Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 52 (2015)

Depth-4 Identity Testing and Noether's Normalization Lemma

Partha Mukhopadhyay *

Chennai Mathematical Institute, India

April 7, 2015

Abstract

We consider the *black-box* polynomial identity testing (PIT) problem for a sub-class of depth-4 $\Sigma\Pi\Sigma\Pi(k,r)$ circuits. Such circuits compute polynomials of the following type:

$$C(\mathrm{X}) = \sum_{i=1}^{k} \prod_{j=1}^{d_i} Q_{i,j},$$

where k is the fan-in of the top Σ gate and r is the maximum degree of the polynomials $\{Q_{i,j}\}_{i\in[k],j\in[d_i]}$, and $k, r = O(1)$. We consider a sub-class of such circuits satisfying a *generic* algebraic-geometric restriction, and we give a deterministic polynomial-time black-box PIT algorithm for such circuits.

Our study is motivated by two recent results of Mulmuley (FOCS 2012, [Mul12]), and Gupta (ECCC 2014, [Gup14]). In particular, we obtain the derandomization by solving a particular instance of derandomization problem of Noether's Normalization Lemma (NNL). Our result can also be considered as a unified way of viewing the depth-4 PIT problems closely related to the work of Gupta [Gup14], and the approach suggested by Mulmuley [Mul12]. The importance of unifying PIT results is already exhibited by Agrawal et al. via the Jacobian approach (STOC 2012, [ASSS12]). To the best of our knowledge, the only known result that shows a derandomization of restricted NNL in the context of PIT problem, is the work of Forbes and Shpilka (RANDOM 2013, [FS13a], and FOCS 2013, [FS13b]). Forbes and Shpilka considered the black-box identity testing of noncommutative algebraic branching programs (ABPs).

*Email: partham@cmi.ac.in

ISSN 1433-8092

1 Introduction

Polynomial Identity Testing (PIT) is the following problem : Given an arithmetic circuit C computing a polynomial in $\mathbb{F}[x_1, \ldots, x_n]$, decide whether $C(\mathrm{X}) \equiv 0$ or not. The problem can be presented either in *white-box* model or in *black-box* model. In the white-box model, the arithmetic circuit is given explicitly as the input. In the black-box model, the arithmetic circuit is given as a black-box, and the circuit can be evaluated over any point in the field (or in a suitable extension field). Over the years, the problem has played pivotal role in many important results in complexity theory and algorithms: Primality Testing [AKS04], the PCP Theorem [ALM+98], IP = PSPACE [Sha90], graph matching algorithms [Lov79, MVV87]. The problem PIT admits a co-RP algorithm via the Schwartz-Zippel Lemma [Sch80, Zip79], but an efficient derandomized algorithm is not known.

An important result of Impagliazzo and Kabanets [KI04] (also, see [HS80]) showed a connection between the derandomization of PIT and arithmetic circuit lower bound. In particular, it is now known that if PIT can be derandomized using a certain type of pseudo-random generator, then the Permanent polynomial can not be computed by a polynomial-size arithmetic circuit [Agr05, KI04]. As a result, it will prove the algebraic analogue of P vs NP problem: VP $\neq$ VNP. We refer the reader to the survey of Shpilka and Yehudayoff [SY10] for the exposition to many important results in arithmetic circuit complexity, and polynomial identity testing problem.

Depth Reduction and Lower Bounds

In a surprising result, Agrawal and Vinay [AV08] showed that the derandomization of PIT only for depth-4 $\Sigma\Pi\Sigma\Pi$ circuits is sufficient to derandomize the PIT for the general arithmetic circuits. The main technical ingredient in their proof is an ingenious depth-reduction technique. As a result, it is now known that a sufficiently strong lower bound for only $\Sigma\Pi\Sigma\Pi$ circuits (even for depth-3 $\Sigma\Pi\Sigma$ circuits over large fields [GKKS13b]) will separate VP from VNP. Currently, there are many impressive partial results in this direction showing depth four lower bounds for explicit polynomials in VP and in VNP. All these papers use the shifted partial derivative technique first used in [GKKS13a].

Identity Testing for $\Sigma\Pi\Sigma$ and $\Sigma\Pi\Sigma\Pi$ Circuits

Motivated by the results of [KI04, Agr05, AV08], a large body of works consider the polynomial identity testing problem for restricted classes of depth-3 and depth-4 circuits. A particularly popular model in depth three arithmetic circuits is $\Sigma\Pi\Sigma(k)$ circuit, where the fan-in of the top Σ gate is bounded. Dvir-Shpilka showed a *white-box* quasi-polynomial time deterministic PIT algorithm for $\Sigma\Pi\Sigma(k)$ circuits [DS07]. Kayal-Saxena gave a polynomial-time white-box algorithm for the same problem [KS07]. Following the result of [KS07], Arvind-Mukhopadhyay gave a somewhat simpler algorithm of same running time [AM10]. Karnin and Shpilka gave the first *black-box* quasi-polynomial time algorithm for $\Sigma\Pi\Sigma(k)$ circuits [KS11]. Later, Kayal and Saraf [KS09] gave polynomial-

time deterministic black-box PIT algorithm for the same class of circuits over $\mathbb{Q}$ or $\mathbb{R}$. Finally, Saxena and Sheshadhri settled the situation completely by giving a deterministic polynomial-time *black-box* algorithm for $\Sigma\Pi\Sigma(k)$ circuits [SS12] over any field.

For $\Sigma\Pi\Sigma\Pi$ circuits, relatively a fewer deterministic algorithms are known. Just like in depth three, in depth four also the model $\Sigma\Pi\Sigma\Pi(k)$ is of considerable interest (where the top Σ gate is of bounded fan-in). Karnin et al. showed a quasi-polynomial time black-box identity testing algorithm for *multilinear* $\Sigma\Pi\Sigma\Pi(k)$ circuits [KMSV13]. Later, Saraf and Volkovich improved it to a deterministic polynomial time algorithm [SV11]. In 2013, Beecken et al. [BMS13] considered an algebraic restriction on $\Sigma\Pi\Sigma\Pi(k)$ circuits: bounded *transcendence degree*, and they showed an efficient deterministic black-box algorithm for such a class of circuits. Finally, Agrawal et al. showed that all these results can be proved under a unified framework using *Jacobian Criterion* [ASSS12].

Recent results of Mulmuley [Mul12] and Gupta [Gup14]

Noether's Normalization Lemma (NNL) is a fundamental result in algebraic geometry. Recently, Mulmuley observed a close connection between a certain formulation of *derandomization of* NNL, and the problem of showing explicit circuit lower bounds in arithmetic complexity [Mul12]. His main result is that these seemingly different looking problems are computationally equivalent. We explain the setting briefly.

