynomials each of degree $\leq D$. Then, $\tilde{P} \in \sqrt{\left\langle \tilde{Q}_1, \ldots, \tilde{Q}_k \right\rangle}$ if and only if*

$$\forall (\hat{a}_{0,0}, \ldots, \hat{a}_{n,2k+1}) \in \mathcal{H}_{D,M'} \ : \ \tilde{P}(\hat{A}\mathbf{y}) \in \sqrt{\left\langle \tilde{Q}_1(\hat{A}\mathbf{y}), \ldots, \tilde{Q}_k(\hat{A}\mathbf{y}) \right\rangle}$$

where $\tilde{F}(\hat{A}\mathbf{y}) := \tilde{F}\left(\sum_{j=0}^{2k+1} \hat{a}_{0,j} y_j, \ \ldots \ , \sum_{j=0}^{2k+1} \hat{a}_{n,j} y_j\right)$. Moreover, $\tilde{P} \in_? \sqrt{\left\langle \tilde{Q}_1, \ldots, \tilde{Q}_k \right\rangle}$ can be decided deterministically in time $|\mathcal{H}_{D,M'}| \cdot \mathsf{poly}(V, (nk)^{\tilde{d}\cdot 13r^{2k+2}})$.

But before addressing the radical membership problem, we will first address the Ideal Membership membership problem for homogenous polynomials and derive its linear algebraic formulation. This will be used crucially in the proof of Lemma 19.

4.1 Linear Algebraic Formulation of Ideal Membership

The Ideal Membership problem is defined as follows:

Homogenous Ideal Membership: Given homogenous $P, Q_1, \ldots, Q_k \in \mathbb{C}[y_0, \ldots, y_m]$ of degrees $d, d_1, \ldots, d_k$ respectively decide whether $P \in \langle Q_1, \ldots, Q_k \rangle$.

In this subsection we describe the well-known linear algebraic formulation of this problem. In the case of a homogenous ideal the following proposition provides an immediate bound on the degree of the membership-certifying coefficient polynomials.

Proposition 20. *Let $P, Q_1, \ldots, Q_k \in \mathbb{C}[y_0, \ldots, y_m]$ be homogenous. $P \in \langle Q_1, \ldots, Q_k \rangle$ if and only if $P = \sum_{i \in [k]} R_i Q_i$ for some homogenous $R_1, \ldots, R_k \in \mathbb{C}[y_0, \ldots, y_m]$ where, for each i, $\deg(R_i) = \deg(P) - \deg(Q_i)$.*

Proof. If $P \in \langle Q_1, \ldots, Q_k \rangle$ then, for some $f_1, \ldots, f_k \in \mathbb{C}[y_0, \ldots, y_m]$, $P = \sum_{i \in [k]} f_i Q_i$. As P is homogenous, it equals $\left(\sum_{i \in [k]} f_i Q_i\right)^{[\deg(P)]}$ which equals $\sum_{i \in [k]} (f_i Q_i)^{[\deg(P)]}$. As Q_i is homogenous, $(f_i Q_i)^{[\deg(P)]} = Q_i \cdot f_i^{[\deg(P) - \deg(Q_i)]}$ and the assertion follows. □

From Proposition 20 it follows that the Homogenous Ideal Membership, as described above, is equivalent to deciding if there are homogenous $R_1, \ldots, R_k \in \mathbb{C}[y_0, \ldots, y_m]$ of degree $d - d_i$ respectively such that $P = \sum_{i \in [k]} R_i Q_i$. W.l.o.g. we can now assume that d_i's are $\leq d$. Let

$D_{m,d} := \{\bar{\alpha} = (\alpha_1, \ldots, \alpha_m) \in \mathbb{Z}^m_{\geq 0} \ : \ \sum_i \alpha_i = d\}$ and $\bar{y}^{\bar{\alpha}} := \prod_i y_i^{\alpha_i}$. Let a degree-$d$ homogenous polynomial $F \in \mathbb{C}[y_0, \ldots, y_m]$ be denoted as $\sum_{\bar{\alpha} \in D_{m,d}} f_{\bar{\alpha}}.\bar{y}^{\bar{\alpha}}$. Then we have,

$$\sum_{\bar{\alpha} \in D_{m,d}} p_{\bar{\alpha}}.\bar{y}^{\bar{\alpha}} \ = \ \sum_{i \in [k]} \left(\sum_{\bar{\beta} \in D_{m,d-d_i}} r_{i,\bar{\beta}}.\bar{y}^{\bar{\beta}} \right) \cdot \left(\sum_{\bar{\delta} \in D_{m,d_i}} q_{i,\bar{\delta}}.\bar{y}^{\bar{\delta}} \right) .$$

Comparing the coefficient of $\bar{y}^{\bar{\alpha}}$ on both sides we get

$$\forall \bar{\alpha} \in D_{m,d} \ : \quad p_{\bar{\alpha}} \ = \ \sum_{i \in [k]} \sum_{\bar{\beta} \leq \bar{\alpha}} r_{i,\bar{\beta}}.q_{i,\bar{\alpha}-\bar{\beta}} \tag{3}$$

where $\bar{\beta} \leq \bar{\alpha}$ denotes that $\forall j \in [0 : m], \ \beta_j \leq \alpha_j$. This is a system of linear equations in $r_{i,\bar{\beta}}$'s with $E := \binom{m+d}{d}$ equations and $V := \sum_{i \in [k]} \binom{m+d-d_i}{d-d_i}$ variables. Let the linear system (3) be denoted as $M_{\bar{q}} \cdot \bar{r} = \bar{p}$ where $M_{\bar{q}}$ is a $E \times V$-matrix with every element as either 0 or a coefficient in some Q_i, and $\bar{p}$ is a $E \times 1$-vector with every element as some coefficient in P. Hence, the Ideal Membership problem is equivalent to deciding if this system has a non-trivial solution over $\mathbb{C}$ or not. The following theorem gives an exact characterization of the existence of such a solution.

Theorem 21 (Rouché-Capelli Theorem)**.** *Over $\mathbb{C}$, a system of linear equations $M \cdot \bar{r} = \bar{p}$ has a non-trivial solution if and only if* $\mathrm{rank}(M) = \mathrm{rank}((M|\bar{p}))$.

It follows from the above theorem that $P \in \langle Q_1, \ldots, Q_k \rangle$ if and only if, in the linear system 3,

$$\mathrm{rank}(M_{\bar{q}}) = \mathrm{rank}((M_{\bar{q}}|\bar{p})).$$

Note that, given $P, Q_1, \ldots, Q_k$ explicitly, one can construct $(M_{\bar{q}}|\bar{p})$ in time $\mathsf{poly}(E \cdot V)$ and compute its rank in time $\mathsf{poly}(E \cdot V)$ using Gaussian elimination. Hence, we can determine $P \in_? \langle Q_1, \ldots, Q_k \rangle$ deterministically in time $\mathsf{poly}(E \cdot V)$. From the above discussion the following lemma follows.

Lemma 22 (Linear System for Ideal Membership)**.** *Let $P, Q_1, \ldots, Q_k \in \mathbb{C}[y_0, \ldots, y_m]$ be homogenous of degrees $d, d_1, \ldots, d_k$ respectively with d_i's $\leq d$. Let $E := \binom{m+d}{d}$ and $V := \sum_{i \in [k]} \binom{m+d-d_i}{d-d_i}$. There exists a $E \times V$-matrix $M_{\bar{q}}$ with every element as either 0 or a coefficient in some Q_i, and a $E \times 1$-vector $\bar{p}$ with every element as some coefficient in P, such that*

$$P \in \langle Q_1, \ldots, Q_k \rangle \quad \iff \quad \mathrm{rank}(M_{\bar{q}}) = \mathrm{rank}((M_{\bar{q}}|\bar{p})).$$

Moreover, given $P, Q_1, \ldots, Q_k$ explicitly, $P \in_? \langle Q_1, \ldots, Q_k \rangle$ can be determined deterministically in time $\mathsf{poly}(E \cdot V)$.

