A note on parameterized polynomial identity testing using hitting set generators ☆

Purnata Ghosal and B.V. Raghavendra Rao[1]

Department of Computer Science and Engineering
IIT Madras, Chennai, INDIA

Abstract

We show that polynomial hitting set generator defined by Shpilka and Volkovich [1] has the following property:

If an n variate polynomial f has a partition of variables such that the partial derivative matrix [2] has large rank then its image under the Shpilka-Volkovich generator too has large rank of the partial derivative matrix even under a random partition.

Further, we observe that our main result is applicable to a larger class of hitting set generators that are defined by polynomials with small dual representation.

Keywords: Arithmetic Circuit Identity Testing, Parameterized Complexity.

1. Introduction

The arithmetic circuit identity testing problem (ACIT) is to test if the given polynomial represented by an arithmetic circuit is identically zero. The problem has received wide attention and there is a randomized polynomial time algorithm for ACIT due to Ore [3], DeMillo, Lipton [4], Schwartz [5] and Zippel [6]. A deterministic polynomial time (or even quasi-polynomial time) for the black-box version of ACIT implies arithmetic circuit lower bounds [7, 8]. Due to its primary importance in algebraic complexity theory, ACIT has received wide attention [9, 10]. Despite several approaches towards the problem, a deterministic polynomial time algorithm for ACIT remains elusive.

While the class P remains the primary notion of efficient computation there are several relaxed notions of efficiency that allow either approximate solutions or efficient solutions for controlled inputs. *Parameterized Complexity Theory*, introduced by Downey and Fellows [11], proposes a parameterized multi-dimensional view of efficiency. More precisely, every input of length n is associated with a parameter k. A problem is said to be *fixed parameter tractable* (FPT for short) if there is a deterministic algorithm that runs in time $f(k)n^{(O(1))}$, where f is an arbitrary computable function on the parameter k. Parameterized Complexity

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

Preprint submitted to Information Processing Letters *April 12, 2019*

Theory has lead to a lot of research in the area of algorithms and FPT is now widely accepted as a relevant notion of efficiency from a practical as well as theoretical perspective. In the parameterized world, the W hierarchy is the primary notion of intractability. (See [11] for a formal definition of the W hierarchy.)

Lack of progress in obtaining a deterministic polynomial time algorithm for ACIT is a natural reason to look into other notions of efficiency. In particular, it would be interesting to develop techniques that give efficient parameterized algorithms for ACIT. There are several candidates for parameters, viz., the number of variables, the degree of the polynomial, multiplication depth of the circuit given at the input etc. Müller [12] considered some of these parameters and studied the corresponding parameterized ACIT. He also designed the parameterized versions of the randomized algorithm by Schwartz and Zippel [5, 6] for the same. It may be noted that the algorithms proposed by Müller requires $f(k)n^{O(1)}$ many random bits, where n is the number of variables and f an arbitrary function of the parameter. To be able to compare the parameterized complexity of ACIT with problems in the the W hierarchy, the randomized algorithms for parameterized variants of ACIT should use random bits bounded by $f(k)\log n$, where $f(k)$ is a computable function of the parameter. (The corresponding complexity classes were defined by Müller [12] and extended in [13].) While such randomness efficient parameterized algorithms are not known for the parameters introduced by Müller [12], Chauhan and Rao [13] obtained what can be called bounded randomness version of Schwartz-Zippel [5, 6] with the degree of the polynomial as a parameter by giving a randomized algorithm that uses at most $f(k)\log n$ random bits.

The primary component in the algorithm by Chauhan and Rao [13] is a hitting set generator defined by Shpilka and Volkovich [1]. Recall that a hitting set generator for a class $\mathcal{C}$ of arithmetic circuits is a family $G = (G_n)_{n\geq 0}$ of polynomial maps such that for any polynomial $f \in \mathcal{C}$, $f \equiv 0$ if and only if $G(f) \equiv 0$. The main observation in [13] was that the hitting set generator defined in [14] (SV-generator) is indeed a hitting set generator for degree k polynomials. In fact the SV-generator has received wide attention in the literature. Anderson, van Melkebeek and Volkovich [15] obtained quasipolynomial time algorithm for ACIT on multilinear read-k formulas using the SV-generators as one of the ingredients. In [16] Minahan and Volkovich use the SV-generator for obtaining a complete black-box deterministic algorithm for reconstructions of read once polynomials.