Let $V \subseteq \mathbb{P}(\mathbb{C}^n)$ be any projective variety and $\dim V = m$. Then any homogeneous and random (generic) linear map $\Psi : \mathbb{P}^n \to \mathbb{P}^m$ restricts to a finite-to-one surjective closed map: $\Psi : V \to \mathbb{P}^m$. By derandomization of NNL, we mean an explicit construction of the map Ψ for any *explicit* variety. Mulmuley showed that this problem is equivalent to the problem of black-box derandomization of polynomial identity testing (PIT) [Mul12]. Here we note that efficient explicit derandomization of NNL is known for particular explicit varieties [FS13a]. This result is closely related to the breakthrough result of the same authors where they first showed a quasi-polynomial time *black-box* derandomization of noncommutative ABPs [FS13b].

In a recent work, Gupta [Gup14] takes a fresh approach to the black-box identity testing of depth-4 circuits. He considers a class of depth-4 circuits denoted by $\Sigma\Pi\Sigma\Pi(k, r)$. Such a circuit C computes a polynomial (over a field $\mathbb{F}$) of the following form:

$$C(\mathrm{X}) = \sum_{i=1}^{k} Q_i = \sum_{i=1}^{k} \prod_{j=1}^{d_i} Q_{i,j}(x_1, \ldots, x_n),$$

where $Q_{i,j}$s are polynomials over $\mathbb{F}$ and $\{x_1, x_2, \ldots, x_n\}$ are the variables appearing in the polynomial, and $k, r = O(1)$. It is an open problem to find an efficient deterministic black-box algorithm to identity test the circuit class $\Sigma\Pi\Sigma\Pi(k, r)$. Gupta considers an interesting sub-class of $\Sigma\Pi\Sigma\Pi(k, r)$ circuits by applying an algebraic-geometric restriction which he defines as *Sylvester-Gallai* property. Since he works in a projective space $\mathbb{P}^n$ over $\mathbb{C}$, it can be assumed that Q_{ij}s are homogeneous polynomials over the variables $x_0, \ldots, x_n$. The circuit C is not Sylvester-Gallai (SG) if the following property is true:

$$\exists i_k \in [k] : V(Q_{i_1}, \ldots, Q_{i_{k-1}}) \not\subseteq V(Q_{i_k})^1. \quad (1)$$

The indices $i_1, \ldots, i_{k-1}$ are the indices in $[k] \setminus \{i_k\}$. Gupta gives an efficient deterministic polynomial-time algorithm for polynomial identity testing for such a class of depth-4 circuits. He further conjectures that if C is SG, then the transcendence degree of the polynomials Q_{ij}s is $O(1)$. Then one can use the result of [BMS13], to solve the problem completely. His algorithm is interesting for several reasons. Firstly, his approach gives a clean and systematic algebraic-geometric approach to an interesting sub-class of depth-4 identity testing. Secondly, the algorithm connects the classical algebraic-geometric results such as Bertini's Theorem, and Ideal Membership Testing to the PIT problem for depth four circuits. We note that for $\Sigma\Pi\Sigma(k)$ circuits, Arvind-Mukhopadhyay [AM10] used ideal membership testing to give a simplified and alternative proof of Kayal-Saxena's algorithm [KS07].

Our Results

The main motivation of our study comes from the work of Mulmuley [Mul12], and from the work of Gupta [Gup14]. In this paper, we try to connect their approaches from a conceptual perspective. More precisely, we try to answer the following question: is there an interesting sub-class of $\Sigma\Pi\Sigma\Pi(k, r)$ circuits for which we can find a black-box polynomial-time deterministic PIT algorithm by derandomizing a special instance of NNL ? We give an affirmative answer. In the context of noncommutative ABPs, the work of Forbes and Shpilka gives such a result [FS13a, FS13b].

One of our key ideas is to start from a slightly different assumption (than Gupta's assumption), on the algebraic structure of the circuit. Let $\max\{d_i\} \leq D$. The family of circuits that we consider has the following property. There exists $i_1, i_2, \ldots, i_{k-1} \in [k]$, and $j_1, j_2, \ldots, j_{k-1} \in [D]$ such that $\forall S \subseteq [D]$ of size at most r^k, the following is true: In $\mathbb{P}^{n}$ [2],

$$\dim(V(Q_{i_1,j_1}, \ldots, Q_{i_{k-1},j_{k-1}}, \prod_{j_k \in S} Q_{i_k,j_k})) < \dim(V(Q_{i_1,j_1}, \ldots, Q_{i_{k-1},j_{k-1}})). \quad (2)$$

The fact that it is a generic assumption follows easily from the proof technique in Section 4. Again, by generic we mean that when the polynomials $Q_{i,j}$ are selected uniformly and independently at random, the circuit will have the property described in 2 with high probability. Our algorithm has three main stages.

[1] It is easy to observe that such a circuit class is *generic* in the sense that, when the polynomials $Q_{i,j}$s are selected uniformly and independently at random, the circuit is not SG with high probability.

[2] We also work in the projective spaces. The reason is explained later that w.l.o.g the polynomials $Q_{i,j}$s are homogeneous polynomials over $n+1$ variables.

Variable Reduction

In this stage, our idea is to construct an explicit linear transformation T such that $C(\mathrm{X}) \equiv 0$ if and only if $C(T(\mathrm{X})) \equiv 0$, and that T transforms the polynomial computed by C over a fewer number of variables. In particular, $\forall i, T : x_i \to L_i(y_0, \ldots, y_{2k-1})$ where L_i's are linear forms. We use Proposition 3 to argue that such a transformation always exists. The idea of this section is inspired by the work of Gupta in [Gup14] (in particular, Theorem 13, and Lemma 14), but with a key difference. Since our starting assumption on the circuit is different than Gupta's assumption, we do not need to use the classical result of Bertini directly (Theorem 13, [Gup14]).

Explicit Subspace Construction

In this stage, we find the sufficient algebraic conditions that the coefficients of the linear forms $L_i : 0 \leq i \leq n$ should satisfy. This section contains the main technical idea of our work, where we connect the problem to the derandomization of a particular instance of NNL. The idea is inspired by the work of [Mul12]. The main derandomization tool is the *multivariate resultant*. Using multivariate resultant, we reduce our problem to the problem of finding a hitting point of a product of a small number of *sparse* polynomials.

Hitting Set Construction

In this stage, we complete the algorithm by constructing a hitting set by applying the result of Klivans and Spielman [KS01]. More precisely, using the theory of multivariate resultant, and the hitting set construction of Klivans-Spielman, we argue that there is a small collection of points for the coefficients of L_is, such that at least for one such point $C(T(\mathrm{X})) \not\equiv 0$ if $C(\mathrm{X}) \not\equiv 0$. Moreover, $C(T(\mathrm{X}))$ is a polynomial over $O(1)$ variables and the individual degree of each variable is small. Then we can use the combinatorial nullstellensatz [Alo99] to find a small size hitting set for such a circuit.

Organization

The paper is organized as follows. In Section 1.1, we state the necessary results from algebraic geometry. In Section 1.2, we collect the necessary background from arithmetic complexity. We define our problem precisely in Section 2. The main algorithm and the correctness are given in Sections 3, 4, 4.1, 5. For the sake of completeness, we include a construction of hitting set for the product of sparse polynomials in Section A. We conclude in Section 6.