4.2 Radical Membership to Ideal Membership : Proof of Lemma 19

We now return to the proof of Lemma 19 as restated below.

Lemma (Lemma 19 restated)**.** *Let $\tilde{P}, \tilde{Q}_1, \ldots, \tilde{Q}_k \in \mathbb{C}[x_0, \ldots, x_n]$ be homogenous of degrees $\tilde{d}, d_1, \ldots, d_k$ respectively with d_i's $\leq r$. Let $E := \binom{2k+1+\tilde{d}\cdot 13r^{2k+2}}{2k+1}$, $V := k\binom{2k+1+\tilde{d}\cdot 13r^{2k+2}-r}{2k+1}$, $M' := 2^{E+V}$, $D := E \cdot \tilde{d} \cdot 13r^{2k+2}$ and $\mathcal{H}_{D,M'}$ be a hitting set for all polynomials in $\mathbb{C}[a_{0,0}, \ldots, a_{n,2k+1}]$ which are a product of at most M' polynomials each of degree $\leq D$. Then, $\tilde{P} \in \sqrt{\left\langle \tilde{Q}_1, \ldots, \tilde{Q}_k \right\rangle}$ if and only if*

$$\forall (\hat{a}_{0,0}, \ldots, \hat{a}_{n,2k+1}) \in \mathcal{H}_{D,M'} \;\;:\;\; \tilde{P}(\hat{A}\mathbf{y}) \in \sqrt{\left\langle \tilde{Q}_1(\hat{A}\mathbf{y}), \ldots, \tilde{Q}_k(\hat{A}\mathbf{y}) \right\rangle}$$

where $\tilde{F}(\hat{A}\mathbf{y}) := \tilde{F}\left(\sum_{j=0}^{2k+1} \hat{a}_{0,j} y_j, \;\ldots\; , \sum_{j=0}^{2k+1} \hat{a}_{n,j} y_j\right)$. Moreover, $\tilde{P} \in_? \sqrt{\left\langle \tilde{Q}_1, \ldots, \tilde{Q}_k \right\rangle}$ can be decided deterministically in time $|\mathcal{H}_{D,M'}| \cdot \mathsf{poly}(V, (nk)^{\tilde{d}\cdot 13r^{2k+2}})$.

Proof. We first state the radical membership problem -

Homogenous Low-Degree Radical Membership: Let $\tilde{P}, \tilde{Q}_1, \ldots, \tilde{Q}_k \in \mathbb{C}[x_0, \ldots, x_n]$ be homogenous of degrees $\tilde{d}, d_1, \ldots, d_k$ respectively with d_i's $\leq r$. Decide if $\tilde{P} \in \sqrt{\left\langle \tilde{Q}_1, \ldots, \tilde{Q}_k \right\rangle}$.

As noted earlier we are interested in the setting in which $k << n$. So we can reduce the number of variables involved using a random projection as stated in Lemma 18. From Lemma 18 we have,

$$\tilde{P} \in \sqrt{\left\langle \tilde{Q}_1, \ldots, \tilde{Q}_k \right\rangle} \quad \Longleftrightarrow \quad \tilde{P}(A\mathbf{y}) \in \sqrt{\left\langle \tilde{Q}_1(A\mathbf{y}), \ldots, \tilde{Q}_k(A\mathbf{y}) \right\rangle}$$

where $\tilde{F}(A\mathbf{y}) := \tilde{F}\left(\sum_{j=0}^{2k+1} a_{0j} y_j, \;\ldots\; , \sum_{j=0}^{2k+1} a_{nj} y_j\right)$ and a_{ij}'s are generic in $\mathbb{C}$. [6]

Note that, as $\tilde{Q}_i(A\mathbf{y})$ is just a linear projection of $\tilde{Q}_i$, $\deg(\tilde{Q}_i(A\mathbf{y})) \leq \deg(\tilde{Q}_i) \leq r$. Now, using the following version of the *effective* Nullstellensatz, in our setting, we will be effectively able to reduce Radical Membership to Ideal Membership. Although the best bound is due to Kollár [Kol88], we use Dubé's bound for its somewhat simpler statement which is better suited to our case.

Theorem 23 (Dubé, Theorem 7.1 in [Dub93])**.** *Let $P, Q_1, \ldots, Q_k \in \mathbb{C}[y_0, \ldots, y_m]$ and degree of each Q_i is at most r. Then,*

$$P \in \sqrt{\langle Q_1, \ldots, Q_k \rangle} \quad \Longleftrightarrow \quad P^{13r^{m+1}} \in \langle Q_1, \ldots, Q_k \rangle \,.$$

[6] alternatively, a_{ij}'s are transcendental over $\mathbb{C}$.

From Theorem 23, it follows that

$$\tilde{P} \in \sqrt{\left\langle \tilde{Q}_1, \ldots, \tilde{Q}_k \right\rangle} \quad \Longleftrightarrow \quad (\tilde{P}(A\mathbf{y}))^{13r^{2k+2}} \in \left\langle \tilde{Q}_1(A\mathbf{y}), \ldots, \tilde{Q}_k(A\mathbf{y}) \right\rangle .$$

Note that every $\tilde{Q}_i(A\mathbf{y}) \in \mathbb{C}[y_0, \ldots, y_{2k+1}]$ is a homogenous polynomial where the coefficient of every monomial is a polynomial in a_{ij}'s of degree at most r. Similarly, $(\tilde{P}(A\mathbf{y}))^{13r^{2k+2}} \in \mathbb{C}[y_0, \ldots, y_{2k+1}]$ is a homogenous polynomial where the coefficient of every monomial is a polynomial in a_{ij}'s of degree at most $\tilde{d} \cdot 13r^{2k+2}$. Let $E := \binom{2k+1+\tilde{d}\cdot 13r^{2k+2}}{2k+1}$ and $V := k\binom{2k+1+\tilde{d}\cdot 13r^{2k+2}-r}{2k+1}$. From Lemma 22, there exists a $E \times V$-matrix $M_{\bar{q}}$ with every element as either 0 or a coefficient in some $\tilde{Q}_i(A\mathbf{y})$, and a $E \times 1$-vector $\bar{p}$ with every element as some coefficient in $(\tilde{P}(A\mathbf{y}))^{13r^{2k+2}}$, such that

$$(\tilde{P}(A\mathbf{y}))^{13r^{2k+2}} \in \left\langle \tilde{Q}_1(A\mathbf{y}), \ldots, \tilde{Q}_k(A\mathbf{y}) \right\rangle \quad \Longleftrightarrow \quad \operatorname{rank}(M_{\bar{q}}) = \operatorname{rank}((M_{\bar{q}}|\bar{p})).$$

Now, $(M_{\bar{q}}|\bar{p})$ is a $E \times (V+1)$-matrix such that every entry is a polynomial in $\mathbb{C}[a_{0,0}, \ldots, a_{n,2k+1}]$ of degree at most $\tilde{d} \cdot 13r^{2k+2}$. Moreover,

$$\text{for a generic choice of } a_{ij}\text{'s in } \mathbb{C} : \quad \tilde{P} \in \sqrt{\left\langle \tilde{Q}_1, \ldots, \tilde{Q}_k \right\rangle} \Longleftrightarrow \operatorname{rank}_{\mathbb{C}}(M_{\bar{q}}) = \operatorname{rank}_{\mathbb{C}}((M_{\bar{q}}|\bar{p})).$$

