On Parameterized Arithmetic Circuit Identity Testing of Depth Three and Four Circuits *

Purnata Ghosal, Om Prakash, and B.V. Raghavendra Rao

Department of Computer Science and Engineering
IIT Madras, Chennai, INDIA
{purnatag,op708543}@gmail.com, bvrr@cse.iitm.ac.in

Abstract. In this article we study the parameterized complexity of the Arithmetic Circuit Identity Testing Problem parameterized by the syntactic degree of the circuit. We show that ACIT for depth three $\Sigma\Pi\Sigma$ arithmetic circuits parameterized by the fan-in of the middle Π gates is fixed parameter tractable. The algorithm is obtained by an application of the hitting set generator defined by Shpilka and Volkovich [Approx-Random 2009] and the identity testing algorithm for non-commutative formulas by Raz and Shpilka [CC, 2005]. Further, we give a polynomial of degree k that can be computed by a degree k, polynomial size, depth four $\Sigma\Pi\Sigma\Pi$ circuit that requires $n^{\Omega(k)}$ size for any depth three circuit computing it.
Finally, we exhibit the limitations of the Shpilka-Volkovich generator in obtaining fixed parameter tractable algorithms for ACIT. In particular, we show that the Shpilka-Volkovich generator preserves the rank of the coefficient matrix of polynomials.

1 Introduction

Parameterized Complexity is the discipline where an additional parameter along with the input is considered for measuring the complexity of computational problems. This leads to a more fine-grained complexity classification of computational problems and a relaxed notion of tractability. Downey and Fellows [DF13] were the first to study complexity of problems with a parameter, and develop the area of parameterized complexity theory. Over the last two decades, parameterized complexity has played a pivotal role in algorithmic research [DF13].

Fixed Parameter Tractability (FPT) is the notion of tractability in Parameterized Complexity Theory. A decision problem with parameter k that is decidable in deterministic time $f(k)\mathsf{poly}(n)$, where f is an arbitrary, computable function, is said to be fixed parameter tractable (FPT for short). The whole area of parameterized complexity theory is centered around this definition of tractability. The parameterized intractable problems are based on the hierarchy of classes known as the W-hierarchy. The smallest member of W-hierarchy, W[1] consists of problems that are FPT equivalent to the clique problem with the size of the clique as the parameter.

Motivation: Parameterized complexity of problems based on graphs and other combinatorial structures played pivotal role in the development of Parameterized Algorithms and Complexity Theory. Many of the parameterized algorithms involve evaluation of polynomials of degree bounded by the parameter. For example, in [BHT12], Björklund et. al., defined and used a degree k polynomial which is identically zero if and only if the given

* A preliminary version of this article was published at the The 23rd Annual International Computing and Combinatorics Conference, COCOON 2017

graph has no cycle of length k or smaller. Polynomials of degree bounded by the parameter have been extensively used to develop efficient randomized parameterized algorithms, see e,g., [Bjö10,AFS12,FLR$^+$12]. Further, obtaining a deterministic $f(k)n^{O(1)}$ time algorithm checking if an n variate polynomial of degree at most k is zero or not for some function f of k would lead to fast deterministic FPT algorithms for a wide variety of problems. The construction of representative sets in [FLPS16] can also be viewed a parameterized derandomization of the polynomial identity testing problem for a special class of polynomials where the monomials have a matroidal structure.

Wide application of polynomials whose degree is bounded by the paramater in Parameterized Complexity Theory merits a study of such polynomials in algebraic models of computation. We initiate the study of polynomials with the degree as the parameter.

Our Model: Motivated by the applications of polynomials parameterized by degree, we study the parameterized complexity of polynomials with degree as a parameter. More specifically, given a parameter $k = k(n)$, classify the the families of polynomials of degree k based on the minimum size of the arithmetic circuit computing it. Here, the notion of efficiency is based on the fixed parameter tractability. A natural model of computation for polynomials with degree bounded by k would be arithmetic circuits where every gate computes a polynomial of degree at most k. However, such a circuit of size $f(k)n^{O(1)}$ for some function f of k can compute polynomials with coefficients as large as 2^{2^n} where n is the number of variables, and hence evaluation of such polynomials unlikely to be Fixed Parameter Tractable. Thus we need models where the coefficients computed will be representable in $f(k)n^{O(1)}$ many bits. Towards this, we consider the arithmetic circuits where the syntactic degree (see Section 2 for a definition) is bounded by the degree of the polynomial being computed as the computational model.

Further, we study the parameterized version of Arithmetic Circuit Identity Testing (ACIT) problem: testing if the given arithmetic circuit computes the zero polynomial or not. ACIT is one of the fundamental computational questions on polynomials. Schwartz [Sch80] and Zippel [Zip79] independently showed that there is a randomized polynomial time algorithm for ACIT. Their algorithm worked for a more general setting, where the polynomials are given in the black-box form. However, obtaining deterministic polynomial time algorithm for ACIT has been one of the prominent open questions for decades, playing a pivotal role in Algebraic Complexity Theory. Motivated by the application of ACIT in several parameterized algorithms [BHT12,Bjö10,AFS12,FLR$^+$12] with degree as the parameter, we study the complexity of ACIT with degree as the parameter.

Our Results: We define the notion of fixed parameter tractability (FPT) of a family of polynomials parameterized by the degree. We study the parameterized complexity of the arithmetic circuit identity testing problem and show that non-black box identity testing of depth three circuits of syntactic degree at most k is fixed parameter tractable (Theorem 5). This result is obtained by the application of a hitting set generator defined by Shpilka and Volkovich [SV09]. We also show that the techniques used in Theorem 5 cannot be used to obtain efficient parameterized identity tests for depth four circuits by proving that the generator given by [SV09] preserves rank of certain matrix associated with polynomials

(Theorem 6). Finally, we obtain a parameterized separation between depth three and four circuits (Theorem 3). Further, we show that there is a polynomial computed by depth four $\Sigma\Pi\Sigma\wedge$ circuits of polynomial size, that cannot be computed by a degree k $h(k)\text{poly}(n)$ sized $\Sigma \wedge^{o(k)} \Sigma \wedge \Sigma$ circuit (Theorem 4).

Related work: Though algebraic techniques have been well utilized in obtaining efficient parameterized algorithms, the focus on parameterized complexity of algebraic problems is very limited. Chen et. al. [CFLS13] studied the parameterized complexity of detecting and testing monomials in polynomials given as arithmetic circuits. Arvind et. al [AKKT16] obtained parameterized algorithms for solving systems of linear equations parameterized by the hamming weight. Engels [Eng16] developed Parameterized Algebraic Complexity theory in analogy to Valiant's notion of Algebraic Complexity. Apart from these results, there have not been much attention on algebraic problems in the parameterized world.

Müller [Mül08] studied several parameterized variants of the ACIT problem and obtained randomized parameterized algorithms for those variants that use $O(k \log n)$ random bits where k is the parameter. Further, Chauhan and Rao [CR15] studied ACIT with the syntactic degree of the circuit as a parameter, and showed that the problem has a randomized algorithm that uses only $O(k \log n)$ random bits, where k is the syntactic degree. Finally, it can be seen from the observations in [CR15] that ACIT with syntactic degree as a parameter is equivalent to the same problem with the number of variables as a parameter (Section 2).

2 Preliminaries

In this section we will introduce necessary notions on arithmetic circuits and parameterized complexity. For more details the reader is referred to [SY10] and [DF13].