1.1 Algebraic Geometry

We recall the necessary background briefly.

Projective Varieties

In this work, we focus in the setting of projective spaces. We recall the standard definition from Chapter 2 of [Mum76]. Complex projective n-space $\mathbb{P}^n$ is the set of $(n+1)$-tuples $a_0, \ldots, a_n$ of complex numbers, not all zero, modulo the equivalence relation: $(a_0, \ldots, a_n) \sim (\lambda a_0, \ldots, \lambda a_n)$, where $\lambda \in \mathbb{C} \setminus \{0\}$. A projective variety is the set of common zeros of a system of homogeneous polynomial equations in $\mathbb{P}^n$.

Dimension of a variety

We use the following definition of dimension of a projective variety [Har92].

Definition 1. *Dimension of $V \subseteq \mathbb{P}^n$ is the largest k such that for every linear subspace Λ of dimension $\geq n-k$, we have $V \cap \Lambda \neq \phi$.*

Co-dimension of a variety $V \subseteq \mathbb{P}^n$ is denoted by $\mathrm{codim}(V)$ and it is defined as $n - \dim(V)$. The following basic facts are useful for us. Those can be found in the standard text [CLO07].

Proposition 1. *The following facts extend our intuition from standard linear algebra:*

1. *Let $f \in \mathbb{C}[x_0, \ldots, x_n]$ be a non-zero homogenous polynomial. Then $\dim(V(f)) = n-1$ in $\mathbb{P}^n$.*
2. *Let $V, W \subseteq \mathbb{P}^n$. If $V \subseteq W$ then $\dim(V) \leq \dim(W)$.*
3. *$V \cap W$ has co-dimension $\leq \mathrm{codim}(V) + \mathrm{codim}(W)$ in $\mathbb{P}^n$.*

Hilbert's Nullstellnesatz

We state the following version from Theorem 2 of Chapter 4 [CLO07]. Let $f, f_1, \ldots, f_s$ are polynomials in $\mathbb{C}[x_1 \ldots, x_n]$. Then, $V(f_1, f_2, \ldots, f_s) \subseteq V(f)$ if and only if $f \in \sqrt{\langle f_1, f_2, \ldots, f_s \rangle}$, where $\sqrt{\langle f_1, f_2, \ldots, f_s \rangle}$ is the radical generated by $f_1, \ldots, f_s$.

Noether's Normalization

We recall the following version of Noether's Normalization Lemma from the book by Mumford [Mum76]. Consider the following class of maps: $Y_i = \sum_{j=0}^{n} a_{i,j} X_j, 0 \leq i \leq r'$, be $r'+1$ independent linear forms. Let $L \subset \mathbb{P}^n$ be the $(n-r'-1)$-dimensional linear space $V(Y_0, \ldots, Y_{r'})$. Define the projection $p_L : \mathbb{P}^n - L \longrightarrow \mathbb{P}^{r'}$ by $(b_0, \ldots, b_n) \longrightarrow (\sum a_{0,j} b_j, \ldots, \sum a_{r',j} b_j)$.

Theorem 1. *(Corollary 2.29, [Mum76]) Let V be an r'-dimensional variety in $\mathbb{P}^n$. Then there is a linear subspace L of dimension $n-r'-1$ such that $L \cap V$ is empty. For all such L, the projection p_L restricts to a finite-to-one surjective closed map:*

$$p_L : V \longrightarrow \mathbb{P}^{r'},$$

and the homogeneous coordinate ring $\mathbb{C}[X_0, \ldots, X_n]/I(V)$ *of* V *is a finitely generated module over* $\mathbb{C}[Y_0, \ldots, Y_{r'}]$.

One can derive the following algorithmically useful consequence of the above theorem (See Lemma 2.14, [Mul12]).

Lemma 1. *Let* $V \subseteq \mathbb{P}^n$ *be the variety defined by a set of homogeneous polynomials* $f_1, \ldots, f_k \in \mathbb{C}[x_0, \ldots, x_n]$, *and* $\dim(V)$ *be the dimension of* V. *Consider the random linear forms,*

$$L_j(x) = \sum_{\ell=0}^{n} b_{\ell,j} x_\ell; 0 \leq j \leq s.$$

Let $H_j \subseteq \mathbb{P}^n$ *be the hyperplane defined by* $L_j(x) = 0$. *If* $s < \dim(V)$, *then* $V \cap \bigcap_j H_j \neq \phi$. *If* $s = \dim(V)$, *then with high probability,* $V \cap \bigcap_j H_j$ *is empty.*

When $s < \dim(V)$, the fact that $V \cap \bigcap_j H_j \neq \phi$ follows from the definition 1. If $s = \dim(V)$, then Theorem 1 implies the existence of a linear subspace $L = \bigcap_j H_j$ of dimension $n - s - 1$ such that $V \cap L = \phi$. Lemma 1 implies that such a linear subspace L exists with high probability.

Multivariate Resultant

We recall the concept of multivariate resultant from Chapter 3 of [CLO05]. Suppose we have $n+1$ homogeneous polynomials $F_0, F_1, \ldots, F_n$ in the variables $x_0, \ldots, x_n$, and assume that each F_i has positive total degree. We get $n+1$ equations in $n+1$ unknowns:

$$F_0(x_0, \ldots, x_n) = \ldots = F_n(x_0, \ldots, x_n) = 0. \tag{3}$$

The multivariate resultant answers precisely the following question: what conditions must the coefficients of $F_0, \ldots, F_n$ satisfy in order that the system in Equation 3 has a nontrivial solution. Suppose d_i be the total degree of F_i. Then F_i can be written as

$$F_i = \sum_{\alpha:|\alpha|=d_i} c_{i,\alpha} x^\alpha.$$

For each pair i, α, we introduce a variable $u_{i,\alpha}$. Now we are ready to state the following important Theorem.

Theorem 2. *(Theorem 2.3, [CLO05]) There is a unique irreducible polynomial* $\mathrm{Res}[u_{i,\alpha}] \in \mathbb{Z}[u_{i,\alpha}]$ *such that the system of polynomial equations 3 has a nontrivial solution if and only if* $\mathrm{Res}[c_{i,\alpha}] = 0$ *(i.e. we substitute* $u_{i,\alpha}$ *by* $c_{i,\alpha}$*).*

For our application, we need an upper bound on the degree of the polynomial $\mathrm{Res}[u_{i,\alpha}]$. If $d_i \leq d$ for $i \in [0; n]$, $\deg(\mathrm{Res}) \leq (n+1) \cdot d^n$ (Theorem 3.1, [CLO05]).

1.2 Arithmetic Complexity

Arithmetic Circuits

An arithmetic circuit over a field $\mathbb{F}$ with the set of variables $x_1, x_2, \ldots, x_n$ is a directed acyclic graph such that the internal nodes are labelled by addition or multiplication gates and the leaf nodes are labelled by the variables or the field elements. The node with fan-out zero is the output gate. An arithmetic circuit computes a polynomial in the polynomial ring $\mathbb{F}[x_1, x_2, \ldots, x_n]$. Size of an arithmetic circuit is the number of nodes and the depth is the length of a longest path from the root to a leaf node.