Equivalently, viewing $a_{0,0}, \ldots, a_{n,2k+1}$ as transcendental quantities over $\mathbb{C}$ and viewing the matrix $(M_{\bar{q}}|\bar{p})$ as a matrix over $\mathbb{C}(a_{0,0}, \ldots, a_{n,2k+1})$, we have

$$\tilde{P} \in \sqrt{\left\langle \tilde{Q}_1, \ldots, \tilde{Q}_k \right\rangle} \quad \Longleftrightarrow \quad \operatorname{rank}_{\mathbb{C}(a_{0,0},\ldots,a_{n,2k+1})}((M_{\bar{q}}|\bar{p})) = \operatorname{rank}_{\mathbb{C}(a_{0,0},\ldots,a_{n,2k+1})}(M_{\bar{q}}).$$

Therefore, in the case when $\tilde{P} \notin \sqrt{\left\langle \tilde{Q}_1, \ldots, \tilde{Q}_k \right\rangle}$, from the above assertion, we have that

$$\operatorname{rank}_{\mathbb{C}(a_{0,0},\ldots,a_{n,2k+1})}((M_{\bar{q}}|\bar{p})) = \operatorname{rank}_{\mathbb{C}(a_{0,0},\ldots,a_{n,2k+1})}(M_{\bar{q}}) + 1.$$

Moreover, it is easy to see that any choice of a_{ij}'s in $\mathbb{C}$ that preserves this rank relation over $\mathbb{C}$, also preserves radical non-membership. We now show how to find this substitution efficiently.

Note that as $E \leq V$, the $\operatorname{rank}((M_{\bar{q}}|\bar{p}))$ is at most E. Let $\mathcal{M}_{\leq E}((M_{\bar{q}}|\bar{p}))$ be the set of all minors of $(M_{\bar{q}}|\bar{p})$ of size at most E, i.e.

$$\mathcal{M}_{\leq E}((M_{\bar{q}}|\bar{p})) := \{t \times t \text{ minor of } (M_{\bar{q}}|\bar{p}) \ , \ t \leq E\}.$$

As every entry of $(M_{\bar{q}}|\bar{p})$ is a polynomial in $\mathbb{C}[a_{0,0}, \ldots, a_{n,2k+1}]$ of degree at most $\tilde{d} \cdot 13r^{2k+2}$ we have that $\mathcal{M}_{\leq E}((M_{\bar{q}}|\bar{p}))$ is a set of at most $M' := 2^{E+V}$ polynomials of degree at most

$D := E \cdot \tilde{d} \cdot 13r^{2k+2}$. Let, the product of all non-zero polynomials in $\mathcal{M}_{\leq E}((M_{\bar{q}}|\bar{p}))$ be the non-zero polynomial $G \in \mathbb{C}[a_{0,0}, \ldots, a_{n,2k+1}]$.

Recall that $\mathcal{H}_{D,M'} \subseteq \mathbb{C}^{(2k+2)(n+1)}$ is such that for every such non-zero $G \in \mathbb{C}[a_{0,0}, \ldots, a_{n,2k+1}]$

$$\exists(\hat{a}_{0,0}, \ldots, \hat{a}_{n,2k+1}) \in \mathcal{H}_{D,M'} \ : \ G(\hat{a}_{0,0}, \ldots, \hat{a}_{n,2k+1}) \neq 0.$$

It follows from the definition of $\mathcal{H}_{D,M'}$ that $\exists(\hat{a}_{0,0}, \ldots, \hat{a}_{n,2k+1}) \in \mathcal{H}_{D,M'}$ s.t. $G(\hat{a}_{0,0}, \ldots, \hat{a}_{n,2k+1}) \neq 0$. Then, we have that the rank of every sub-matrix of $(M_{\bar{q}}|\bar{p})$ over $\mathbb{C}(a_{0,0}, \ldots, a_{n,2k+1})$ is preserved under the substitution of $a_{i,j}$'s with $\hat{a}_{i,j}$'s and therefore

$$\text{rank}_{\mathbb{C}(a_{0,0},\ldots,a_{n,2k+1})}((M_{\bar{q}}|\bar{p})) = \text{rank}_{\mathbb{C}(a_{0,0},\ldots,a_{n,2k+1})}(M_{\bar{q}}) \iff \text{rank}_{\mathbb{C}}((M_{\bar{q}}|\bar{p})) = \text{rank}_{\mathbb{C}}(M_{\bar{q}})$$

after choosing $(a_{0,0}, \ldots, a_{n,2k+1})$ to be $(\hat{a}_{0,0}, \ldots, \hat{a}_{n,2k+1})$, thus preserving the (non-)membership of $\tilde{P}$ in $\sqrt{\left\langle \tilde{Q}_1, \ldots, \tilde{Q}_k \right\rangle}$.

Time Complexity : Note that at any fixed $(a_{0,0}, \ldots, a_{n,2k+1})$, the coefficients of $(\tilde{P}(A\mathbf{y}))^{13r^{2k+2}}$, $\tilde{Q}_1(A\mathbf{y}), \ldots, \tilde{Q}_k(A\mathbf{y})$ can be determined in time $\mathsf{poly}((nk)^{\tilde{d}\cdot 13r^{2k+2}})$ and the matrix $(M_{\bar{q}}|\bar{p})$ can be formed in time $\mathsf{poly}(V)$. Similarly, $\text{rank}_{\mathbb{C}}((M_{\bar{q}}|\bar{p}))$ and $\text{rank}_{\mathbb{C}}(M_{\bar{q}})$ can be determined in time $\mathsf{poly}(V)$ using Gaussian elimination. Therefore, the relation $\text{rank}_{\mathbb{C}}((M_{\bar{q}}|\bar{p})) = \text{rank}_{\mathbb{C}}(M_{\bar{q}})$ can be verified in time $\mathsf{poly}(V, (nk)^{\tilde{d}\cdot 13r^{2k+3}})$. Hence, radical membership can be determined in deterministic time $|\mathcal{H}_{D,M'}| \cdot \mathsf{poly}(V, (nk)^{\tilde{d}\cdot 13r^{2k+2}})$. □

4.3 Deterministic Radical Membership

Being armed with Lemma 19, in this subsection, we finally present our algorithms for radical membership. We first consider a whitebox version in which the factors are given explicitly as it highlights the main approach for the blackbox case and is easier to understand.

Theorem 24 (Deterministic Whitebox Radical Membership)**.** *Let $P := P_1 \cdots P_d$ and, for each $i \in [k]$, $Q_i := Q_{i1} \cdots Q_{id_i}$ where P_i's are homogenous of degree $\leq r_1$ and Q_{ij}'s are homogenous of degree $\leq r$ in $\mathbb{C}[x_0, \ldots, x_n]$. Given P_i's and Q_{ij}'s,*

$$P_1 \cdots P_d \in_? \sqrt{\langle Q_{11} \cdots Q_{1d_1}, \ldots, Q_{k1} \cdots Q_{kd_k} \rangle}$$

can be decided deterministically in time $d_1 \cdots d_k \cdot \binom{d}{r^k} \cdot (nkDM')^{O(D)} \cdot \mathsf{poly}(V, (nk)^{\tilde{d}\cdot 13r^{2k+2}})$ where $\tilde{d} = r_1 \cdot r^k$, $E := \binom{2k+1+\tilde{d}\cdot 13r^{2k+2}}{2k+1}$, $V := k\binom{2k+1+\tilde{d}\cdot 13r^{2k+2}-r}{2k+1}$, $M' := 2^{E+V}$ and $D := E \cdot \tilde{d} \cdot 13r^{2k+2}$.