An arithmetic circuit C over a field $\mathbb{F}$ and the set of variables $X = \{x_1, \ldots, x_n\}$ is a labelled directed acyclic graph. The nodes in C are called gates. Gates of zero in-degree are called input gates and are labelled by either variables in X, or constants in $\mathbb{F}$. Other gates in C are labelled by either $\times$ or $+$. Gates with zero out-degree are called output gates. In our applications, an arithmetic circuit will have a unique output gate. Every gate in C naturally represents a polynomial in $\mathbb{F}[x_1, \ldots, x_n]$. The polynomial computed by C is the polynomial represented at the output gate.

Depth of an arithmetic circuit is the length of the longest path from an input gate to the output gate. In this paper, our focus is on constant depth arithmetic circuits. It should be noted that, constant depth circuits are interesting only when the fan-in of gates are allowed to be unbounded. $\Sigma\Pi\Sigma$ denotes the class of depth three circuits of the form $\sum_{i=1}^{r} \prod_{j=1}^{t} \ell_{i,j}$ for some $r, t \geq 0$ and $\ell_{i,j}$s are linear functions of the input variables. Similarly, depth four $\Sigma\Pi\Sigma\Pi$ circuits are defined. The fan-in restriction on the gates at a specific layer are denoted by superscripts, e.g., $\Sigma\Pi^k\Sigma$ denotes the sub class of $\Sigma\Pi\Sigma$ circuits where the middle layer of product gates have fan-in bounded by k.

Saxena [Sax08] introduced the notion of *dual representation of polynomials*. Let $f \in \mathbb{F}[x_1, \ldots, x_n]$. Then f is said to have a dual representation of size t, if there are univariate polynomials $g_{ij}(x_j)$ such that $f = \sum_{i=1}^{t} g_{i1}(x_1) \cdots g_{in}(x_n)$.

The *syntactic degree*[1] denoted by *syntdeg* for every gate v of an arithmetic circuit is defined as follows:

$$syntdeg(v) = \begin{cases} 1 & \text{if } v \text{ is an input gate} \\ \max\{syntdeg(v_1), syntdeg(v_2)\} & \text{if } v = v_1 + v_2 \\ syntdeg(v_1) + syntdeg(v_2) & \text{if } v = v_1 \times v_2 \end{cases}$$

We need the notion of *hitting sets* for arithmetic circuits [SY10]. Let $\mathcal{C}_n$ be a class of polynomials in n variables. A set $\mathcal{H}_n \subseteq \mathbb{F}^n$ is called a hitting set the class $\mathcal{C}_n$ with n inputs, such that for all polynomials $f \in \mathcal{C}_n,\ f \not\equiv 0, \exists a \in \mathcal{H}_n,\ f(a) \neq 0$.

We also require the notion of *hitting set generators*. Consider a polynomial mapping $G = (G_1, \ldots, G_n) : \mathbb{F}^t \to \mathbb{F}^n$ where $G_1, \ldots, G_n$ are t variate polynomials. G is a generator for the circuit class $\mathcal{C}_n$ if for every polynomial $f \in \mathcal{C}_n,\ f \not\equiv 0$, it holds that $f(G) \not\equiv 0$.

It is known that that the image of a generator for polynomials in $\mathcal{C}_n$ contains a hitting-set for all non-zero polynomials in $\mathcal{C}_n$. In this paper we will require a hitting set generator defined by Shpilka and Volkovich [SV09].

Definition 1 (S-V Generator [SV09]). *Let $a_1, a_2 \ldots a_n$ be distinct elements in the given field $\mathbb{F}$. Let $G_k^i \in \mathbb{F}[y_1, y_2 \ldots y_k, z_1, z_2 \ldots z_k]$ be the polynomial defined as follows:*

$$G_k^i(y_1, y_2 \ldots y_k, z_1, z_2 \ldots z_k) = \sum_{j=1}^{k} L_i(y_j) z_j, \text{ where } L_i(x) = \frac{\prod_{j \neq i}(x - a_j)}{\prod_{j \neq i}(a_i - a_j)}.$$

The generator G_k is defined as $G_k \stackrel{\Delta}{=} (G_k^1, \ldots G_k^n)$.

For a polynomial f, $G_k(f)$ is the image of f under G_k, i.e, $G_k(f) = f(G_k^1, \ldots, G_k^n)$. In [SV09], Shpilka and Volkovich showed that G_k is a hitting set generator for sum of k read-once polynomials. Further, in [CR15] Chauhan and Rao showed that the generator G_k is also a hitting set generator for degree k polynomials. We state the result without proof.

Lemma 1. *[CR15] Let $f \in \mathbb{F}[X]$ with $deg(f) \leq k$, then $f \equiv 0 \iff G_k(f) \equiv 0$, where G_k is as in Definition 1.*

They show that the identity of the polynomial p is preserved over a subset $S,\ |S| = k+1$ of inputs of Hamming weight k, k being the syntactic degree of the polynomial. Using Lemma 1, we can reduce identity testing of an n-variate degree-k polynomial to the identity testing of a $2k$-variate degree-nk polynomial. It is enough to see that the polynomial $G_k(p)$ preserves the identity of p over all possible choices of S.

Parameterized Complexity A *parameterized problem* is a set $P \subseteq \Sigma^* \times \mathbb{N}$, where Σ is a finite alphabet. If $(x, k) \in \Sigma^* \times \mathbb{N}$ is an instance of a parameterized problem, we refer to x as the input and k as the parameter.

[1] Syntactic degree is also known as the formal degree [KSS14] and is a standard parameter for arithmetic circuits

Definition 2 (Fixed Parameter Tractability). *A parameterized problem $P \subseteq \Sigma^* \times \mathbb{N}$ is fixed-parameter tractable if there is a computable function $f : \mathbb{N} \to \mathbb{N}$, a constant $c \in \mathbb{N}$ and an algorithm that, given a pair $(x, k) \in \Sigma^* \times \mathbb{N}$, decides if $(x, k) \in P$ in at most $f(k)poly(n)$ steps, where n is the length of input.*

Definition 3 (FPT). *FPT is the class of parameterized problems that are fixed parameterized tractable.*

ACIT is the problem of testing whether a given arithmetic circuit C computes a polynomial p that is identically zero. There have been several parameterized variants of ACIT studied in the literature [Mül08]. Following [CR15] we consider the syntactic degree of the arithmetic circuit as a parameter.
Problem: para-ACIT
INPUT: A polynomial p given as an arithmetic circuit C of syntactic degree k.
PARAMETER: k
OUTPUT: YES if $p \equiv 0$.

Chauhan and Rao [CR15] show that $\mathsf{para} - \overline{\mathsf{ACIT}} \in \mathsf{W[P]} - \mathsf{RFPT}$, a parameterized class analogous to RP. In this paper we consider the problem when restricted to depth three circuits.

Coefficient Matrix of a polynomial We consider the notion of partial derivative matrix of a polynomial defined by Nisan [Nis91] and later used in [NW96]. Raz [Raz09] used a variant of partial derivative matrix, which was later generalized by Kumar et al [KMS13]. In this paper we consider yet another variant of partial derivative matrices, which we call as the *coefficient matrix*.