Depth-4 Circuits

Usually a depth-4 circuit over a field $\mathbb{F}$ is denoted by $\Sigma\Pi\Sigma\Pi$. The circuit has an addition gate at the top, then a layer of multiplication gates, followed by a layer of addition gates, and a bottom layer of multiplication gates. In this work we focus on a class of $\Sigma\Pi\Sigma\Pi$ circuits that we denote by $\Sigma\Pi\Sigma\Pi(k, r)$, where k is the fan-in of the top Σ gate and r is the upper bound on the fan-in of the bottom Π gate. A $\Sigma\Pi\Sigma\Pi(k, r)$ circuit C computes a polynomial of the following form.

$$C(\mathrm{X}) = \sum_{i=1}^{k} Q_i = \sum_{i=1}^{k} \prod_{j=1}^{d_i} Q_{i,j}(x_1, \ldots, x_n)$$

where $Q_{i,j}$s are polynomials over $\mathbb{F}$ and $\{x_1, x_2, \ldots, x_n\}$ are the variables appearing in the polynomial. In this work, we will consider depth four circuits with $k, r = O(1)$. We will also assume that $\forall i : d_i \leq D$. Also, we always assume that the circuit is given as a black-box.

Homogenization

We can homogenize the circuit w.r.t a new variable x_0 by obtaining the black-box for $C' = x_0^d C(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0})$, where d is the degree of the polynomial computed by C. Clearly, $C' \equiv 0 \iff C \equiv 0$. We can also factorize the polynomials Q_{ij}s to their irreducible factors [3]. Since the degrees of the polynomials Q_{ij} are bounded by r, each Q_{ij} can be factored in at most r irreducible factors, increasing the fan-in of the Π-gate in the second layer by a factor r. We continue to use the notation C to represent the homogeneous circuit, and use D for the fan-in upper bound of the Π gates in the second layer.

Combinatorial Nullstellensatz

We recall the following theorem from [Alo99].

[3] We do not explicitly use the fact that $Q_{i,j}$s are irreducible in the analysis. This fact is useful if we would like to formulate a conjecture in the similar spirit of Conjecture 1 in [Gup14]. This issue is discussed in Section 6.

Theorem 3. *Let $f(x_1, x_2, \ldots, x_n)$ be a polynomial in n variables over an arbitrary field $\mathbb{F}$. Suppose that the degree of f as a polynomial in x_i is at most t_i, for $1 \leq i \leq n$ and let $S_i \subseteq \mathbb{F}$ such that $|S_i| \geq t_i+1$. If $f(a_1, a_2, \ldots, a_n) = 0$ for all n-tuples in $S_1 \times S_2 \times \cdots \times S_n$, then $f \equiv 0$.*

Hitting Set and Sparse Polynomials

Let $\mathcal{C}$ be a family of arithmetic circuits computing n-variate polynomials over a field $\mathbb{F}$. A hitting set for $\mathcal{C}$ is a subset $\mathcal{H}$ of $\mathbb{F}^n$, such that for any non-zero circuit $C \in \mathcal{C}$, there exists $\vec{b} \in \mathcal{H}$ such that $C(\vec{b}) \neq 0$. If $\mathcal{H}$ can be constructed in deterministic polynomial time (in the input size), then we say that $\mathcal{H}$ is an efficiently computable explicit hitting set. The problem of black-box derandomization and efficient explicit hitting set construction are equivalent. A multivariate polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$ is t-sparse if it has at most t non-zero monomials.

Notations : For integers $a, b \geq 0$, the notation $[a; b] = \{x \in \mathbb{Z} : a \leq x \leq b\}$. We use the notation $C(\mathrm{X})$ to denote the multivariate polynomial output of a circuit C. Otherwise, we use the notation $Q(x)$ to denote a multivariate polynomial $Q(x_1, \ldots, x_n)$.

2 The Problem

The circuit C (computing a polynomial in $\mathbb{C}[x_0, \ldots, x_n]$) is given by a black-box and we need to test whether $C \equiv 0$ or not. Here we consider an assumption that either $C \equiv 0$ or C satisfies a *generic* property that we call the property $\mathcal{P}$. It is defined as follows.

We say that the circuit C satisfies the property $\mathcal{P}$, if there exist $i_1, i_2, \ldots, i_{k-1} \in [k]$, and $j_1, j_2, \ldots, j_{k-1} \in [D]$ such that $\forall S \subseteq [D]$ of size at most r^k, the following is true.

In the projective space $\mathbb{P}^n$,

$$\dim(V(Q_{i_1,j_1}, \ldots, Q_{i_{k-1},j_{k-1}}, \prod_{j_k \in S} Q_{i_k,j_k})) < \dim(V(Q_{i_1,j_1}, \ldots, Q_{i_{k-1},j_{k-1}})). \tag{4}$$

The following claim is obvious from the above assumption.

Claim 1. *For all $S \subseteq [D]$ of size at most r^k, $V(Q_{i_1,j_1}, \ldots, Q_{i_{k-1},j_{k-1}}) \not\subseteq V(\prod_{j_k \in S} Q_{i_k,j_k})$.*

For the simplicity, we will assume that (w.l.o.g) $i_1 = 1, \ldots, i_{k-1} = k-1, i_k = k$, and $j_1 = j_2 = \ldots = j_{k-1} = 1$. Using Bézout's theorem Gupta made the following simple but very useful observation.

Lemma 2 ([Gup14], Claim 11)**.** *Let $P_1, \ldots, P_d, Q_1, \ldots, Q_k \in \mathbb{C}[x_0, \ldots, x_n]$ be homogeneous polynomials and degree of each Q_i is at most r. Then,*

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

We use the above lemma to observe that if C satisfies property $\mathcal{P}$, then $C \not\equiv 0$.

Lemma 3. *if C is a circuit computing a polynomial that satisfies the property $\mathcal{P}$, then C can not compute an identically zero polynomial.*

Proof. By Hilbert Nullstellensatz and from Claim 1, $\prod_{j\in S} Q_{k,j} \notin \sqrt{\langle Q_{1,1}, Q_{2,1}, \ldots, Q_{k-1,1}\rangle}$ for any S of size at most r^k. Now using Lemma 2, we get that $Q_k \notin \sqrt{\langle Q_{1,1}, Q_{2,1}, \ldots, Q_{k-1,1}\rangle}$, which is not possible if $C \equiv 0$. □

3 Variable Reduction Phase

The goal of this section is to find an efficiently computable explicit linear transformation T such that $C(\mathrm{X}) \equiv 0$ if and only if $C(T(\mathrm{X})) \equiv 0$, and $C(T(\mathrm{X}))$ is a polynomial over a fewer number of variables.