Proof. From Corollary 12, $P \in \sqrt{\langle Q_1, \ldots, Q_k \rangle}$ if and only if

$$\forall \mathbf{i} = (i_1, \ldots, i_k) \in [d_1] \times \ldots \times [d_k] \ \exists S_{\mathbf{i}} \in \binom{[d]}{r^k} \ : \ \prod_{j \in S_{\mathbf{i}}} P_j \in \sqrt{\langle Q_{1i_1}, \ldots, Q_{ki_k} \rangle}.$$

By iterating over all $d_1 \cdots d_k$ $\mathbf{i} \in [d_1] \times \ldots \times [d_k]$ and all $\binom{d}{r^k}$ $S_{\mathbf{i}} \in \binom{[d]}{r^k}$ one can check if

$$\prod_{j \in S_{\mathbf{i}}} P_j \in_? \sqrt{\langle Q_{1i_1}, \ldots, Q_{ki_k} \rangle}.$$

Note that degree of $\prod_{j \in S} P_j$ is $\leq \tilde{d} := r_1 \cdot r^k$. Hence, from Lemma 19 we have that for $E := \binom{2k+1+\tilde{d} \cdot 13r^{2k+2}}{2k+1}$, $V := k\binom{2k+1+\tilde{d} \cdot 13r^{2k+2}-r}{2k+1}$, $M' := 2^{E+V}$ and $D := E \cdot \tilde{d} \cdot 13r^{2k+2}$, $\prod_{j \in S_{\mathbf{i}}} P_j \in_? \sqrt{\langle Q_{1i_1}, \ldots, Q_{ki_k} \rangle}$ can be decided deterministically in time $|\mathcal{H}_{D,M'}| \cdot \mathsf{poly}(V, (nk)^{\tilde{d} \cdot 13r^{2k+2}})$ where $\mathcal{H}_{D,M'}$ is as defined in Proposition 4. From Proposition 4, $|\mathcal{H}_{D,M'}| = (nkDM')^{O(D)}$. □

We now present our algorithm for the blackbox case. The main step is to construct an explicit set of projections s.t. on at least one of them the non-membership is maintained. Once we are reduced to the case of bounded number of variables, we can simply interpolate and check for radical non-membership explicitly as described previously.

Theorem 25 (Deterministic Blackbox Radical Membership)**.** *Let $P := P_1 \cdots P_d$ and, for each $i \in [k]$, $Q_i := Q_{i1} \cdots Q_{id_i}$ where P_i's are homogenous of degree $\leq r_1$ and Q_{ij}'s are homogenous of degree $\leq r$ in $\mathbb{C}[x_0, \ldots, x_n]$. Given blackbox access to P and Q_i's,*

$$P_1 \cdots P_d \in_? \sqrt{\langle Q_{11} \cdots Q_{1d_1}, \ldots, Q_{k1} \cdots Q_{kd_k} \rangle}$$

can be decided deterministically in time

$$(nkDM'')^{O(D)} \cdot \left\{ (r_1 \cdot d)^{O(k)} + k(r \cdot d_{max})^{O(k)} + (dr_1 \cdot 13(r \cdot d_{max})^{2k+2})^{O(k)} + \mathsf{poly}(\tilde{E} \cdot \tilde{V}) \right\}$$

where $\tilde{d} = r_1 \cdot r^k$, $E := \binom{2k+1+\tilde{d} \cdot 13r^{2k+2}}{2k+1}$, $V := k\binom{2k+1+\tilde{d} \cdot 13r^{2k+2}-r}{2k+1}$, $M'' := \binom{d}{r^k} \cdot 2^{E+V}$, $D := E \cdot \tilde{d} \cdot 13r^{2k+2}$, $d_{max} := \max\{d_1, \ldots, d_k\}$, $\tilde{\tilde{d}} := dr_1 \cdot 13(r \cdot d_{max})^{2k+2}$, $\tilde{E} := \binom{2k+1+\tilde{\tilde{d}}}{2k+1}$ and $\tilde{V} := k\binom{2k+1+\tilde{\tilde{d}}}{2k+1}$.

Proof. **Step 1:** Suppose $P \notin \sqrt{\langle Q_1, \ldots, Q_k \rangle}$. From Proposition 9, $P \notin \sqrt{\langle Q_1, \ldots, Q_k \rangle}$ if and only if $\exists (i_1, \ldots, i_k) \in [d_1] \times \ldots \times [d_k]$ s.t. $P \notin \sqrt{\langle Q_{1i_1}, \ldots, Q_{ki_k} \rangle}$. W.l.o.g. let $P \notin \sqrt{\langle Q_{11}, \ldots, Q_{k1} \rangle}$. From Claim 11,

$$\forall S \in \binom{[d]}{r^k} \; : \; \prod_{j \in S} P_j \notin \sqrt{\langle Q_{11}, \ldots, Q_{k1} \rangle}.$$

Note that for any fixed $S \in \binom{[d]}{r^k}$, degree of $\prod_{j \in S} P_j$ is $\leq \tilde{d} := r_1 \cdot r^k$. Hence, from Lemma 19 we have that for $E := \binom{2k+1+\tilde{d} \cdot 13r^{2k+2}}{2k+1}$, $V := k\binom{2k+1+\tilde{d} \cdot 13r^{2k+2}-r}{2k+1}$, $M' := 2^{E+V}$ and $D := E \cdot \tilde{d} \cdot 13r^{2k+2}$

$$\exists (\hat{a}_{0,0}, \ldots, \hat{a}_{n,2k+1}) \in \mathcal{H}_{D,M'} \; : \; \prod_{j \in S} P_j(\hat{A}\mathbf{y}) \notin \sqrt{\left\langle Q_{11}(\hat{A}\mathbf{y}), \ldots, Q_{k1}(\hat{A}\mathbf{y}) \right\rangle}.$$

where $F(\hat{A}\mathbf{y}) := F\left(\sum_{j=0}^{2k+1} \hat{a}_{0,j}y_j,\ \ldots\ ,\sum_{j=0}^{2k+1} \hat{a}_{n,j}y_j\right)$ and $\mathcal{H}_{D,M'}$ is as defined in Proposition 4. As there are $\binom{d}{r^k}$ choices of S, from the definition of $\mathcal{H}_{D,M'}$ and proof of Lemma 19, it follows that for $E := \binom{2k+1+\tilde{d}\cdot 13r^{2k+2}}{2k+1}$, $V := k\binom{2k+1+\tilde{d}\cdot 13r^{2k+2}-r}{2k+1}$, $M'' := \binom{d}{r^k}\cdot M'$ and $D := E\cdot\tilde{d}\cdot 13r^{2k+2}$

$$\exists(\hat{a}_{0,0},\ldots,\hat{a}_{n,2k+1}) \in \mathcal{H}_{D,M''}\ :\ \forall S \in \binom{[d]}{r^k}\ :\ \prod_{j\in S} P_j(\hat{A}\mathbf{y}) \notin \sqrt{\left\langle Q_{11}(\hat{A}\mathbf{y}),\ldots,Q_{k1}(\hat{A}\mathbf{y})\right\rangle}.$$

As degrees of $Q_{ij}(\hat{A}\mathbf{y})$'s is $\le r$, from Claim 11 we have $P(\hat{A}\mathbf{y}) \notin \sqrt{\left\langle Q_{11}(\hat{A}\mathbf{y}),\ldots,Q_{k1}(\hat{A}\mathbf{y})\right\rangle}$ and hence $P(\hat{A}\mathbf{y}) \notin \sqrt{\left\langle Q_1(\hat{A}\mathbf{y}),\ldots,Q_k(\hat{A}\mathbf{y})\right\rangle}$. From Proposition 4, $|\mathcal{H}_{D,M''}| = (nkDM'')^{O(D)}$ and hence such a $\hat{A}$ can be guessed in $(nkDM'')^{O(D)}$ iterations.