Definition 4. *Let $f \in \mathbb{F}[x_1, \ldots, x_n]$ be a polynomial of degree d, $\varphi : X \to Y \cup Z$ be a partition of the input variables of f. Then the coefficient matrix M_{f^φ} has its rows indexed by monomials μ of degree at most d in variables in Y, and columns indexed by monomials ν of degree at most d in variables in Z. For monomials μ and ν respectively in variables Y and Z, the entry $M_{f^\varphi}(\mu, \nu)$ is the coefficient of the monomial $\mu\nu$ in f.*

Remark 1. It should be noted that the definition above is different from the notion of polynomial coefficient matrices in [KMS13], where the entries of the matrix are polynomials rather than field elements. Whereas, our definition is nothing but that in [Nis91] except that we use a partition of variables.

The coefficient matrix of a matrix is well studied in the literature in various forms, the specific form used in the above definition has not been mentioned explicitly in the literature. The following fundamental properties of the rank of the coefficient matrix follow directly from [Raz09].

Lemma 2 (Sub-additivity). *If $f, g, h \in \mathbb{F}[X]$ such that $f = g + h$, then $\forall \varphi : X \to Y \cup Z$, $\mathsf{rank}(M_{f^\varphi}) \leq \mathsf{rank}(M_{g^\varphi}) + \mathsf{rank}(M_{h^\varphi})$.*

Proof. The above claim holds by matrix addition and subsequent Gaussian elimination. The upper bound is tight when $g \in \mathbb{F}[A], h \in \mathbb{F}[B]$ such that $A, B \subseteq X, A \cap B = \phi$, as otherwise rows r_1 in M_{g^φ}, and r_2 in M_{h^φ} having same entries corresponding to the monomials in variables in $A \cap B$, and 0 entries elsewhere, cancel out to give a lower rank.

Lemma 3 (Sub-multiplicativity). *If $f, g, h \in \mathbb{F}[X]$ such that $f = g \cdot h$, then $\forall \varphi : X \to Y \cup Z$, $\mathsf{rank}(M_{f^\varphi}) \leq \mathsf{rank}(M_{g^\varphi}) \times \mathsf{rank}(M_{h^\varphi})$.*

Proof. Let g and h be variable disjoint, i.e $\mathsf{var}(g) \cap \mathsf{var}(h) = \phi$. Then, as $\varphi : X \to Y \cup Z$, we can define $\varphi|_g : X_g \to Y_1 \cup Z_1$, and $\varphi|_h : X_h \to Y_2 \cup Z_2$, where $X_g = \mathsf{var}(g),\ X_h = \mathsf{var}(h)$, $Y = Y_1 \cup Y_2$, $Z = Z_1 \cup Z_2$.

Now, rows in M_{f^φ} are indexed by monomials in variables in Y, and columns are indexed by monomials in variables in Z. So each row index of M_{f^φ} can be written as a product of $\exists m_{11}, m_{12}$, monomials in variables in Y_1 and Y_2 respectively. Similarly, each column index of M_{f^φ} can be written as a product of $\exists m_{21}, m_{22}$, monomials in variables in Z_1 and Z_2 respectively.

Then, $\forall m_1, m_2\ M_{f^\varphi}(m_1, m_2) = ab$, where $M_{g^\varphi}(m_{11}, m_{21}) = a$, $M_{h^\varphi}(m_{12}, m_{22}) = b$. Hence, $\mathsf{rank}(M_{f^\varphi}) = \mathsf{rank}(M_{g^\varphi}) \times \mathsf{rank}(M_{h^\varphi})$.

In case $\mathsf{var}(g) \cap \mathsf{var}(h) \neq \phi$, the rows indexed by $m_{g,p_1} m_{h,q_1}$ and $m_{g,p_2} m_{h,q_2}$ are added up for all distinct row, column pairs (p_i, q_i) if $m_{g,p_1} m_{h,q_1} = m_{g,p_2} m_{h,q_2}$. Hence, the rank of M_{f^φ} can be lower than $\mathsf{rank}(M_{g^\varphi}) \times \mathsf{rank}(M_{h^\varphi})$.

The following is a simple observation regarding polynomial identities.

Lemma 4. *For a polynomial $h \in \mathbb{F}[X]$, and all partitions $\varphi : X \to Y \cup Z$, $\mathsf{rank}(M_{h^\varphi}) = 0 \iff h \equiv 0$.*

Proof. For the forward direction, we can see that M_{h^φ} has no non-zero entries. If $h \not\equiv 0$, then there must be at least one monomial in h with a non-zero coefficient. But, then, $\mathsf{rank}(M_{h^\varphi}) \geq 1$. Hence, $h \equiv 0$.

Similarly, if $h \equiv 0$, all the monomials in h have coefficient 0, hence all entries of M_{h^φ} should be 0. Therefore, $\mathsf{rank}(M_{h^\varphi}) = 0$.

Recall that an arithmetic circuit is a *formula* if the out-degree of every gate is either one or zero. Finally, we need the following result on testing identity of non-commutative formulas. Let $\mathbb{F}\{x_1, x_2 \ldots, x_n\}$ be the non-commutative polynomial ring over the field $\mathbb{F}$. The following theorem was proved by Raz and Shpilka [RS05].

Theorem 1. *[RS05] Let $C \in \mathbb{F}\{X\}$ be a non-commutative arithmetic formula, then there is a white-box identity testing algorithm for C having time complexity linear in size(C).*

3 Arithmetic Computation with degree as a parameter

In this section, we consider arithmetic circuits for polynomials parameterized by degree. We define the notions of fixed parameter tractability for polynomials with degree as the

parameter and then consider the feasibility of parameterized depth reduction. Finally we prove lower bounds against depth three $\Sigma\Pi^k\Sigma$ circuits and depth five $\Sigma \wedge^{o(k)} \Sigma \wedge^{o(k)} \Sigma$ circuits. Our results imply that a parameterized version of the depth reduction given by Agrawal and Vinay [AV08] is not possible with full generality.

3.1 Fixed Parameter Tractability in Arithmetic Computation

In this section we define the notion of parameterized tractability of polynomials over $\mathbb{Z}$ parameterized by degree.

Definition 5. *Let $k = k(n)$. A family $(p_n)_{n\geq 0}$ of polynomials over $\mathbb{Z}$ is said to be degree k parameterized if*

- *There is a $c > 0$ such that p_n is an n^c variate polynomial for every $n \geq 0$;*
- *Degree of p_n is bounded by $k = k(n)$ for every $n \geq 0$; and*
- *The absolute value of the coefficients of p_n is bounded by $2^{g(k)n^c}$, for some function g that depends only on k.*

Since any arithmetic circuit can be homogenized efficiently, we have:

Proposition 1. *[Bür13] For any parameterized polynomial family (p, k) if there is a family of arithmetic circuits $C = (C_n)_{n\geq 0}$ of size $f(k)n^c$ computing p, where $f(k)$ is a function of k and c is a constant, then there is a family of arithmetic circuits $C' = (C'_n)$ of size $f'(k)n^{c'}$ for p such that every gate in C'_n computes a polynomial of degree at most k.*

It can be seen that a circuit C_n of size $f(k)n^{O(1)}$ where every gate computes a polynomial of degree at most k can compute polynomials where the absolute value of the coefficient can be as large as $2^{2^{n^{O(1)}}}$ even when the constants allowed in the circuit are from $\{-1, 0, 1\}$. This makes the evaluation of such polynomial in FPT time infeasible. A natural restriction would be to bound the syntactic degree of the circuit. An arithmetic circuit C_n is said to be of syntactic degree d if every gate in C_n has syntactic degree bounded by d.