Let $Q_S = \prod_{j\in S} Q_{k,j}$. Recall that the subset S is of size at most r^k, and for each such S, $V(Q_{1,1}, Q_{2,1}, \ldots, Q_{k-1,1}) \not\subseteq V(Q_S)$. The total number of such sets are only $\leq D^{r^k}$ which is polynomially bounded for $r, k = O(1)$. Notice that $\forall S$: $\mathrm{codim}(V(Q_{1,1}, Q_{2,1}, \ldots, Q_{k-1,1}, Q_S)) \leq k$ (Proposition 1). Now, we mention the following simple fact (Exercise 11.6) from [Har92].

Proposition 2. *Let $V \subseteq \mathbb{P}^n$ be any projective variety and $Z \subseteq \mathbb{P}^n$ be any hypersurface not containing an irreducible component of V. Then* $\mathrm{codim}(V \cap Z) = \mathrm{codim}(V) + 1$.

In other words, a generic (random) hypersurface satisfies the above property. Using the above proposition repeatedly, one can easily observe the following result. It was first observed and used by Gupta [Gup14].

Proposition 3. *For a variety $V \subseteq \mathbb{P}^n$ of co-dimension c and a generic(random) linear subspace Λ of co-dimension $\leq n - c - 1$,* $\mathrm{codim}(V \cap \Lambda) = \mathrm{codim}(V) + \mathrm{codim}(\Lambda)$.

From Proposition 3, we know that for each S, $\exists$ a subspace Λ_S such that

$$\mathrm{codim}(V(Q_{1,1}, \ldots, Q_{k-1,1}, Q_S, \Lambda_S) = \mathrm{codim}(V(Q_{1,1}, \ldots, Q_{k-1,1}, Q_S)) + \mathrm{codim}(\Lambda_S),$$

and the dimension of $\Lambda_S = 2k - 1$ [4].

Since the number of possible sets S is *small* (polynomially bounded), by an union bound, one can observe that $\exists\Lambda$ of dimension $2k-1$ that satisfies the above property for all S simultaneously [5]. The following fact is also immediately clear.

Lemma 4. *$\forall S \subseteq [D]$ of size at most r^k, in $\mathbb{P}^n$,* $\dim(V(Q_{1,1}, \ldots, Q_{k-1,1}, Q_S, \Lambda)) = \dim(V(Q_{1,1}, \ldots, Q_{k-1,1}, Q_S) - (n - 2k + 1)$, *and* $\dim(V(Q_{1,1}, \ldots, Q_{k-1,1}, Q_S, \Lambda)) < \dim(V(Q_{1,1}, \ldots, Q_{k-1,1}, \Lambda))$.

The following is an easy observation.

[4] Notice that $\mathrm{codim}(\Lambda_S) = n - (2k-1) \leq n - k - 1$ for $k \geq 2$.

[5] In the next section, we show how to construct such a subspace deterministically.

Observation 1. *From Proposition 1, we get that in* $\mathbb{P}^n$, $\dim(V(Q_{1,1},\ldots,Q_{k-1,1})) \geq n-(k-1)$ *and* $\dim(V(Q_{1,1},\ldots,Q_{k-1,1},Q_S)) = \dim(V(Q_{1,1},\ldots,Q_{k-1,1}))-1$ *for all subsets* $S \subseteq [D]$ *of size at most* r^k.

Now our goal is to explicitly construct the subspace Λ (of dimension $2k-1$) such that $\forall S \subseteq [D]$ of size at most r^k, $\dim(V(Q_{1,1},\ldots,Q_{k-1,1},Q_S,\Lambda)) = \dim(V(Q_{1,1},\ldots,Q_{k-1,1},Q_S))-(n-(2k-1))$ in $\mathbb{P}^n$.

The subspace Λ

We fix a subspace Λ of co-dimension $n-(2k-1)$ in $\mathbb{P}^n$ as follows. For each $i \in \{0,1,\ldots,n\}$, set

$$x_i = \sum_{j=0}^{2k-1} a_{ij}y_j$$

where $a_{ij} \in \mathbb{C}$ are the constants to be specialized later in the analysis. We define the matrix $A = (a_{i,j})_{0\leq i\leq 2k-1, 0\leq j\leq 2k-1}$. To ensure that the dimension of the subspace Λ is $2k-1$, we will choose the constants in such a way that the symbolic determinant $\det(A)$ is non-zero.

After the above substitution, we identify the polynomials $Q_{1,1},\ldots,Q_{k-1,1},Q_S$ over the variables $y_0,y_1,\ldots,y_{2k-1}$ with coefficients as polynomials in $\mathbb{C}[\{a_{i,j}\}_{0\leq i\leq n,0\leq j\leq 2k-1}]$. Notice that the degree of coefficient polynomials $\leq r^{k+1}$ [6], and also the coefficient polynomials are $(2k(n+1))^{r^{k+1}}$-sparse. In the next section, we fix the coefficients $\{a_{i,j}\}_{0\leq i\leq n,0\leq j\leq 2k-1}$ explicitly, using an application of Noether's Normalization Lemma. To summarize, the transformation T does the following:

$$0 \leq i \leq n : T : x_i \to \sum_{j=0}^{2k-1} a_{ij}y_j.$$

After the substitution by the map T, we identify the variety $V(Q_{1,1},\ldots,Q_{k-1,1},\Lambda)$ by $V(Q_{1,1}(y),\ldots,Q_{k-1,1}(y))$. Also, for any subset S, we identify the variety $V(Q_{1,1},\ldots,Q_{k-1,1},Q_S,\Lambda)$ by $V(Q_{1,1}(y),\ldots,Q_{k-1,1}(y),Q_S(y))$.

4 An Explicit Subspace Construction

In $\mathbb{P}^n$, for each subset S, $n-k \leq \dim(V(Q_{1,1},\ldots,Q_{k-1,1},Q_S)) \leq n-1$. Let $s_0 = \dim(V(Q_{1,1},\ldots,Q_{k-1,1},Q_S))-(n-2k+1)$. Clearly $k-1 \leq s_0 \leq 2k-2$, but notice that we do not know the exact value of s_0. For each $s \in [k-1;2k-2]$, we apply Lemma 1 to construct linear subspaces $\bigcap_{0\leq j\leq s} H_j$ given by: $H_j(y) : L_j(y) = \sum_{\ell=0}^{2k-1} w_{\ell,j}y_\ell; 0 \leq j \leq s$, where $w_{\ell,j} \in \mathbb{C}$ are constants to be fixed. To ensure that the dimension of the varieties

[6] Recall that $\deg(Q_S) \leq r^{k+1}$ for any S.