Step 2: As $P(\hat{A}\mathbf{y})$ is a $(2k+2)$-variate polynomial of degree $\le dr_1$, it can be interpolated deterministically from its blackbox using the Klivans-Spielman interpolation (Theorem 26) in time $(dr_1)^{O(k)}$.

Theorem 26 (Sparse Interpolation [KS01])**.** *Given blackbox access to $g \in \mathbb{C}[y_0,\ldots,y_m]$ of degree $\le \delta$ and having at most s non-zero monomials, the non-zero monomials of g along with their respective coefficients can be determined deterministically in* $\mathsf{poly}(m,\delta,s)$ *time.*

Similarly, $Q_i(\hat{A}\mathbf{y})$'s can be interpolated in time $k(r\cdot d_{max})^{O(k)}$.

Step 3: We now describe how to determine if $P(\hat{A}\mathbf{y}) \in_? \sqrt{\left\langle Q_1(\hat{A}\mathbf{y}),\ldots,Q_k(\hat{A}\mathbf{y})\right\rangle}$. Let for any polynomial F, $\tilde{F} := F(\hat{A}\mathbf{y})$. As $\tilde{Q}_i$'s are $(2k+2)$-variate polynomials of degree $\le r\cdot d_{max}$, from Theorem 23

$$\tilde{P} \in \sqrt{\left\langle \tilde{Q}_1,\ldots,\tilde{Q}_k\right\rangle} \quad\iff\quad \tilde{P}^{13(r\cdot d_{max})^{2k+2}} \in \left\langle \tilde{Q}_1,\ldots,\tilde{Q}_k\right\rangle.$$

Let $\tilde{\tilde{P}} := \tilde{P}^{13(r\cdot d_{max})^{2k+2}}$. We have that degree of $\tilde{\tilde{P}}$ is $\le \tilde{\tilde{d}} := dr_1\cdot 13(r\cdot d_{max})^{2k+2}$ and hence it can be computed from $\tilde{P}$ in time $(dr_1\cdot 13(r\cdot d_{max})^{2k+2})^{O(k)}$ by straightforward unfolding.

Let $\tilde{E} := \binom{2k+1+\tilde{\tilde{d}}}{2k+1}$ and $\tilde{V} := k\binom{2k+1+\tilde{\tilde{d}}}{2k+1}$. From Lemma 22, $\tilde{\tilde{P}} \in_? \left\langle \tilde{Q}_1,\ldots,\tilde{Q}_k\right\rangle$ can be reduced to determining the consistency of a linear system of size at most $\tilde{E}\times\tilde{V}$. This can be determined deterministically in time at most $\mathsf{poly}(\tilde{E}\cdot\tilde{V})$. □

5 PIT for $\Sigma\Pi\Sigma\Pi(k,r)$ Circuits

Having described our main result on radical membership, in this section we prove our main theorem on blackbox PIT for $\Sigma\Pi\Sigma\Pi(k,r)$ circuits. The algorithm will have two stages. The first one covers the case of non SG circuits and will essentially be on the lines of the earlier described blackbox radical membership. The second stage covers the case of SG circuits and is conditioned on Conjecture 1 under which the transcendence degree of the simple part of such a circuit is bounded. In this situation we will simply use the result by [BMS13, ASSS12] for constructing a hitting set.

Theorem 27. *Given blackbox access to the output $f \in \mathbb{C}[x_1,\ldots,x_n]$ of a $\Sigma\Pi\Sigma\Pi(k,r)$ circuit C of degree $\le d$, $f \equiv_? 0$ can be decided deterministically in time*

1. *$T := d^{O(k)} \cdot (nkD(M''' + 2d))^{O(D)}$ if C is not* SG.
2. *$T + (dn\lambda')^{O(r\lambda')}$ if Conjecture 1 is true ($\lambda' := \lambda(k,r,r^{k-1})$).*

where $\tilde{d} := r^k$, $E := \binom{2(k-1)+1+\tilde{d}\cdot 13r^{2(k-1)+2}}{2(k-1)+1}$, $V := (k-1)\binom{2(k-1)+1+\tilde{d}\cdot 13r^{2(k-1)+2}-r}{2(k-1)+1}$, $D := E \cdot \tilde{d} \cdot 13r^{2(k-1)+2}$ and $M''' := \binom{d}{r^{k-1}} \cdot 2^{E+V}$.

Proof. Let $f \not\equiv 0$. As we are in the blackbox case we can w.l.o.g. assume that C is minimal (otherwise we can eliminate a few gates to make it minimal). We are given that $f(x_1,\ldots,x_n) = \sum_{i=1}^{k} F_i = \gcd(C)\cdot \mathrm{sim}(C)$ where $\gcd(C)$ is a product of at most d polynomials of degree $\le r$ and $\mathrm{sim}(C)$ is a simple, minimal $\Sigma\Pi\Sigma\Pi(k,r)$ circuit.

Homogenization : We first homogenize the circuit C w.r.t. a new variable x_0 by obtaining blackbox to $F := x_0^d \cdot f(\frac{x_1}{x_0},\ldots,\frac{x_n}{x_0})$ which clearly is 0 iff f is 0. Then, we have that

$$F = G \cdot H(\mathrm{sim}(C))$$

where $H(\mathrm{sim}(C))$ is a simple minimal homogenous $\Sigma\Pi\Sigma\Pi(k,r)$ circuit and G is a product of at most $2d$ homogenous polynomials of degree $\le r$. Moreover, by definition of SG-$\Sigma\Pi\Sigma\Pi(k,r)$ circuits, $\mathrm{sim}(C)$ is SG iff $H(\mathrm{sim}(C))$ is SG. Also, degree of $H(\mathrm{sim}(C))$ is $\le d$. Let

$$F = G \cdot (H(\mathrm{sim}(C))) = G \cdot \left(\sum_{i=1}^{k} Q_i\right) = G \cdot \left(\sum_{i=1}^{k}\prod_{j=1}^{d_i} Q_{ij}\right) \tag{4}$$

where d_i's are $\le d$ and Q_{ij}'s are irreducible and homogenous of degree $\le r$.

Proof of part (1.) : C **is not SG**
Therefore, $H(\mathrm{sim}(C))$ is not SG. W.l.o.g. $V(Q_1,\ldots,Q_{k-1}) \nsubseteq V(Q_k)$. This implies that w.l.o.g. $V(Q_{1,1},\ldots,Q_{k-1,1}) \nsubseteq V(Q_k)$. By Hilbert's Nullstellensatz $Q_k \notin \sqrt{\langle Q_{1,1},\ldots,Q_{k-1,1}\rangle}$. From Claim 11,

$$\forall S \in \binom{[d_k]}{r^{k-1}} \;:\; \prod_{j\in S} Q_{k,j} \notin \sqrt{\langle Q_{1,1},\ldots,Q_{k-1,1}\rangle}.$$

Note that for any fixed $S \in \binom{[d_k]}{r^{k-1}}$, degree of $\prod_{j \in S} Q_{k,j}$ is $\leq \tilde{d} := r \cdot r^{k-1}$.