A degree parameterized polynomial family $(p = (p_n)_{n\geq 0}, k)$ with $k = k(n)$ as the parameter is said to be *fixed parameter tractable* (FPT) if for every $n \geq 0$, there is an arithmetic circuit C_n of syntactic degree at most k and of size $f(k)n^c$ computing p_n where f is a function of k and c is a constant.

3.2 Parameterized Depth Reduction

Depth reduction is one of the most fundamental structural aspects in algebraic complexity theory: Given a polynomial family $p = (p_n)_{n\geq 0}$ and a size bound $s = s(n)$, what is the minimum depth of an arithmetic circuit of size s computing p? The parameterized depth reduction problem can be stated as:
Given a parameterized polynomial family (p, k) in FPT what is the minimum depth of a size $f(k)n^c$ circuit computing p where $f(k)$ is an arbitrary function of k and c is some constant?

By applying the well known depth reduction technique in [VSBR83], we have:

Proposition 2. *[VSBR83] Any parameterized polynomial family (p, k) in FPT can be computed by circuits of depth $f(k)\log n$ and size $f'(k)n^{O(1)}$, for some functions f and f' that depend only on the parameter.*

In a surprising result, Agrawal and Vinay [AV08] showed that any homogeneous polynomial p computed by polynomial size arithmetic circuits can be computed by depth four $\Sigma\Pi^{\sqrt{n}}\Sigma\Pi^{\sqrt{n}}$ homogeneous circuits of size $2^{o(n)}$. Further, Tavenas [Tav15] improved this bound to $2^{\sqrt{n}\log n}$. Over infinite fields, there is a depth three $\Sigma\Pi\Sigma$ circuit of size $2^{\sqrt{n}\log n}$ for p [GKKS13].

A parameterized counterpart of the depth reduction in [AV08] would be to transform a circuit C_n of size $f(k)n^{O(1)}$ and syntactic degree k to a depth four $\Sigma\Pi\Sigma\Pi$ circuit of syntactic degree k and size $f'(k)n^{O(1)}$ where f and f' are functions of k alone. Note that a $\Sigma\Pi\Sigma\Pi$ circuit C of syntactic degree k will have Π fan-in bounded by k at both of the Π layers. So we can assume it to be of the form $\Sigma\Pi^k\Sigma\Pi^k$. Further, if C is homogeneous with the bottom Π layer having syntactic degree t then C can be assumed to be a homogeneous $\Sigma\Pi^{k/t}\Sigma\Pi^t$ circuit. We first observe that we can replace Π gates with $\wedge$ (powering) gates in any depth four circuit with syntactic degree bounded by the parameter k. The proof is a direct application of Fischer's identity [Fis94] twice and is omitted.

Lemma 5. *Let C be a $\Sigma\Pi^{k/t}\Sigma\Pi^t$ circuit of size s computing a polynomial p over $\mathbb{Z}$. Then there is a $\Sigma \wedge^{k/t} \Sigma \wedge^t \Sigma$ circuit C' of size $\max\{2^{k/t}, 2^t\} \cdot s$ computing p. Moreover, if C is homogeneous, so is C'.*

Thus a parameterized version of depth reduction in [AV08] would imply that every parameterized polynomial family (p, k) in FPT can be computed by a homogeneous $\Sigma \wedge^{O(\sqrt{k})} \Sigma \wedge^{O(\sqrt{k})} \Sigma$ circuit of size $f(k)n^{O(1)}$ for some function f of k. However, in the next section, we show that if the degree of top layer of powering gates is bounded by $o(k)$, then this is not possible.

3.3 Parameterized Lower Bounds against constant depth circuits

In this section we prove parameterized lower bounds against depth three $\Sigma\Pi^k\Sigma$ and restricted depth five $\Sigma \wedge \Sigma \wedge \Sigma$ circuits with powering and sum gates.

Depth Three Circuits In this section, we show that there are polynomial families parameterized by degree, computable by depth four circuits such that any depth three $\Sigma\Pi^k\Sigma$ circuit computing it has size $n^{\Omega(k)}$ we observe that there is a polynomial computed by parameterized depth four circuits that has large rank .

Lemma 6. *Let $X = \{y_1, \ldots, y_m, z_1, \ldots, z_m\}$. Let $f = \prod_{i=1}^{k} Q_i$ where*

$$Q_i = (1 + y_{\frac{(i-1)m}{k}+1} z_{\frac{(i-1)m}{k}+1} + y_{\frac{(i-1)m}{k}+2} z_{\frac{(i-1)m}{k}+2} + \ldots + y_{\frac{im}{k}} z_{\frac{im}{k}})$$

are multivariate quadratic polynomials in $\mathbb{F}[X]$, then $\exists \varphi : X \to Y \cup Z$ such that $\mathsf{rank}(M_{f^\varphi}) = \Omega((\frac{m+k}{k})^k)$.

Proof. Let $\mid Y \mid = \mid Z \mid = m$ and $Y = \{y_1, y_2, \ldots, y_m\},\ Z = \{z_1, z_2, \ldots, z_m\}$. Let us consider the natural partition $\varphi : X \to Y \cup Z$. By expanding f^φ we get: $f^\varphi = (1 + y_1z_1 + \cdots + y_{\frac{m}{k}}z_{\frac{m}{k}}) \ldots (1 + y_{\frac{(k-1)m}{k}+1}z_{\frac{(k-1)m}{k}+1} + \ldots + y_mz_m)$.

Hence, f^φ is product of k quadratic polynomials such that each monomial is of the form pq or 1 where p is product of y_i's and q is product of z_i's. So, the coefficients of all monomials correspond to the diagonal elements of the coefficient matrix M_{f^φ} assuming natural ordering of indices as $1 \preceq z_1 \preceq z_2 \preceq \ldots \preceq z_1z_2 \preceq \ldots z_1z_2z_3 \ldots$ and similarly for row indices. Thus, $\mathsf{rank}(M_{f^\varphi}) = \left(\frac{m}{k} + 1\right)^k = \binom{m+k}{k}$, and partition function φ is the required partition. This completes the proof.

Now, we need the folklore fact that for any partition of its variables, a polynomial with a 'small' dual representation will have rank of the coefficient matrix small.

Lemma 7. *(folklore) Suppose $f = \sum_{i=1}^{t} g_{i,1}(x_1)g_{i,2}(x_2) \ldots g_{i,n}(x_n)$. Then, for all partitions $\varphi : X \to Y \cup Z$, $\mathsf{rank}(M_{f^\varphi}) \leq t$ where $g_{i,1},\ g_{i,2}, \ldots, g_{i,n}$ are univariate polynomials in $x_1, x_2, \ldots, x_n$ respectively.*

Proof. Since $g_{i,j}$'s are univariate polynomials, for all partitions φ, the coefficient matrix $M_{g_{i,j}^\varphi}$ has rank 1. Then, for all partitions $\varphi : X \to Y \cup Z$, it follows from the sub-additivity and sub-multiplicativity of the measure that $\mathsf{rank}(M_{g_{i,1}^\varphi \cdots g_{i,n}^\varphi}) = 1$. Thus, $\forall \varphi,\ \mathsf{rank}(M_{f^\varphi}) \leq t$.