The applications of SV-generator for obtaining deterministic algorithms for ACIT on special classes of circuits leads to the following question: Can the existing hitting set generators be used to obtain deterministic parameterized algorithms for ACIT for larger classes of circuits? More specifically, we ask: what are the classes of circuits where SV-generator can be used to obtain efficient deterministic parameterized algorithms for ACIT?

One possible approach to obtain a deterministic algorithm for ACIT on a class $\mathcal{C}$ of circuits is to obtain a hitting set generator G such that for every $f \in \mathcal{C}$, $G(f)$ is in a class of circuits where deterministic algorithms for ACIT are known (e.g., sparse polynomials, non-commutative formulas). We show that this approach for the SV-generator does not work when we consider $G(f)$ to be a small sum of product of univariate polynomials (Theorem 1 and Corollary 1), a class for which ACIT is known [18]. This is done by showing that for any polynomial f with large rank of the polynomial coefficient matrix (See Section 2 for a definition), the coefficient matrix for $G(f)$ has large rank with high probability. Our proof exploits the structure of the SV-generator and generalizes to generator families $\mathcal{F}$ such that it is possible to project $G \in \mathcal{F}$ to a smaller set of variables and obtain $G' \in \mathcal{F}$ (Corollary 1).

Our result indicates that the classes of circuits that contain polynomials whose polynomial coefficient matrices have full rank under every partition are perhaps the hardest instances for obtaining deterministic algorithms for ACIT.

2. Preliminaries

In this section we introduce necessary notions on arithmetic circuits and parameterized complexity. For more details the reader is referred to [17] and [11]. We represent the polynomial ring $\mathbb{F}[x_1, \ldots, x_n]$ by $\mathbb{F}[X]$.

We require the notion of *hitting set generators*. Consider a polynomial mapping $G : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{F}[y_1, \ldots, y_t]$ where G is defined by t variate polynomials $G_1, \ldots, G_n$ such that $G(x_i) = G_i$ for $1 \le i \le n$. Image of a polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$ under G is denoted by $G(f)$ and is given by $f(G_1, \ldots, G_n)$. G is said to be a hitting set generator for the circuit class $\mathcal{C}_n$ if for every polynomial $f \in \mathcal{C}_n,\ f \not\equiv 0$, it holds that $G(f) \not\equiv 0$.

Primary interest of this article is a hitting set generator defined by Shpilka and Volkovich [1]:

Definition 1 (SV-generator [1])**.** Let n be the number of variables and $a_1, a_2, \ldots, a_n$ be distinct elements in the field $\mathbb{F}$. Let $G^i_{n,k} \in \mathbb{F}[y_1, y_2 \ldots y_k, z_1, z_2 \ldots z_k]$ be the polynomial defined as follows:

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

$L_i(x)$ are Lagrangian Interpolation polynomials, and $L_i(a_j) = 1$ if $i = j$. The generator $G_{n,k}$ is defined as $G_{n,k} \triangleq (G^1_{n,k}, \ldots G^n_{n,k})$.

However, when n is clear from the context, we can denote $G_{n,k}$ by G_k. For a polynomial f, $G_k(f)$ is the image of f under G_k, i.e, $G_k(f) = f(G^1_k, \ldots, G^n_k)$. In [1], Shpilka and Volkovich showed that G_k is a hitting set generator for sum of k read-once polynomials. Further, in [13] 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. *[13] Let $f \in \mathbb{F}[X]$ with $deg(f) \le k$, then $f \equiv 0 \iff G_k(f) \equiv 0$, G_k is as in Definition 1.*

Coefficient Matrix of a polynomial

We consider the notion of partial derivative matrix of a polynomial defined by Nisan [19] and later used in [20]. Raz [2] used a variant of partial derivative matrix, which was later generalized by Kumar et al [21]. In this paper we consider yet another variant of partial derivative matrices, which we call as the *coefficient matrix* of a polynomial.

Definition 2. 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.

The coefficient matrix of a polynomial 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 fundamental properties of sub-additivity and sub-multiplicativity of the rank of the coefficient matrix follow directly from [2].

3. SV generator preserves rank

In this section, we show that images of a polynomial f under the SV generator have many partitions where the coefficient matrix has non-FPT rank provided f has one such partition. More generally, we show that the rank of the coefficient matrix of a polynomial acts as an invariant for the SV generator.