$V(Q_{1,1}(y),\ldots,Q_{k-1,1}(y),Q_S(y))$ are exactly s, we consider the multivariate resultant of the system of polynomial equations (for each fixed S),

$$Q_{1,1}(y) = \ldots = Q_{k-1,1}(y) = Q_S(y) = 0,$$

$$H_j(y) : L_j(y) = \sum_{\ell=0}^{2k-1} w_{\ell,j} y_\ell = 0; 0 \leq j \leq s.$$

Multivariate Resultant Criterian

We use the following ideas from (Lemma 2.14, [Mul12]). It can be derived by applying the formulation of NNL in Lemma 1. For each S, we construct the following system of polynomials.

$$F_j^S(y) = \sum_{i=1}^{k-1} z_{i,j} Q_{i,1}(y) + z_j Q_S(y),\ 0 \leq j \leq (2k-1)-(s+1)$$

and,

$$L_j(y) = \sum_{\ell=0}^{2k-1} w_{\ell,j} y_\ell,\ 0 \leq j \leq s.$$

Notice that for each j and S, the polynomial F_j^S is a generic linear combination of the polynomials $Q_{1,1},\ldots,Q_{k-1,1},Q_S$.

Remark 1. *From Lemma 2.11, and Lemma 2.14 of [Mul12], one observes that to implement the above idea, the polynomials $Q_{1,1}(y),\ldots,Q_{k-1,1}(y),Q_S(y)$ should be of same degree . This can be ensured by raising each $Q_{i,1}$ to the power $\left(\prod_{j=1}^{k-1}\deg(Q_{j,1})\cdot\deg(Q_S)\right)/\deg(Q_{i,1})$. For the polynomial Q_S, we raise it to the power $\left(\prod_{j=1}^{k-1}\deg(Q_{j,1})\right)$. So the final degree of each polynomial is at most $r^{O(k)}$.*

For any subset S, the coefficients of the above system of polynomials (in the variables $y_0,\ldots,y_{2k-1}$) are polynomials in the ring

$$\mathbb{C}[\{a_{i,j}\}_{0\leq i\leq n,0\leq j\leq 2k-1},\{z_{ij},z_j\}_{1\leq i\leq k-1,0\leq j\leq(2k-1)-(s+1)},\{w_{\ell,j}\}_{0\leq\ell\leq 2k-1,0\leq j\leq s}].$$

So, the coefficients of the polynomials $Q_{1,1}(y),\ldots,Q_{k-1,1}(y),Q_S(y)$ can be viewed as polynomials with at most $N = ((2k(n+1)+2k(s+1)+k(2k-1-s))$ variables and degree bounded by $r^{O(k)}$.

Now we use the estimate on the degree of the multivariate resultant polynomial given in Section 1.1.

Observation 2. *For each fixed S, the multivariate resultant polynomial corresponding to the above system of polynomials $\{F_j^S(y)\}_{0\leq j\leq(2k-1)-(s+1)}$, and $\{L_j(y)\}_{0\leq j\leq s}$ is a $\leq (2k)\cdot(r^{O(k)})^{2k}\cdot(r^{O(k)})$-degree polynomial in at most N variables.*

So the polynomials are $N^{r^{O(k^2)}}$-sparse. Also, the number of such resultant polynomials are bounded by D^{r^k}.

Non zero-ness of the resultant polynomials

Suppose we choose the subspace Λ (by fixing the indeterminates $\{a_{i,j}\}_{0\leq i\leq n, 0\leq j\leq 2k-1}$ over $\mathbb{C}$) in such a way that $s_0 = \dim(V(Q_{1,1}(y),\ldots,Q_{k-1,1}(y),Q_S(y)) = \dim(V(Q_{1,1},\ldots,Q_{k-1,1},Q_S) - (n-2k+1)$. Then if $s = s_0$, for each S, the resultant polynomial R_S is a non-identically zero polynomial. It follows as a consequence of NNL that the above system of polynomial equations has only trivial solution for some rational values of $z_{i,j}$'s, z_j's and $w_{\ell,j}$'s, when $s = s_0$. This point is discussed explicitly in Lemma 2.14 of [Mul12]. This also implies that the resultant polynomials $R_S(z_{i,j}, z_j, w_{\ell,j})$ are non identically zero. So, in particular, when $s = s_0$ and the subspace Λ is not fixed, the resultant polynomials $R_S(a_{i,j}, z_{i,j}, z_j, w_{\ell,j})$ are non identically zero polynomials.

Next, our idea is to specialize the values of the N indeterminates using the hitting set construction of Kilvans-Spielman [KS01] for the product of $N^{r^{O(k^2)}}$-sparse polynomials, so that *all* the resultant polynomials and the polynomial $\det(A)$, evaluate to nonzero at some point in the hitting set. In the next section, we explain that such an idea is sufficient for our problem.

4.1 The Correctness Proof

In Section 4, we repeat the construction for all possible values for the parameter $s \in [k-1; 2k-2]$. From the discussion in the last section, we know that if $s = s_0$, the resultant polynomials R_S are non identically zero polynomials.

Using the hitting set construction of [KS01], we can specialize the indeterminates so that for each S, the polynomial R_S and $\det(A)$ evaluate to non-zero. Once we fix the values for $\{a_{i,j}\}_{0\leq i\leq n, 0\leq j\leq 2k-1}$ to $\{a^*_{i,j}\}_{0\leq i\leq n, 0\leq j\leq 2k-1}$, we also define the subspace Λ. Moreover, since $\det(A) \neq 0$, we ensure that $\mathrm{codim}(\Lambda) = n-(2k-1)$.

Lemma 5. *Let* $\{a^*_{i,j}\}_{0\leq i\leq n, 0\leq j\leq 2k-1}, \{z^*_{ij}, z^*_j\}_{1\leq i\leq k-1, 0\leq j\leq (2k-1)-(s+1)}, \{w^*_{\ell,j}\}_{0\leq \ell\leq 2k-1, 0\leq j\leq s}$ *be a hitting point for* $\prod_{S\in\binom{[D]}{r^k}} R_S \cdot \det(A)$. *Then on such a point* $\dim(V(Q_{1,1}(y),\ldots,Q_{k-1,1}(y),Q_S(y))) = s_0$.

Proof. If $\dim(V(Q_{1,1}(y),\ldots,Q_{k-1,1}(y),Q_S(y)))$ is more than s_0, then $\dim(V(\{F^S_j\}_{0\leq\leq(2k-1)-(s_0+1)}))$ is also more than s_0. The dimension of the linear space defined by $\{L_j(y)\}_{0\leq j\leq s_0}$ is $\geq (2k-1)-(s_0+1)$. Then using the definition 1, we can easily see that the system of polynomials $\{F^S_j\}_{0\leq\leq(2k-1)-(s_0+1)}), \{L_j(y)\}_{0\leq j\leq s_0}$ has a nontrivial solution and $R_S = 0$. Since the $\mathrm{codim}(\Lambda) = n-(2k-1)$ on the point $\{a^*_{i,j}\}_{0\leq i\leq n, 0\leq j\leq 2k-1}$, it is not possible that $\dim(V(Q_{1,1}(y),\ldots,Q_{k-1,1}(y),Q_S(y))) < s_0$. □

From Lemma 5, it is obvious that for $s = s_0$ and on a hitting point, the following is true.

$$\forall S\subseteq[D]; |S|\leq r^k : \dim(Q_{1,1}(y),\ldots,Q_{k-1,1}(y),Q_S(y)) < \dim(Q_{1,1}(y),\ldots,Q_{k-1,1}(y))$$
$$\Rightarrow \forall S\subseteq[D]; |S|\leq r^k : V(Q_{1,1}(y),\ldots,Q_{k-1,1}(y)) \not\subseteq V(Q_S) \text{ (Claim 1)}$$
$$\Rightarrow \forall S\subseteq[D]; |S|\leq r^k : Q_S(y) \notin \sqrt{\langle Q_{1,1}(y),\ldots,Q_{k-1,1}(y)\rangle}.$$

The last relation follows from the Hilbert Nullstellensatz. Now we apply Lemma 2, to deduce that

$$Q_k(y) \notin \sqrt{\langle Q_{1,1}(y), \ldots, Q_{k-1,1}(y)\rangle} \Rightarrow C(\mathrm{Y}) \not\equiv 0.$$

Recall that in the remark 1, the degrees of $Q_{1,1}, \ldots, Q_{k-1,1}, Q_S$ are pretended to be increased by appropriate powering, is only for the analysis purpose.