As an immediate consequence of Lemmas 7 and 6 we have:

Theorem 2. *There exists a polynomial $f \in \mathbb{F}[x_1, \ldots, x_n], f = \sum_{i=1}^{s} \prod_{j=1}^{d_i} Q_{i,j}$, where $s > 0$, $Q_{i,j}$ is a multivariate quadratic polynomial with $max_i\{d_i\} \leq k$, such that*

$$f = \Sigma_{i=1}^{t} g_{i,1}(x_1)g_{i,2}(x_2) \ldots g_{i,n}(x_n) \implies t = n^{\Omega(k)},$$

where $g_{i,1}g_{i,2} \ldots g_{i,n}$ are univariate polynomials of syntactic degree k.

Further, we observe that depth three $\Sigma\Pi\Sigma$ circuits of syntactic degree k, compute polynomials of 'small' degree under every partition:

Lemma 8. *Let $f \in \mathbb{F}[x_1, \ldots, x_n], f \in \Sigma\Pi^k\Sigma$ and M_{f^φ} is the coefficient matrix corresponding to the partition of variables of f, $\varphi : X \to Y \cup Z$. Then $\mathsf{rank}(M_{f^\varphi}) \leq s \cdot 2^{O(k)}$, where s is the smallest size of a $\Sigma\Pi^k\Sigma$ circuit for f.*

Proof. Let $f \in \mathbb{F}[x_1, \ldots, x_n], f \in \Sigma\Pi^k\Sigma$. Hence $f = \sum \prod^k \sum_i^n a_ix_i$, where $a_i \in \mathbb{F}$. Then, $\forall \varphi,\ \mathsf{rank}(M_{f^\varphi}) \leq 2^{O(k)}s$ since $\mathsf{rank}(M_{\ell^\varphi}) \leq 2$, for all linear functions $\ell = \sum_{i=1}^{n} a_ix_i$; and rank of the coefficient matrix is sub-multiplicative and sub-additive.

Combining Lemma 6 and Lemma 8 we get the following:

Theorem 3. *Let $f \in \mathbb{F}[x_1, \ldots, x_n]$, $f \in \Sigma\Pi^{k/2}\Sigma\Pi^2$ such that f has degree k, then any depth-3 $\Sigma\Pi^k\Sigma$ circuit computing f has size $n^{\Omega(k)}$.*

Proof. Let f be the polynomial defined in Lemma 6, $f = \prod_{i=1}^{k} Q_i$. Then, there is some partition φ, for which f has $\mathsf{rank}(M_{f^\varphi}) = \Omega(g(k)n^k)$, for some function g (putting $m = \frac{n}{2}$).

Now, for all polynomials p computed by depth-3 $\Sigma\Pi^k\Sigma$ circuits, we know from Lemma 8, $\mathsf{rank}(M_{f^\varphi}) = s2^{O(k)}$ for all partitions $\varphi : X \to Y \cup Z$.

Hence, the least size s of a depth-3 $\Sigma\Pi^k\Sigma$ circuit computing f would be $\Omega(\frac{g(k)n^k}{2^k}) = n^{\Omega(k)}$, since $k = o(n)$.

Thus, we can conclude that FPT-sized depth-4 $\Sigma\Pi^{\frac{k}{2}}\Sigma\Pi^2$ circuits strictly contain the class of FPT-sized depth-3 $\Sigma\Pi^k\Sigma$ circuits.

From Theorems 2 and 3 it follows that there are depth four $\Sigma\Pi^{k/t}\Sigma\Pi^t$ arithmetic circuits that cannot have dual representation of FPT size.

Lower bound against $\Sigma \wedge \Sigma \wedge \Sigma$ circuits In this section, we consider $\Sigma \wedge^{O(\frac{k}{t})} \Sigma \wedge^t \Sigma$ circuits. By Lemma 5, we know that $\Sigma\Pi^{O(\frac{k}{t})}\Sigma\Pi^t$ circuit of size s can be transformed into a $\Sigma \wedge^{O(\frac{k}{t})} \Sigma \wedge^t \Sigma$ circuit of size $s2^{\max\{k/t,t\}}$. In fact Lemma 5 hold for any chosen $t \leq k$. We show that there is a polynomial computable by depth four $\Pi^k\Sigma\wedge^2$ circuits of polynomial size that cannot be computed by a $\Sigma \wedge^{o(k)} \Sigma \wedge^k \Sigma$ circuit of size $g(k)n^{O(1)}$.

Let $f \in \mathbb{F}[X]$ be such that $f = \ell_1^d + \ell_2^d + \cdots + \ell_t^d$ where each ℓ_i is a linear form in n variables and $t = g(k)\mathsf{poly}(n)$ for some computable $g : \mathbb{N} \to \mathbb{N}$. We prove:

Theorem 4. *There is a polynomial p computed by a $\Pi^{k/2}\Sigma\wedge^2$ circuit of polynomial size such that any $\Sigma \wedge^\alpha \Sigma \wedge^d \Sigma$ circuit computing p has size $n^{\Omega(k)}$, for any $\alpha = o(k)$.*

This in turn implies that a parameterized version of depth reduction in [AV08] is not possible when the top layer of product gates have fan-in bounded by $o(k)$:

Corollary 1. *There is a parameterized family of polynomials that can be computed by depth four circuits of polynomial size, but any depth four $\Sigma\Pi^{o(k)}\Sigma\Pi^k$ circuit computing it requires size $n^{\Omega(k)}$.*

Let $\partial^{\leq k}(f)$ be the space spanned by k^{th} order partial derivatives of a polynomial f. Let $\dim(S)$ denote the dimension of the space spanned by polynomials in $S \subseteq \mathbb{F}[X]$. We show that Theorem 4 follows immediately from Lemma 9 and 10.

Lemma 9. *Let $\alpha = o(k)$ and $f = \ell_1^d + \ell_2^d + \cdots + \ell_t^d$ where $\ell_1, \ldots, \ell_t$ are linear forms in $\{x_1, \ldots, x_n\}$ and $t = g(k)n^c$ for some $c > 0$. Then $dim(\langle \partial^{\leq r} f^\alpha \rangle) \leq g'(k)n^{o(k)}$ for some computable function g' and $r = o(k)$.*

Proof. Note that, for any $r < k$, we have

$$\langle \partial^{=r} f^\alpha \rangle \subseteq \mathbb{F} - \text{span}\left\{ f^{\alpha-i} \odot \ell_{j_1}^{d-r_1} \cdot \ldots \cdot \ell_{j_i}^{d-r_i} \;\middle|\; i \in [r], \, {}^{r_1+\ldots+r_i=r}_{j_1,\ldots,j_i \in [t]} \right\},$$

assuming $\alpha < r < k$.

Now, there can be at most r^i partitions of r into $r_1, \ldots, r_i$. There are $\binom{t}{i}$ linear terms whose powers add up to $r(d-1)$. Hence the dimension of $\mathbb{F} - \text{span}(\langle \partial^{\leq r} f^\alpha \rangle)$ is bounded by $\sum_{i=1}^{\alpha} \binom{t}{i} r^i \leq k\binom{t}{\alpha} k^\alpha$. Given that $t = g(k)n^c$ for some $c > 0$ and g a function of k, we get $\dim(\mathbb{F} - \text{span}(\langle \partial^{\leq r} f^\alpha \rangle)) \leq g'(k)n^{o(k)}$, where $g'(k) = kg(k)^k$.