Theorem 1. *Let $f \in \mathbb{F}[x_1, \ldots, x_n]$ be a polynomial of degree $\leq k$. Let $g = G_{2k}(f)$. Then,*

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

where the probability is taken over the uniform distribution over the set of all partitions of the variables in g into two parts of equal size.

Approach. Suppose there is a partition φ of the variables in f such that $\mathsf{rank}(M_{f^\varphi}) \geq R$. In order to prove that rank is preserved under the map G_{2k}, we show that any R linearly independent rows of the M_{f^φ} remain linearly independent in the coefficient matrix of the image polynomial $g = G_{2k}(f)$. 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 $1/2^{2k}$ fractions of the partitions of variables of g, the coefficient matrix of g has large rank.

Proof. Fix $a_1, \ldots, a_n \in \mathbb{F}$ be distinct elements. Recall that the generator G_{2k} with respect to $a_1, \ldots, a_n$ is defined as $(G_{2k}^1, \ldots, G_{2k}^n)$, i.e, $G_{2k}(x_i) = G_{2k}^i \ \forall i \in \{1, \ldots, n\}$. Consider :

$$\begin{aligned}
G_{2k}(x_i) &= \sum_{p=1}^{2k} z_p L_i(y_p) \\
&= \sum_{p=1}^{2k} z_p \frac{\prod_{j \neq i}(y_p - a_j)}{\prod_{j \neq i}(a_i - a_j)} \\
&= \sum_{p=1}^{2k} z_p \frac{(y_p - a_1) \ldots (y_p - a_{i-1})(y_p - a_{i+1}) \ldots (y_p - a_n)}{(a_i - a_1) \ldots (a_i - a_{i-1})(a_i - a_{i+1}) \ldots (a_i - a_n)} \\
&= \sum_{p=1}^{2k} \sum_{q=1}^{n} b_p z_p y_p^{n-q} (-1)^q \mathsf{SYM}_{n-1,q-1} \quad \text{(by expanding the product, } b_p \text{ is a constant)} \\
&= \sum_{\substack{p \in [2k] \\ q \in [n]}} z_p y_p^{n-q} c_{pqi} \quad \text{(where } c_{pqi} = b_p(-1)^q \mathsf{SYM}_{n-1,q-1}(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)\text{)}.
\end{aligned}$$

Multiplying out any of the k terms obtained above, we get

$$G_{2k}(x_{i_1} x_{i_2} \ldots x_{i_k}) = \sum_{\substack{p_1, \ldots, p_k \in [2k] \\ q_1 \ldots q_k \in [n-1]}} z_{p_1} \ldots z_{p_k} y_{p_1}^{n-q_1} \ldots y_{p_k}^{n-q_k} \prod_{j=1}^{k} c_{p_j q_j i_j}$$

Let $\mathcal{M}_k$ be the set of all degree k monomials in the variables $\{x_1, \ldots, x_n\}$, 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 $I \subseteq \{1, \ldots, 2k\}$ of size k and $\mathsf{q} = (q_1, \ldots, q_k)$ with $1 \leq q_i \leq n-1$. Let $V = \text{Span}(\mathcal{M}_k)$, and $W = \text{Span}(\mathcal{S}_{nk})$ be the vector spaces spanned respectively by the sets $\mathcal{M}_k$ and $\mathcal{S}_{nk}$. 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 $\binom{4k}{k} n^k$. Note that G_{2k} is a linear map from V to W. Let C be the $\binom{n+k}{k} \times \binom{4k}{k} n^k$ matrix representing G_{2k} as a linear map from V to W. Then, $\forall v \in V, \ G_{2k}(v) = C^T v \in W$. Now, we argue that C has full row-rank.

Claim 1. *C has full row-rank.*

Proof of the Claim. Suppose C is not of full row rank. Then $\exists \ \alpha_{i_1}, \ldots, \alpha_{i_r} \in \mathbb{R}$, 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 $r \leq \mathsf{dim}(V)$. Hence, as G_{2k} is linear, we deduce that $\exists v_{i_1}, \ldots, v_{i_r} \in V$ such that $G_{2k}(v_{i_j}) = C[i_j]$. Then we have:

$$\sum_{j=1}^{r} \alpha_{i_j} G_{2k}(v_{i_j}) = 0 \implies \sum_{j=1}^{r} G_{2k}(\alpha_{i_j} v_{i_j}) = 0 \implies G_{2k}(\alpha_{i_1} v_{i_1} + \ldots + \alpha_{i_r} v_{i_r}) = 0$$