The degree of each variable in $C(\mathrm{Y})$ is bounded by $D \cdot r$, and also $C(\mathrm{Y})$ is a $2k$-variate polynomial. We use Combinatorial Nullstellensatz (Theorem 3) to construct a hitting set for $C(\mathrm{Y})$. In the next section, we formally explain the construction of the final hitting set.

5 The Hitting Set Construction

Let $\mathcal{H}_{t,m,N,d} \subset \mathbb{C}^N$ be a hitting set for the product of $\leq m$ polynomials in N variables such that each polynomial is t-sparse, and of degree $\leq d$. One can construct $\mathcal{H}_{t,m,N,d} \subset \mathbb{C}^N$ efficiently following the result of Klivans and Spielman [KS01]. For the sake of completeness, we include a proof in the Appendix (Section A).

For each $s \in [k-1; 2k-2]$, we do the following. We use the hitting set $\mathcal{H}_s = \mathcal{H}_{N(s)^{r^{O(k^2)}}, D^{rk}+1, N(s), r^{O(k^2)}}$ to substitute values to the indeterminates,

$$\{a_{i,j}\}_{0\leq i\leq n, 0\leq j\leq 2k-1}, \{z_{ij}, z_j\}_{1\leq i\leq k-1, 0\leq j\leq (2k-1)-(s+1)}, \{w_{\ell,j}\}_{0\leq \ell\leq 2k-1, 0\leq j\leq s}.$$

For each such substitution, we construct the subspace Λ by setting $\forall i \in [0; n] : x_i = \sum_{j=0}^{2k-1} a_{i,j} y_j$. Next we fix a set $\mathcal{S} \subset \mathbb{Q}$ such that $\mathcal{S} = D \cdot r + 1$, and test whether $C(\mathrm{Y})\big|_{y \in S^{2k}} = 0$. From the correctness proof (Section 4.1), we know that if $C(\mathrm{X}) \not\equiv 0$, then for one of the subspaces Λ that we have constructed, $\exists \vec{b} \in S^{2k}$ such that $C(\vec{b}) \neq 0$.

The Final Algorithm

We state our final algorithm formally.

1. For each $s \in [k-1; 2k-2]$, we do the following.
   (a) For each point in the hitting set $\mathcal{H}_s$, specialize the values for $\{a_{ij}\}_{0\leq i\leq n, 0\leq j\leq 2k-1}$.
   (b) For each such specialization for $\{a_{ij}\}_{0\leq i\leq n, 0\leq j\leq 2k-1}$, construct the subspace Λ by substituting $0 \leq i \leq n : x_i = \sum_{j=0}^{2k-1} a_{ij} y_j$.
   (c) Check whether $C(\mathrm{Y})\big|_{y \in S^{2k}} = 0$, where $S = \{1, \ldots, D \cdot r + 1\}$. If anytime C evaluates to a non-zero value, we stop the procedure and announce that $C \not\equiv 0$.
2. Otherwise, output that $C \equiv 0$.

The Cost

The cost of our algorithm is bounded by $(2k-2) \cdot \max_s \left|\mathcal{H}_s\right| \cdot (D \cdot r + 1)^{2k}$. Using the estimate of Section A for $\max_s \left|\mathcal{H}_s\right|$, one can easily upper bound the cost by $(D \cdot n)^{r^{O(k^2)}}$.

6 Conclusion

In [Gup14], Gupta considers the minimal and simple $\Sigma\Pi\Sigma\Pi(k, r)$ circuits. A circuit C is called *simple* if $\text{g.c.d}(C) = \text{g.c.d}(Q_1, \ldots, Q_k) = 1$. It is said to be *minimal* if for every non-empty subset $A \subseteq [k] : \sum_{i \in A} Q_i \not\equiv 0$. In the black-box case, we can assume that the circuit is minimal (we can always eliminate a few gates if required to make it minimal). Given a circuit C, we can always assume that $C = \gcd(C) \cdot \text{sim}(C)$, where $\text{sim}(C)$ is the simple part of C which is also minimal. One of his main motivations is to formulate a structural conjecture (Conjecture 1, [Gup14]). If the conjecture is true, then using the result of [BMS13], one can derandomize the problem completely even in the case when the circuit is SG. In our case too, it is possible to formulate a conjecture in the similar spirit. We omit the straightforward generalization.

We believe that the main interesting feature of our work is the fact that PIT for a generic sub-class of $\Sigma\Pi\Sigma\Pi(k, r)$ circuits can be tackled by derandomizing a restricted instance of a classical result in algebraic geometry : Noether Normalization Lemma. As a minor point, we note that the running time of our algorithm is similar to the running time in [Gup14].

7 Acknowledgement

I thank K.V. Subrahmanyam for many helpful discussions.

References

[Agr05] Manindra Agrawal. Proving lower bounds via pseudo-random generators. In *FSTTCS 2005: Foundations of Software Technology and Theoretical Computer Science, 25th International Conference*, pages 92–105, 2005.

[AKS04] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES is in P. *Ann. of Math*, 160(2):781–793, 2004.

[ALM+98] Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. Proof verification and the hardness of approximation problems. *J. ACM*, 45(3):501–555, 1998.

[Alo99] Noga Alon. Combinatorial nullstellensatz. *Combinatorics, Probability and Computing*, 8, 1999.

[AM10] Vikraman Arvind and Partha Mukhopadhyay. The ideal membership problem and polynomial identity testing. *Inf. Comput.*, 208(4):351–363, 2010.

[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 the 44th Symposium on Theory of Computing Conference, STOC 2012*, pages 599–614, 2012.

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

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

[CLO05] David A. Cox, John Little, and Donal O'Shea. *Using Algebraic Geometry*. Springer-Verlag New York, Inc., 2005.

[CLO07] David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, 3/e (Undergraduate Texts in Mathematics)*. Springer-Verlag New York, Inc., 2007.

[DS07] Zeev Dvir and Amir Shpilka. Locally decodable codes with two queries and polynomial identity testing for depth 3 circuits. *SIAM J. Comput.*, 36(5):1404–1434, 2007.