Now, we give a parameterized polynomial with large dimension of partial derivatives:

Lemma 10. *There is a polynomial $p \in \mathbb{F}[x_1, \ldots, x_n]$ of degree k that con be computed by polynomial size $\Pi\Sigma\wedge^2$ circuits with $\dim(\partial^{\leq k/2}p) = n^{\Omega(k)}$.*

Proof. The polynomial p is defined as follows:

$$p = (x_1^2 + \cdots + x_{\frac{2n}{k}}^2) \cdot \cdots \cdot (x_{\frac{2(k-1)n}{k}+1}^2 + \cdots + x_n^2).$$

Let $B_i \subseteq \{x_1, \ldots, x_n\}$ such that $B_i = \{x_{\frac{2n}{k}(i-1)+1}, \ldots, x_{\frac{2ni}{k}}\}$, $\forall i \in \{1, \ldots, \frac{k}{2}\}$.

Let $T \subset \{x_1, \ldots, x_n\}$, with $|T| = r$. If $\exists x_p, x_q \in T$ such that $\exists i, x_p, x_q \in B_i$, then $\frac{\partial^r p}{\partial T} = 0$. Otherwise, T contains exactly one variable from r choices of B_is, $r < \frac{k}{2}$, hence:

$$\frac{\partial^r p}{\partial T} = c_T \prod_{x_t \in T} x_t \prod_{j=1}^{\frac{k}{2}-r} p_{i_j},$$

where c_T is a constant and $p_\ell = x_{\frac{2n}{k}(\ell-1)+1}^2 + \ldots + x_{\frac{2n\ell}{k}}^2$. So $\forall \ell$ such that $T \cap B_\ell = \phi$, $p_\ell \mid \frac{\partial^r p}{\partial T}$.

Therefore, $\dim(\langle \partial^{=r} p \rangle) = \binom{\frac{k}{2}}{r} \left(\frac{2n}{k}\right)^r$. For all $r < \frac{k}{2}$, we can say $\dim(\langle \partial^{\leq r} p \rangle) = \frac{n^{\Omega(k)}}{g(k)}$ for some function g.

Combining this with Lemma 9, we can prove Theorem 4:

Proof (of Theorem 4). Suppose p is computable by a $\Sigma \wedge^\alpha \Sigma \wedge^d \Sigma$ circuit of top fan-in s for $\alpha = o(k)$. Then by Lemma 9, we get $\dim(\langle \partial^{\leq r} p \rangle) \leq s \cdot g'(k) n^{o(k)}$, for any $r < k$. By Lemma 10, we have $\dim(\langle \partial^{\leq r} p \rangle) = \frac{n^{\Omega(k)}}{g(k)}$. Therefore we conclude that $s = n^{\Omega(k)}$.

Remark 2. Note that, in the above, it is necessary that $\alpha = o(k)$. Also, the value of d does not affect the upper bound, in fact, the proof holds even when $d = \Omega(k)$. However, for $\alpha = \Omega(k)$, the above proof is not effective in proving the separation between depth-4 circuits and depth-5 powering circuits.

4 Parameterized Identity Testing

In this section we look at depth three $\Sigma\Pi\Sigma$ circuit where the fan-in of the Π gate is bounded by a function of the parameter k. We give a deterministic white-box identity testing algorithm for depth-3 $\Sigma\Pi^k\Sigma$ arithmetic circuits running in FPT-time with k as the parameter.

Theorem 5. *Let f be a polynomial of the form $\sum_{i=1}^m \prod_{j=1}^{d_i} \ell_{i,j}$ where $\ell_{i,j}$s are linear forms, C be a circuit computing f where $d_i \leq k$. There is a white-box identity testing algorithm for C that runs in time $g(k).size(C)^{O(1)}$, where g is a computable function, i.e., the white-box ACIT for $\Sigma\Pi\Sigma$ circuits with syntactic degree as the parameter is in FPT.*

Proof (of Theorem 5). The overall approach is as follows. We apply the Shpilka-Volkovich generator on the polynomial f computed by a $\Sigma\Pi^k\Sigma$ circuit of size C. We observe that the resulting polynomial has a polynomial size dual representation and hence can be thought of as a non-commutative formula whose size is bounded by $g(k) \cdot \mathsf{poly}(s)$ where s is the size of C. The required result follows from Theorem 1.

Note that , since $deg(f) \leq k$ by Lemma 1 we have $f(X) \equiv 0$ if and only if $G_k(f) \equiv 0$. Suppose that $\ell_{i,j} = a_{0,ij} + a_{1,ij}x_1 + a_{2,ij}x_2 + \ldots + a_{n,ij}x_n$ where $a_{1,ij}, \ldots, a_{n,ij} \in \mathbb{F}$. Substituting polynomials for $x_1 = G_k^1, x_2 = G_k^2 \ldots x_n = G_k^n$ we get, $G_k(f) \equiv \sum_{i=1}^{m} \prod_{j=1}^{d_i} \ell'_{ij}$, where,

$$\begin{aligned}
\ell'_{ij} &= a_{0,ij} + a_{1,ij}G_k^1 + a_{2,ij}G_k^2 \cdots + a_{n,ij}G_k^n \\
&= a_{0,ij} + a_{1,ij}\sum_{p=1}^{k} L_1(y_p)z_p + a_{2,ij}\sum_{p=1}^{k} L_2(y_p)z_p + \ldots + a_{n,ij}\sum_{p=1}^{k} L_n(y_p)z_p \\
&= a_{0,ij} + \sum_{r=1}^{n} a_{r,ij}\sum_{p=1}^{k} L_r(y_p)z_p \\
&= a_{0,ij} + \sum_{p=1}^{k} z_p \sum_{r=1}^{n} a_{r,ij}L_r(y_p) \quad \text{by rearranging the terms,} \\
&= a_{0,ij} + \sum_{p=1}^{k} z_p \cdot h_{ij}(y_p), \\
&\text{where } h_{ij} \text{ is a univariate polynomial of degree at most } n.
\end{aligned}$$

By expanding the product of sums to sum of products, we get:

$$G_k(f) = \sum_{i=1}^{m}\sum_{l=1}^{t} g_{il,1}(y_1)g_{il,2}(y_2)\ldots g_{il,k}(y_k) \cdot z_1^{e_{il,1}} z_2^{e_{il,2}} \ldots z_k^{e_{il,k}} \tag{1}$$

where $t \leq k^k$, $\forall p \in [k], e_{il,p} \leq d_i \leq k$, $g_{il,1}(y_1), \ldots, g_{il,k}(y_k)$ are constants or univariate polynomials in variables in $\{y_1, y_2, \ldots, y_k\}$ of degree n. Now, it is not hard to see that (1) is indeed a dual representation of the polynomial $G_k(f)$. (See [Sax08] for more on dual representations of polynomials.) Considering the ordering of the variables: $y_1 \preceq y_2 \ldots \preceq y_k \preceq z_1 \preceq z_2 \ldots \preceq z_k$, (1) can be assumed to be a non-commutative formula for $G_k(f)$ of size $O(mnk^{k+1})$. Now, from Theorem 1, we have a deterministic white-box algorithm for testing if $G_k(f) \equiv 0$ that runs in time polynomial in $O(mnk^{k+1}) = O(g(k)mn)$, where $g(k) = k^{k+1}$. Thus we have an $g(k)\mathsf{poly}(s)$ time deterministic white-box algorithm for testing if $f \equiv 0$ as required.

In Section 5, we show that the approach used in Theorem 5 does not generalize to depth four circuits.