We can see that $P \equiv \alpha_1 v_{i_1} + \ldots + \alpha_{i_r} v_{i_r}$ is a polynomial of degree at most k in $\mathbb{F}[x_1, \ldots, x_n]$, such that $G_{2k}(P) \equiv 0$, 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 $\mathsf{rank}(M_{f^\varphi}) \geq R$. Let $m_1, \ldots, m_R$ be R linearly independent rows of M_f (chosen arbitrarily). Let $p_1, \ldots, p_R$ be the polynomials representing these rows, i.e., $p_i = \sum_{S \subseteq B} M_f[m_i, m_S] m_S$. Then $p_1, \ldots, p_R$ are linearly independent, i.e., $\forall \alpha_1 \ldots \alpha_R \in \mathbb{F}, \sum_{i=1}^{R} \alpha_i p_i = 0 \implies \forall i, \alpha_i = 0$. Let $q_i = G_{2k}(p_i), 1 \leq i \leq R$ then clearly, $\sum_{i=1}^{R} \alpha_i q_i = 0 \implies \forall i, \alpha_i = 0$. Suppose $G_{2k} : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{F}[Y \cup Z]$ where $Y = \{y_1, \ldots, y_{2k}\}$ and $Z = \{z_1, \ldots, z_{2k}\}$. Consider the arbitrary partition: $Y = Y_1 \cup Y_2,\ |Y_1| = |Y_2| = k$. Let $Z = Z_1 \cup Z_2,\ |Z_1| = |Z_2| = k$, where $Z_1 = \{z_i \mid y_i \in Y_1\}$ and $Z_2 = Z \setminus Z_1$. Define the map $\widehat{G_{2k}} = (\widehat{G_{2k}^{(1)}}, \ldots, \widehat{G_{2k}^{(n)}})$, where

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

Note that the polynomial $G_{2k}^{(i)}|_{\{x=0 \mid x \in Y_2 \cup Z_2\}}$ is indeed a copy of G_k^i for every i, and the same holds for $G_{2k}^{(i)}|_{\{x=0 \mid x \in Y_2\}}$. Hence, $\widehat{G_{2k}}$ 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 $q_i' = \widehat{G_{2k}}(p_i)$, $m_i' = \widehat{G_{2k}}(m_i)$. Note that $m_1', \ldots, m_R'$ are linearly independent. This follows from the fact that if $\sum_{i \in [R]} \alpha_i m_i' = 0$ and $\exists i \in [R], \alpha_i \neq 0$, then $\sum_{i \in [R]} \alpha_i \widehat{G_{2k}}(m_i) = \widehat{G_{2k}}(\sum_{i \in [R]} \alpha_i m_i) = 0$, since $\widehat{G_{2k}}$ is a linear map. But we know, $\sum_{i \in [R]} \alpha_i m_i \neq 0$ as $m_1, \ldots, m_R$ are distinct monomials. As $\widehat{G_{2k}}$ is a hitting-set generator, $\widehat{G_{2k}}(\sum_{i \in [R]} \alpha_i m_i) \neq 0$.

From the above observations, we have that the polynomials $q_1', \ldots, q_R'$ are linearly independent. Since each of the q_i's correspond to multiple rows (indexed by all possible monomials $Y_1 \cup Z_1$ occurring in q_i') 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 partition $Y' = Y_1 \cup Y_2$ was arbitrary, and the choice of the partition $Z' = Z_1 \cup Z_2$ follows from that, since $\forall y_j \in Y_1, z_j \in Z_1$. Hence, the rank bound holds for all the $\binom{2k}{k}$ such partitions of Y. Thus $\mathbf{Pr}[\mathsf{rank}(M_{g^{\varphi'}}) \geq R] \geq \binom{2k}{k} / \binom{4k}{2k} = \Omega(1/2^{2k})$. □

It may be noted that the for $R = n^{\Omega(k)}$ there are degree k polynomials computed by $\Pi\Sigma\Pi$ circuits where there is a partition φ such that Theorem 1 is applicable. Here is an example:

Example. The polynomial $p = \prod_{i=0}^{\frac{k}{2}} \left(x_{\frac{in}{2k}+1} x_{\frac{in}{2k}+2} + \ldots + x_{\frac{(i+1)n}{2k}-1} x_{\frac{(i+1)n}{2k}} \right)$ has rank $n^{k/2}/2k^{k/2}$ under the partition φ such that $\forall$ odd $i \in [n], \varphi(x_i) \in Y$, else $\varphi(x_i) \in Z$.