[FS13a] Michael A. Forbes and Amir Shpilka. Explicit noether normalization for simultaneous conjugation via polynomial identity testing. In *17th International Workshop, RANDOM 2013*, pages 527–542, 2013.

[FS13b] Michael A. Forbes and Amir Shpilka. Quasipolynomial-time identity testing of non-commutative and read-once oblivious algebraic branching programs. In *54th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2013*, pages 243–252, 2013.

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

[GKKS13b] Ankit Gupta, Pritish Kamath, Neeraj Kayal, and Ramprasad Saptharishi. Arithmetic circuits: A chasm at depth three. In *FOCS*, pages 578–587, 2013.

[Gup14] Ankit Gupta. Algebraic geometric techniques for depth-4 PIT & sylvester-gallai conjectures for varieties. *Electronic Colloquium on Computational Complexity (ECCC)*, 21:130, 2014.

[Har92] Joe Harris. Algebraic geometry : A first course. *Springer*, 1992.

[HS80] Joos Heintz and Claus-Peter Schnorr. Testing polynomials which are easy to compute (extended abstract). In *Proceedings of the 12th Annual ACM Symposium on Theory of Computing, 1980*, pages 262–272, 1980.

[KI04] Valentine Kabanets and Russell Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *Computational Complexity*, 13(1-2):1–46, 2004.

[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 J. Comput.*, 42(6):2114–2131, 2013.

[KS01] Adam Klivans and Daniel A. Spielman. Randomness efficient identity testing of multivariate polynomials. In *Proceedings on 33rd Annual ACM Symposium on Theory of Computing, July 6-8, 2001*, pages 216–223, 2001.

[KS07] Neeraj Kayal and Nitin Saxena. Polynomial identity testing for depth 3 circuits. *Computational Complexity*, 16(2):115–138, 2007.

[KS09] Neeraj Kayal and Shubhangi Saraf. Blackbox polynomial identity testing for depth 3 circuits. In *50th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2009*, pages 198–207, 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.

[Lov79] László Lovász. On determinants, matchings, and random algorithms. In *FCT*, pages 565–574, 1979.

[Mul12] Ketan Mulmuley. Geometric complexity theory V: equivalence between blackbox derandomization of polynomial identity testing and derandomization of noether's normalization lemma. *CoRR (also, in FOCS 2012)*, abs/1209.5993, 2012.

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

[MVV87] Ketan Mulmuley, Umesh V. Vazirani, and Vijay V. Vazirani. Matching is as easy as matrix inversion. *Combinatorica*, 7(1):105–113, 1987.

[Sch80] Jacob T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27(4):701–717, 1980.

[Sha90] Adi Shamir. IP=PSPACE. In *31st Annual Symposium on Foundations of Computer Science, St. Louis, Missouri, USA, October 22-24, 1990, Volume I*, pages 11–15, 1990.

[SS12] Nitin Saxena and C. Seshadhri. Blackbox identity testing for bounded top-fanin depth-3 circuits: The field doesn't matter. *SIAM J. Comput.*, 41(5):1285–1298, 2012.

[SV11] Shubhangi Saraf and Ilya Volkovich. Black-box identity testing of depth-4 multilinear circuits. In *Proceedings of the 43rd ACM Symposium on Theory of Computing, STOC 2011*, 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.

[Zip79] Richard Zippel. Probabilistic algorithms for sparse polynomials. In *Symbolic and Algebraic Computation, EUROSAM '79, An International Symposiumon Symbolic and Algebraic Computation*, pages 216–226, 1979.

A Hitting Set for the Product of Sparse Polynomials

Let $P_1, \ldots, P_m \in \mathbb{C}[x_1, \ldots, x_n]$ are t-sparse polynomials, and the maximum degree is bounded by d. Our goal is to construct a polynomial-size hitting set for the product polynomial $P = P_1 \cdot P_2 \cdots P_m$.

Theorem 4. *Let $P_1, \ldots, P_m \in \mathbb{C}[x_1, \ldots, x_n]$ are t-sparse polynomials, and the maximum degree is bounded by d. Then we can construct a hitting set of size $(d \cdot n \cdot m \cdot t)^{O(1)}$ for the product polynomial $P(x) = P_1(x) \ldots P_m(x)$ in polynomial time.*

Proof. We make the following substitution:

$$\forall i : x_i = y^{z^i \mod p},$$

where z is an indeterminate and the value for z will be fixed in the analysis. We will also vary p in a suitably chosen set of primes. Consider any polynomial P_i. Two different monomials $x^{\bar{e}}, x^{\bar{f}}$ will be mapped to $y^{m_{\bar{e}}(z)}$ and $y^{m_{\bar{f}}(z)}$, where $m_{\bar{e}}(z) = \sum_{i=1}^{n} e_i z^i$ and $m_{\bar{f}}(z) = \sum_{i=1}^{n} f_i z^i$. To ensure $P_i(y) \not\equiv 0$, it is enough to substitute values for z and p such that:

$$\mathcal{P}_i(z) = \prod_{\bar{e},\bar{f} \in \mathcal{S}_i} (m_{\bar{e}}(z) - m_{\bar{f}}(z)) \mod p \neq 0,$$

where $\mathcal{S}_i$ is the set of all monomials in P_i. The degree of the polynomial $\mathcal{P}_i$ (hence the number of roots) is at most $n \cdot t^2$. Considering all the polynomials $P_1, \ldots, P_m$, we would like to avoid at most $m \cdot n \cdot t^2$ values for z which are the possible roots of $\mathcal{P}(z) = \prod_{i=1}^{m} \mathcal{P}_i(z)$.

So we fix a set $\mathcal{F} = \{1, 2, \ldots, m \cdot n \cdot t^2 + 1\}$, and we substitute for z from the set $\mathcal{F}$. We know that $\mathcal{P}(z)$ will evaluate to a non-zero value for some $z_0 \in \mathcal{F}$. We also need to avoid all prime divisors of $\mathcal{P}(z_0)$. It is easy to observe that $\mathcal{P}(z_0) \leq (d \cdot m \cdot n \cdot t)^{O(m \cdot n \cdot t^2)}$. The number of prime divisors of $\mathcal{P}(z_0)$ is bounded by $O(m \cdot n \cdot t^2 \log(d \cdot m \cdot n \cdot t))$. Using prime number theorem, we get that it is enough to choose the prime p within a bound of $O(m^2 \cdot n^2 \cdot t^4 \cdot \log^2(d \cdot m \cdot n \cdot t))$.

For each such substitution of z and p, the polynomial $P(y)$ is a polynomial of degree at most $d' = O(d \cdot m^3 \cdot n^2 \cdot t^4 \cdot \log^2(d \cdot m \cdot n \cdot t))$. We can test whether the polynomial $P(y) \equiv 0$ by evaluating it on a most $d' + 1$ points. So the size of the overall hitting set is bounded by $(d \cdot m \cdot n \cdot t)^{O(1)}$ (for a small constant in the exponent as $O(1)$). $\square$

ECCC ISSN 1433-8092

http://eccc.hpi-web.de