5 S-V generator preserves rank

In Section 3.3 we concluded that there are polynomials computed by circuits of depth higher than three that do not have a dual representation. The natural next step would be to investigate whether there is a possibility of getting a dual representation via the application of S-V generator. However, in this section, we show that images of a polynomial f under the S-V generator have many partitions where the coefficient matrix has non-FPT rank provided f has one such partition.

Here, we show that the rank of the coefficient matrix of a polynomial acts as an invariant for the S-V generator. By Lemma 6, this implies that the result in Theorem 5 cannot be generalized to depth four $\Sigma\Pi^k\Sigma\Pi^k$ circuits.

Theorem 6. *Let $f \in \mathbb{F}[x_1, \ldots, x_n]$ be a polynomial of degree $\leq k$. Let $g = G_{2k}(f)$. Then,*

$$\exists \varphi, \mathsf{rank}(M_{f^\varphi}) \geq r \implies \mathbf{Pr}_{\varphi'}[\mathsf{rank}(M_{g^{\varphi'}}) = \Omega(r)] \geq \Omega(1/k^2),$$

where the probability is taken over the uniform distribution over the set of all partitions of a set of $4k$ variables into two parts with equal size.

Approach In order to prove that rank is preserved under the map G_k, we show that rank many linearly independent rows of the polynomial f remain linearly independent in the coefficient matrix of the image polynomial $g = G_k(f)$. However, this does not immediately give a partition in the variables of g so that the coefficient matrix has high rank. We show that, in fact for at least $1/k^2$ fractions of the partitions of variables of g, the coefficient matrix of g has large rank.

Proof (of Theorem 6). Fix $a_1, \ldots, a_n \in \mathbb{F}$ be distinct elements. Recall that the generator G_k with respect to $a_1, \ldots, a_n$ is defined as $(G_k^1, \ldots, G_k^n)$, i.e, $G_k(x_i) = G_k^i \ \forall i \in \{1, \ldots, n\}$. Consider :

$$\begin{aligned}
G_k(x_i) &= \sum_{p=1}^{k} z_p L_i(y_p) \\
&= \sum_{p=1}^{k} z_p \frac{\prod_{j \neq i}(y_p - a_j)}{\prod_{j \neq i}(a_i - a_j)} \\
&= \sum_{p=1}^{k} z_p \frac{(y_p - a_1)\ldots(y_p - a_{i-1})(y_p - a_{i+1})\ldots(y_p - a_n)}{(a_i - a_1)\ldots(a_i - a_{i-1})(a_i - a_{i+1})\ldots(a_i - a_n)} \\
&= \sum_{p=1}^{k} \sum_{q=1}^{n} b_p z_p y_p^{n-q} (-1)^q \mathsf{SYM}_{n-1,q-1} \quad \text{(by expanding the product, } b_p \text{ is a constant)} \\
&= \sum_{\substack{p \in [k] \\ q \in [n]}} z_p y_p^{n-q} c_{pqi} \quad \text{(where } c_{pqi} = b_p (-1)^q \mathsf{SYM}_{n-1,q-1}(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)).
\end{aligned}$$

Multiplying out k terms obtained above, we get

$$G_k(x_{i_1}x_{i_2}\dots x_{i_k}) = \sum_{\substack{p_1,\dots,p_k\in[k]\\ q_1\dots q_k\in[n-1]}} z_{p_1}\dots z_{p_k}y_{p_1}^{n-q_1}\dots y_{p_k}^{n-q_k}\prod_{j=1}^{k} c_{p_jq_ji_j}$$

Let $\mathcal{M}_k$ be the set of all degree k monomials in the variables $\{x_1,\dots,x_n\}$, and $\mathcal{S}_{nk}$ be the set of all monomials of the form $\prod_{i\in I} z_i y_i^{n-q_i}$, for all multi-sets $I\subseteq\{1,\dots,k\}$ of size k and $\mathsf{q}=(q_1,\dots,q_k)$ with $1\le q_i\le n-1$.

Let $V=\text{Span}(\mathcal{M}_k)$, and $W=\text{Span}(\mathcal{S}_{nk})$ be the vector spaces spanned by the sets. The vector space V contains all polynomials in $\mathbb{F}$ of degree k, and hence the dimension of V is $\binom{n+k}{k}$. Also, dimension of W is bounded by $\binom{2k}{k}n^k$. Note that G_k is indeed a linear map from V to W. Let C be the $\binom{n+k}{k}\times\binom{2k}{k}n^k$ matrix representing G_k. Then, $\forall v\in V,\ G_k(v)=C^Tv\in W$. Now, we argue that C has full row-rank.

Claim. C has full row-rank.

Proof (of the Claim). Suppose C is not of full row rank. Then $\exists\ \alpha_{i_1},\dots,\alpha_{i_r}\in\mathbb{R}$, such that $\sum_{j=1}^{r}\alpha_{i_j}C[i_j]=0$ with $\alpha_{i_j}\neq 0$ for some j, where $C[i]$ represents the i^{th} row of C, and $r\le\mathsf{dim}(V)$. Hence, as G_k is linear, we deduce that $\exists v_{i_1},\dots,v_{i_r}\in V$ such that $G_k(v_{i_j})=C[i_j]$. Then we have:

$$\sum_{j=1}^{r}\alpha_{i_j}G_k(v_{i_j})=0\implies\sum_{j=1}^{r}G_k(\alpha_{i_j}v_{i_j})=0\implies G_k(\alpha_{i_1}v_{i_1}+\ldots+\alpha_{i_r}v_{i_r})=0$$

We can see that $P\equiv\alpha_1v_{i_1}+\ldots+\alpha_{i_r}v_{i_r}$ is a polynomial of degree at most k in $\mathbb{F}[x_1,\dots,x_n]$, such that $G_k(P)\equiv 0$, whereas $P\not\equiv 0$ since $\exists\alpha_{i_j}\neq 0$. This contradicts Lemma 1. Hence, the Claim is proved.

Consider a partition $\varphi:X\to A\cup B$ and suppose $\mathsf{rank}(M_{f^\varphi})\ge r$. Let $m_1,\dots,m_r$ be r linearly independent rows of M_f (chosen arbitrarily). Let $p_1,\dots,p_r$ be the polynomials representing these rows, i.e., $p_i=\sum_{S\subseteq B}M_f[m_i,m_S]m_S$. Then $p_1,\dots,p_r$ are linearly independent, i.e., $\forall\alpha_1\dots\alpha_r\in\mathbb{F},\sum_{i=1}^{r}\alpha_ip_i=0\implies\forall i,\alpha_i=0$. Let $q_i=G_k(p_i),1\le i\le r$ then clearly, $\sum_{i=1}^{r}\alpha_iq_i=0\implies\forall i,\alpha_i=0$. This however, is not sufficient, since the partition φ does not imply a partition on $Y\cup Z$. To overcome this difficulty we consider the generator G_{2k} rather than G_k. Note that for any degree k polynomial f, $G_{2k}(f)\equiv 0\iff G_k(f)\equiv 0$. Suppose $G_{2k}:\mathbb{F}[x_1,\dots,x_n]\to\mathbb{F}[Y'\cup Z']$ where $Y'=\{y_1,\dots,y_{2k}\}$ and $Z'=\{z_!,\dots,z_{2k}\}$. Consider arbitrary partitions:$Y'=Y_1\cup Y_2,\ |Y_1|=|Y_2|=k$, and $Z'=Z_1\cup Z_2,\ |Z_1|=|Z_2|=k$. Define the map $\widehat{G_{2k}}=(\widehat{G_{2k}^{(1)}},\dots,\widehat{G_{2k}^{(n)}})$, where

$$\widehat{G_{2k}^{(i)}}=\widehat{G_{2k}}(x_i)=\begin{cases}G_{2k}^{(i)}|_{\{w=0|w\in Y_2\cup Z_2\}} & \text{if } i\in A\\ G_{2k}^{(i)}|_{\{w=0|w\in Y_1\cup Z_1\}} & \text{if } i\in B\end{cases}$$