Non-membership preserving projection : Hence, from Lemma 19 we have that for $E := \binom{2(k-1)+1+\tilde{d}\cdot 13r^{2(k-1)+2}}{2(k-1)+1}$, $V := (k-1)\binom{2(k-1)+1+\tilde{d}\cdot 13r^{2(k-1)+2}-r}{2(k-1)+1}$, $M' := 2^{E+V}$ and $D := E \cdot \tilde{d} \cdot 13r^{2(k-1)+2}$

$$\exists(\hat{a}_{0,0}, \ldots, \hat{a}_{n,2(k-1)+1}) \in \mathcal{H}_{D,M'} \ : \ \prod_{j \in S} Q_{k,j}(\hat{A}\mathbf{y}) \notin \sqrt{\left\langle Q_{1,1}(\hat{A}\mathbf{y}), \ldots, Q_{k-1,1}(\hat{A}\mathbf{y}) \right\rangle}.$$

where $P(\hat{A}\mathbf{y}) := P\left(\sum_{j=0}^{2(k-1)+1} \hat{a}_{0,j}y_j, \ \ldots \ , \sum_{j=0}^{2(k-1)+1} \hat{a}_{n,j}y_j\right)$ and $\mathcal{H}_{D,M'}$ is as defined in Proposition 4. As there are $\binom{d_k}{r^{k-1}}$ choices of S, from the definition of $\mathcal{H}_{D,M'}$ and proof of Lemma 19, it follows that for $E := \binom{2(k-1)+1+\tilde{d}\cdot 13r^{2(k-1)+2}}{2(k-1)+1}$, $V := (k-1)\binom{2(k-1)+1+\tilde{d}\cdot 13r^{2(k-1)+2}-r}{2(k-1)+1}$, $M'' := \binom{d_k}{r^{k-1}} \cdot M'$ and $D := E \cdot \tilde{d} \cdot 13r^{2(k-1)+2}$

$$\exists(\hat{a}_{0,0}, \ldots, \hat{a}_{n,2(k-1)+1}) \in \mathcal{H}_{D,M''} \ : \ \forall S \in \binom{[d_k]}{r^{k-1}} \ : \ \prod_{j \in S} Q_{k,j}(\hat{A}\mathbf{y}) \notin \sqrt{\left\langle Q_{1,1}(\hat{A}\mathbf{y}), \ldots, Q_{k-1,1}(\hat{A}\mathbf{y}) \right\rangle}.$$

As degrees of $Q_{ij}(\hat{A}\mathbf{y})$'s is $\leq r$, from Claim 11 we have $Q_k(\hat{A}\mathbf{y}) \notin \sqrt{\left\langle Q_{1,1}(\hat{A}\mathbf{y}), \ldots, Q_{k-1,1}(\hat{A}\mathbf{y}) \right\rangle}$ and hence, from Proposition 9, $Q_k(\hat{A}\mathbf{y}) \notin \sqrt{\left\langle Q_1(\hat{A}\mathbf{y}), \ldots, Q_{k-1}(\hat{A}\mathbf{y}) \right\rangle}$. This further implies that $Q_k(\hat{A}\mathbf{y}) \notin \left\langle Q_1(\hat{A}\mathbf{y}), \ldots, Q_{k-1}(\hat{A}\mathbf{y}) \right\rangle$ which in turn implies that $Q_k(\hat{A}\mathbf{y}) \neq -\sum_{i \in [k-1]} Q_i(\hat{A}\mathbf{y})$ and hence $H(\mathrm{sim}(C))(\hat{A}\mathbf{y}) \not\equiv 0$. As Q_k was chosen arbitrarily among the Q_i's and every d_i is $\leq d$ this argument works in general if $\hat{A}$ it chosen from $\mathcal{H}_{D,M'''}$ where $M''' := \binom{d}{r^{k-1}} \cdot M'$.

Moreover, as G is a product of at most $2d$ homogenous polynomials of degree $\leq r \leq D$, for $M'''' = M''' + 2d$, $\exists \hat{A} \in \mathcal{H}_{D,M''''}$ s.t. $H(\mathrm{sim}(C))(\hat{A}\mathbf{y}) \not\equiv 0$ and $G(\hat{A}\mathbf{y}) \not\equiv 0$, which in turn implies $F(\hat{A}\mathbf{y}) \not\equiv 0$. From Proposition 4, $|\mathcal{H}_{D,M''''}| = (nkDM'''')^{O(D)}$ and hence such a $\hat{A}$ can be guessed in $(nkDM'''')^{O(D)}$ iterations.

Klivans-Spielman : Moreover, for any choice of $\hat{A}$, as $F(\hat{A}\mathbf{y})$ is a $2k$-variate polynomial of degree $\leq d$, its non-zeroness can be determined from its blackbox using the Klivans-Spielman interpolation (Theorem 26) in deterministic time $d^{O(k)}$.

Time Complexity : $\hat{A}$ can be guessed in $(nkDM'''')^{O(D)}$ iterations and in each iteration Klivans-Spielman algorithm takes $d^{O(k)}$ time. Total time taken is $d^{O(k)} \cdot (nkD(M'''+2d))^{O(D)}$.

To summarize, if the condition of part (1.) was satisfied i.e. $\mathrm{sim}(C)$ was not SG and $f \not\equiv 0$ then the above algorithm would have correctly determined its non-zeroness. This completes our proof for part (1.) of the theorem.

Proof of part (2.) : If we are not given the guarantee of part (1.) then we are in the general $\Sigma\Pi\Sigma\Pi(k, r)$ case. We first run the algorithm described above for the case when $\mathrm{sim}(C)$ is not

SG. From proof of part (1.) if sim(C) was not SG then we would have already determined the non-zeroness of F. Therefore we need to run one more step to cover the case when sim(C) is SG.

sim(C) **is SG :** This implies that $H(\text{sim}(C))$ in Equation (4) is SG. By following the first few steps in *Proof of part (1.)*, negating the assertions for Q_{ij}'s and using Ideal-Variety correspondence one can easily deduce the k sets $\mathcal{Q}_i := \{Q_{i1}, \ldots, Q_{id_i}\}$ are sets of irreducible homogenous polynomials in $\mathbb{C}[x_0, \ldots, x_n]$ of degree $\leq r$ s.t. $\cap_i \mathcal{Q}_i = \emptyset$ and for every $k-1$ $Q_1, \ldots, Q_{k-1}$, each from a distinct set, there are $P_1, \ldots, P_{r^{k-1}}$ in the remaining set s.t. $V(Q_1, \ldots, Q_{k-1}) \subseteq \cup_i V(P_i)$. If Conjecture 1 is true then $\text{trdeg}_{\mathbb{C}}\{Q_{11}, Q_{12}, \ldots, Q_{kd_k}\} \leq \lambda' := \lambda(k, r, r^{k-1})$. We now use a result by Beecken et al. [BMS13, ASSS12].