Note that the polynomial $G_{2k}^{(i)}|_{\{x=0|x\in Y_2\cup Z_2\}}$ is indeed a copy of G_k^i for every i, is defined over $Y_1\cup Z_1$ for $i\in A$, and over $Y_2\cup Z_2$ for $i\in B$. Now, the partition φ naturally induces

a partition φ' of $Y' \cup Z'$. Let $q'_i = \widehat{G_{2k}}(p_i)$, then from the above observations, we have that the polynomials $q'_1, \ldots, q'_i$ are linearly independent. Since these polynomials correspond to rows in the matrix $M_{g^{\varphi'}}$, we have $\mathsf{rank}(M_{g^{\varphi'}}) \geq r$. Now, to prove the required probability bound, note that the choice of the partitions $Y' = Y_1 \cup Y_2$ and $Z' = Z_1 \cup Z_2$ was arbitrary, and the rank bound holds for every such partition. There are $\binom{2k}{k}^2$ such partitions. Thus $\mathbf{Pr}[\mathsf{rank}(M_{g^{\varphi'}}) \geq r] \geq \binom{2k}{k}^2 / \binom{4k}{2k} = \Omega(1/k^2)$.

Note that, in the above the rank preservation is argued against G_{2k} rather than G_k. Though, we do not know if Theorem 6 holds true when G_{2k} is replaced by G_k, we conclude with the observation that, polynomials with high partial derivative dimension will have high rank coefficient matrix for some partition φ.

6 Conclusions and Future Directions

We studied complexity of polynomials parameterized by degree and continued the study of parameterized complexity of the arithmetic circuit identity testing problem initiated in [Mül08] and [CR15]. Our results indicate possibility of obtaining more special classes of ACIT that are fixed parameter tractable. We conclude with the following open questions:

- Extend the parameterized separation of depth three and four circuits to higher depths, perhaps with the restriction of multi-linearity etc,.
- Improve Theorem 6 to the generator G_k rather than G_{2k}.
- Obtain a black-box version of Theorem 5.
- Obtain a parameterized version of the depth reduction by Agrawal and Vinay [AV08].

References

[AFS12] Omid Amini, Fedor V. Fomin, and Saket Saurabh. Counting subgraphs via homomorphisms. *SIAM J. Discrete Math.*, 26(2):695–717, 2012.

[AKKT16] Vikraman Arvind, Johannes Köbler, Sebastian Kuhnert, and Jacobo Torán. Solving linear equations parameterized by hamming weight. *Algorithmica*, 75(2):322–338, 2016.

[AV08] Manindra Agrawal and V. Vinay. Arithmetic circuits: A chasm at depth four. In *FOCS*, pages 67–75, 2008.

[BHT12] Andreas Björklund, Thore Husfeldt, and Nina Taslaman. Shortest cycle through specified elements. In *SODA*, pages 1747–1753, 2012.

[Bjö10] Andreas Björklund. Exact Covers via Determinants. In *STACS*, pages 95–106, 2010.

[Bür13] Peter Bürgisser. *Completeness and reduction in algebraic complexity theory*, volume 7. Springer Science & Business Media, 2013.

[CFLS13] Zhixiang Chen, Bin Fu, Yang Liu, and Robert T. Schweller. On testing monomials in multivariate polynomials. *Theor. Comput. Sci.*, 497:39–54, 2013.

[CR15] Ankit Chauhan and B. V. Raghavendra Rao. Parameterized analogues of probabilistic computation. In *CALDAM*, pages 181–192, 2015.

[DF13] Rodney G. Downey and Michael R. Fellows. *Fundamentals of Parameterized Complexity*. Texts in Computer Science. Springer, 2013.

[Eng16] Christian Engels. *Why are certain polynomials hard?: A look at non-commutative, parameterized and homomorphism polynomials*. PhD thesis, Saarland University, 2016.

[Fis94] Ismor Fischer. Sums of like powers of multivariate linear forms. *Mathematics Magazine*, 67(1):59–61, 1994.

[FLPS16] Fedor V. Fomin, Daniel Lokshtanov, Fahad Panolan, and Saket Saurabh. Efficient computation of representative families with applications in parameterized and exact algorithms. *J. ACM*, 63(4):29:1–29:60, 2016.

[FLR+12] Fedor V. Fomin, Daniel Lokshtanov, Venkatesh Raman, Saket Saurabh, and B. V. Raghavendra Rao. Faster algorithms for finding and counting subgraphs. *J. Comput. Syst. Sci.*, 78(3):698–706, 2012.

[GKKS13] Ankit Gupta, Pritish Kamath, Neeraj Kayal, and Ramprasad Saptharishi. Arithmetic circuits: A chasm at depth three. In *FOCS 2013*, pages 578–587. IEEE, 2013.

[KMS13] Mrinal Kumar, Gaurav Maheshwari, and Jayalal Sarma. Arithmetic circuit lower bounds via maxrank. In *ICALP*, pages 661–672. Springer, 2013.

[KSS14] Neeraj Kayal, Chandan Saha, and Ramprasad Saptharishi. A super-polynomial lower bound for regular arithmetic formulas. In *STOC*, pages 146–153. ACM, 2014.

[Mül08] Moritz Müller. *Parameterized Randomization*. PhD thesis, Albert-Ludwigs-Universität Freiburg im Breisgau, 2008.

[Nis91] Noam Nisan. Lower bounds for non-commutative computation. In *STOC*, pages 410–418. ACM, 1991.

[NW96] Noam Nisan and Avi Wigderson. Lower bounds on arithmetic circuits via partial derivatives. *Computational Complexity*, 6(3):217–234, 1996.

[Raz09] Ran Raz. Multi-linear formulas for permanent and determinant are of super-polynomial size. *J. ACM*, 56(2), 2009.

[RS05] Ran Raz and Amir Shpilka. Deterministic polynomial identity testing in non-commutative models. *Computational Complexity*, 14(1):1–19, 2005.

[Sax08] Nitin Saxena. Diagonal circuit identity testing and lower bounds. In *ICALP*, pages 60–71. Springer, 2008.

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

[SV09] Amir Shpilka and Ilya Volkovich. Improved polynomial identity testing for read-once formulas. In *RANDOM*, pages 700–713. Springer, 2009.

[SY10] Amir Shpilka and Amir Yehudayoff. Arithmetic circuits: A survey of recent results and open questions. *FTTS*, 5(3–4):207–388, 2010.

[Tav15] Sébastien Tavenas. Improved bounds for reduction to depth 4 and depth 3. *Information and Computation*, 240:2–11, 2015.

[VSBR83] Leslie G. Valiant, Sven Skyum, S Berkowitz, and Charles Rackoff. Fast parallel computation of polynomials using few processors. *SIAM J. Comput.*, 12(4):641–644, 1983.

[Zip79] Richard Zippel. *Probabilistic algorithms for sparse polynomials*. Springer, 1979.