Theorem 28 (implicit in [BMS13, ASSS12])**.** *Let $f_1, \ldots, f_m \in \mathbb{C}[x_0, \ldots, x_n]$ have degree $\leq r$ and $\text{trdeg}_{\mathbb{C}} \leq \lambda$. Let $\mathcal{G} = (\mathcal{G}_1, \ldots, \mathcal{G}_n)$ be the generator for the class of degree $\leq r\lambda$ polynomials in $\mathbb{C}[x_0, \ldots, x_n]$. Let C be a m-variate circuit over $\mathbb{C}$ s.t. $C(f_1, \ldots, f_m) \not\equiv 0$. Let $\Phi : x_i \mapsto \mathcal{G}_i + \sum_{j=0}^{\lambda} y_i \cdot w^{ij}$ where y_i's and w are new variables. Then, $C(\Phi(f_1), \ldots, \Phi(f_m)) \not\equiv 0$.*

As $\text{trdeg}_{\mathbb{C}}\{Q_{11}, Q_{12}, \ldots, Q_{kd_k}\} \leq \lambda'$ and each factor of G has degree $\leq r$, from Theorem 28, map Φ preserves non-zeroness of $G \cdot H(\text{sim}(C))$. From Lemma 3, $\mathcal{G}_i$ are degree n polynomials on $t = O(r\lambda')$ variables $z_1, \ldots, z_t$. After the substitution we get a non-zero polynomial on $O(r\lambda')$ variables of degree $O(dn\lambda')$. Hence by Lemma 3 a hitting set can be generated in time $(dn\lambda')^{O(r\lambda')}$.

Time Complexity : The time required is the time taken in part (1.) + $(dn\lambda')^{O(r\lambda')}$. □

6 Sylvester-Gallai Conjectures for Varieties

We now give a series of conjectures leading to our main conjecture under which we derandomize PIT for $\Sigma\Pi\Sigma\Pi(k, r)$ circuits.

1. Kelly's Theorem

Conjecture 29. *Let $Q_1, \ldots, Q_m \in \mathbb{C}[x_0, \ldots, x_n]$ be irreducible and homogenous of degree $\leq r$ s.t. for every pair of distinct Q_i, Q_j there is a distinct Q_k s.t. $V(Q_i, Q_j) \subseteq V(Q_k)$. Then $\text{trdeg}_{\mathbb{C}}\{Q_1, \ldots, Q_m\} \leq \lambda(r)$.*

Over $\mathbb{C}$, by Nullstellensatz, the above condition can be restated as $Q_k \in \sqrt{\langle Q_i, Q_j \rangle}$. For the case $r = 1$ the above conjecture is true and is called Kelly's Theorem.

2. Edelstein-Kelly Theorem

Conjecture 30. *Let R, B, G be finite sets of irreducible homogenous polynomials in $\mathbb{C}[x_0, \ldots, x_n]$ of degree $\leq r$ s.t. $R \cap B \cap G = \emptyset$ and for every pair of Q, Q' from distinct sets there is a Q'' in the remaining set s.t. $V(Q, Q') \subseteq V(Q'')$. Then $\text{trdeg}_{\mathbb{C}}(R \cup B \cup G) \leq \lambda(r)$.*

Over $\mathbb{C}$, by Nullstellensatz, the above condition can be restated as $Q'' \in \sqrt{\langle Q, Q' \rangle}$. For the case $r = 1$ the above conjecture is true over $\mathbb{R}$ and was proved by Edelstein and Kelly.

We also need the following generalization of this conjecture to k colors.

Conjecture 31. *Let $F_1, \ldots, F_k$ be finite sets of irreducible homogenous polynomials in $\mathbb{C}[x_0, \ldots, x_n]$ of degree $\leq r$ s.t. $\cap_i F_i = \emptyset$ and for every $k-1$ $Q_1, \ldots, Q_{k-1}$'s, each from a distinct set, there is a Q_k in the remaining set s.t. $V(Q_1, \ldots, Q_{k-1}) \subseteq V(Q_k)$. Then $\operatorname{trdeg}_{\mathbb{C}}(\cup_i F_i) \leq \lambda(k, r)$.*

Over $\mathbb{C}$, by Nullstellensatz, the above condition can be restated as $Q_k \in \sqrt{\langle Q_1, \ldots, Q_{k-1} \rangle}$. For the case $r = 1$ the above conjecture is true over $\mathbb{R}$ and was first proved in [KS09].

3. Robust version of Conjecture 31

Conjecture 32. *Let $F_1, \ldots, F_k$ be finite sets of irreducible homogenous polynomials in $\mathbb{C}[x_0, \ldots, x_n]$ of degree $\leq r$ s.t. $\cap_i F_i = \emptyset$ and for every $k-1$ $Q_1, \ldots, Q_{k-1}$, each from a distinct set, there are $P_1, \ldots, P_c$ in the remaining set s.t. $V(Q_1, \ldots, Q_{k-1}) \subseteq \cup_i V(P_i)$. Then $\operatorname{trdeg}_{\mathbb{C}}(\cup_i F_i) \leq \lambda(k, r, c)$.*

Over $\mathbb{C}$, by Nullstellensatz, the above condition can be restated as $P_1 \cdots P_c \in \sqrt{\langle Q_1, \ldots, Q_{k-1} \rangle}$. For the case $r = 1$ this conjecture reduces to the case $c = 1$ by the irreducibility of vector spaces. We note that our notion of *robustness* is different from that in [BDWY13].

4. Sparse versions of the above conjectures

We conjecture that the above conjectures also hold for d-degree s-sparse polynomials with λ being a function of $\log_n d, \log_n s$ (and k). For e.g. the corresponding sparse version of Conjecture 29 is

Conjecture 33. *Let $S_1, \ldots, S_m \in \mathbb{C}[x_0, \ldots, x_n]$ be irreducible, homogenous, s-sparse polynomials of degree $\leq d$ s.t. for every pair of distinct S_i, S_j there is a distinct S_k s.t. $V(S_i, S_j) \subseteq V(S_k)$. Then $\operatorname{trdeg}_{\mathbb{C}}\{S_1, \ldots, S_m\} \leq \lambda(\log_n d, \log_n s)$.*

Although its unclear at this point if it would be helpful or not but one can also start by proving the above mentioned bounds for the co-dimension of the variety of the respective polynomial set. E.g. by proving that $\operatorname{codim}(V(Q_1, \ldots, Q_m)) \leq \lambda(r)$ instead of proving the bound on trdeg. Of course, this wouldn't imply the bound on trdeg as for e.g. $\operatorname{codim}(V(yx_1, \ldots, yx_t)) = 1$ but $\operatorname{trdeg}(\{yx_1, \ldots, yx_t\}) = t$. For bounding trdeg one must bound the co-dimension of every component of $V(Q_1, \ldots, Q_m)$.

We also conjecture that these conjectures also hold over $\mathbb{R}$ (the varieties are also taken in $\mathbb{P}^n(\mathbb{R})$) and hence one may also start by proving these over $\mathbb{R}$.

We strongly note here that although we present the above conjectures in form of a series leading to the one we require for derandomizing $\Sigma\Pi\Sigma\Pi(k, r)$ PIT, this theme by no means is limited to PIT and one can very well study other higher degree variants of the already proved SG theorems, e.g. the quantitative SG theorems of [BDWY13].

7 Approach for $\Sigma\Pi\Sigma\Pi(k)$ circuits

In this section we state our overall approach for $\Sigma\Pi\Sigma\Pi(k)$ PIT. Note that we have already used the same approach to prove Theorem 27. Our approach is as follows

1. Sparse Irreducibility Testing

Problem 1 (Sparse Irreducibility Testing)**.** *Let $S \in \mathbb{C}[x_0, \ldots, x_n]$ be s-sparse and of degree $\leq d$. Decide if S is reducible over $\mathbb{C}$ in deterministic $\mathsf{poly}(n, s, d)$ time.*

2. Generic Case : Sparse Radical Membership

Problem 2 (Sparse Radical Membership)**.** *Let $P_1, \ldots, P_D, S_1, \ldots, S_k \in \mathbb{C}[x_0, \ldots, x_n]$ be homogenous s-sparse of degrees $\leq d$ and $k = O(1)$. Decide in deterministic $\mathsf{poly}(n, s, d, D)$ time if $P_1 \cdots P_D \in_? \sqrt{\langle S_1, \ldots, S_k \rangle}$.*

This would essentially solve $\Sigma\Pi\Sigma\Pi(k)$ PIT in the generic case leaving only the degenerate case of SG circuits. Currently, we do not even have a solution to this problem even for the case when $k = D = 1$.

3. Degenerate Case : SG type theorems Prove the SG type conjectures for sparse polynomials as stated in Section 6. Although we actually need to prove these for factors of sparse polynomials, proving the conjectures for sparse polynomials would be a substantial progress.

Conclusion

In this paper we presented new techniques for the problem of radical membership in computational algebraic geometry, PIT in arithmetic complexity, and in the process, proposed a new line of problems in incidence geometry. For PIT, we considered the model of $\Sigma\Pi\Sigma\Pi(r, k)$ circuits and presented an algorithm for it modulo a conjecture on the transcendence degree of a set of varieties which have a lot of local dependencies. Moreover, our algorithm works unconditionally for "most" $\Sigma\Pi\Sigma\Pi(k, r)$ circuits. Although it is undeniable that PIT for $\Sigma\Pi\Sigma\Pi(k)$ circuits might very well have other approaches and algorithms, for us the motivation was to devise an approach which in the process also makes progress on other existing fundamental problems in computational algebraic geometry. We conclude by highlighting the two frontiers of our approach :

1. Prove/disprove Conjecture 29.
2. Solve Problem 1 on sparse irreducibility testing.

Acknowledgements

I thank MSR Outreach group and Satya Lokam for hosting me at MSR India where a major part of this work was done. I am also immensely grateful to Amir Shpilka for championing me in the community and for his constant support and encouragement.

References

[ASSS12] Manindra Agrawal, Chandan Saha, Ramprasad Saptharishi, and Nitin Saxena. Jacobian hits circuits: hitting-sets, lower bounds for depth-d occur-k formulas & depth-3 transcendence degree-k circuits. In *Proceedings of ACM Symposium on Theory of Computing (STOC)*, pages 599–614, 2012.

[AV08] Manindra Agrawal and V. Vinay. Arithmetic circuits: A chasm at depth four. In *Proceedings of IEEE Foundations of Computer Science (FOCS)*, pages 67–75, 2008.

[BDWY13] Boaz Barak, Zeev Dvir, Avi Wigderson, and Amir Yehudayoff. Fractional sylvester–gallai theorems. *Proceedings of the National Academy of Sciences*, 110(48):19213–19219, 2013.

[BM90] Peter Borwein and William OJ Moser. A survey of sylvester's problem and its generalizations. *Aequationes Mathematicae*, 40(1):111–135, 1990.

[BMS13] Malte Beecken, Johannes Mittmann, and Nitin Saxena. Algebraic independence and blackbox identity testing. *Information and Computation*, 222:2–19, 2013.

[BSS89] Lenore Blum, Mike Shub, and Steve Smale. On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines. *Bulletin (New Series) of the American Mathematical Society*, 21(1):1–46, 1989.

[CLO07] D.A. Cox, J.B. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Undergraduate Texts in Mathematics. Springer, 3rd edition, 2007.

[DE05] Alicia Dickenstein and Ioannis Z. Emiris, editors. *Solving Polynomial Equations : Foundations, Algorithms, and Applications*, volume 14 of *Algorithms and Computation in Mathematics*. Springer, Berlin, 2005.

[DS06] Zeev Dvir and Amir Shpilka. Locally decodable codes with 2 queries and polynomial identity testing for depth 3 circuits. *SIAM Journal on Computing*, 36(5):1404–1434, 2006.

[Dub93] Thomas W. Dubé. A combinatorial proof of the effective Nullstellensatz. *Journal of Symbolic Computation*, 15:277–296, 1993.

[Dvi12] Zeev Dvir. Incidence theorems and their applications. *Foundations and Trends in Theoretical Computer Science*, 6(4):257–393, 2012.

[GKKS13a] Ankit Gupta, Pritish Kamath, Neeraj Kayal, and Ramprasad Saptharishi. Approaching the chasm at depth four. In *Proceedings of IEEE Conference on Computational Complexity (CCC)*, pages 65–73, 2013.

[GKKS13b] Ankit Gupta, Pritish Kamath, Neeraj Kayal, and Ramprasad Saptharishi. Arithmetic circuits: A chasm at depth three. In *Proceedings of IEEE Foundations of Computer Science (FOCS)*, pages 578–587, 2013.

[Har77] Robin Hartshorne. *Algebraic Geometry.* Graduate texts in mathematics. Springer, New York, 1977.

[Har92] Joe Harris. *Algebraic Geometry: A First Course*, volume 133. Springer, 1992.

[HS81] Joos Heintz and Malte Sieveking. Absolute primality of polynomials is decidable in random polynomial time in the number of variables. In *Proceedings of International Colloquium on Automata, Languages and Programming (ICALP)*, pages 16–28, 1981.

[KMSV13] Zohar Shay Karnin, Partha Mukhopadhyay, Amir Shpilka, and Ilya Volkovich. Deterministic identity testing of depth-4 multilinear circuits with bounded top fan-in. *SIAM Journal on Computing*, 42(6):2114–2131, 2013.

[Kol88] János Kollár. Sharp effective nullstellensatz. *Journal of the American Mathematical Society*, 1(4):963–975, 1988.

[KS01] Adam Klivans and Daniel A. Spielman. Randomness efficient identity testing of multivariate polynomials. In *Proceedings of ACM Symposium on Theory of Computing (STOC)*, pages 216–223, 2001.

[KS09] Neeraj Kayal and Shubhangi Saraf. Blackbox polynomial identity testing for depth 3 circuits. In *Proceedings of IEEE Foundations of Computer Science (FOCS)*, 2009.

[KS11] Zohar Shay Karnin and Amir Shpilka. Black box polynomial identity testing of generalized depth-3 arithmetic circuits with bounded top fan-in. *Combinatorica*, 31(3):333–364, 2011.

[Mum76] David Mumford. *Algebraic Geometry I : Complex Projective Varieties.* Grundlehren der mathematischen Wissenschaften. Springer, Berlin, Heidelberg, New York, 1976.

[Sax14] Nitin Saxena. Progress on polynomial identity testing - II. *CoRR*, abs/1401.0976, 2014.

[Sch07] Peter Scheiblechner. *On the Complexity of Counting Irreducible Components and Computing Betti Numbers of Algebraic Varieties.* PhD thesis, 2007.

[Sud99] Madhu Sudan. Algebra and Computation. people.csail.mit.edu/madhu/FT98/. 1999. Lecture notes.

[SV85] S. Skyum and L. G. Valiant. A complexity theory based on boolean algebra. *Journal of the ACM*, 32(2):484–502, 1985.

[SV08] Amir Shpilka and Ilya Volkovich. Read-once polynomial identity testing. In *Proceedings of ACM Symposium on Theory of Computing (STOC)*, pages 507–516, 2008.

[SV11] Shubhangi Saraf and Ilya Volkovich. Black-box identity testing of depth-4 multilinear circuits. In *Proceedings of ACM Symposium on Theory of Computing (STOC)*, pages 421–430, 2011.

[SY10] Amir Shpilka and Amir Yehudayoff. Arithmetic circuits: A survey of recent results and open questions. *Foundations and Trends in Theoretical Computer Science*, 5(3-4):207–388, 2010.

[Val79] Leslie G. Valiant. Completeness Classes in Algebra. In *Proceedings of ACM Symposium on Theory of Computing (STOC)*, pages 249–261, 1979.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de