It is not clear if Theorem 1 can be generalized to arbitrary hitting set generators for polynomials parameterized by the degree. The main challenge here is to obtain a partition under which the image of the generator has rank R. The crucial property of the SV-generator that is used to obtain a partition is the fact that substituting a suitable subset of variables to zero results in a a copy of the generator with a fewer number of variables. In fact, it may noted that any family of generators whose suitably chosen projections give a generator from the same family. We call such generators *SV-like* generators.

Let $H = (H_{n,t})_{1 \leq t \leq n}$ be a family of generators, where $H_{n,t} : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{F}[y_1, \ldots, y_t]$. We say that $H_{n,t}$ is a *SV like* generator, if for $1 \leq t \leq n$, $H_{n,t}(x_i)$ there exists a subset $S \subseteq \{y_1, \ldots, y_t\}, |S| = t/2$ such that, $H_{(n,t)}\mid_{\{y=0|y\in S\}}$ and $H_{(n,t)}\mid_{\{y=0|y\notin S\}}$ are both copies of $H_{(n,t/2)}$.

Corollary 1. *Let $H = (H_{n,2t})_{1\le 2t\le n}$ be an SV like hitting set generator such that $H_{n,2t}$ is a hitting set generator for degree t polynomials on n variables. Let $f = f(x_1,\ldots,x_n)$ be any polynomial of degree $t/2$ and $h = H(f)$. Then,*

$$\exists\varphi, \mathsf{rank}(M_{f^{\varphi}}) \ge R \implies \exists\varphi'\mathsf{rank}(M_{h^{\varphi'}}) \ge R.$$

Proof. The argument is essentially the same as in Theorem 1. Let $k = t/2$, and let $\mathcal{M}_k$ be the set of all degree k monomials in the variables $\{x_1,\ldots,x_n\}$, and $\mathcal{S}_{n,k}$ be the set of all monomials that appear in at least one of the polynomials in the image set of $\mathcal{M}_k$ under the map $H_{n,2t}$. Note that $\mathcal{S}_{n,k}$ is a finite set. Let $V = \mathrm{Span}(\mathcal{M}_k)$, and $W = \mathrm{Span}(\mathcal{S}_{n,k})$ be the vector spaces spanned by the sets of monomials. The vector space V contains all polynomials in $\mathbb{F}$ of degree k. As in Claim 1, it can be concluded that H is a linear map from V to W that has full row-rank.

Consider a partition $\varphi : X \to A\cup B$ such that $\mathsf{rank}(M_{f^{\varphi}}) \ge R$. Let $m_1,\ldots,m_R$ be row indices of R linearly independent rows of M_f (chosen arbitrarily). Let $p_1,\ldots,p_R$ be the polynomials represented by these rows, i.e., $p_i = \sum_{S\subseteq B} M_f[m_i, m_S]m_S$. Then the polynomials $p_1,\ldots,p_R$ are linearly independent, i.e., $\forall\alpha_1\ldots\alpha_R\in\mathbb{F}, \sum_{i=1}^{R}\alpha_i p_i = 0 \implies \forall i, \alpha_i = 0$. Let $q_i = G_{2k}(p_i), 1\le i\le R$ then clearly, $\sum_{i=1}^{R}\alpha_i q_i = 0 \implies \forall i, \alpha_i = 0$. Consider the partition of $Y = \{y_1,\ldots,y_{2t}\}$ to $Y_1\cup Y_2$, where $Y_1 = S, Y_2 = \{y_1,\ldots,y_{2t}\}\setminus S$. We have $|Y_1| = |Y_2| = t$. Define the map $\widehat{H_{(n,2t)}} = (\widehat{H^{(1)}},\ldots,\widehat{H^{(n)}})$, where

$$\widehat{H^{(i)}} = \widehat{H}(x_i) = \begin{cases} H^{(i)}_{(n,2t)}|_{\{w=0|w\in Y_2\}} & \text{if } i\in A \\ H^{(i)}_{(n,2t)}|_{\{w=0|w\in Y_1\}} & \text{if } i\in B \end{cases}$$

Note that the polynomial $H^{(i)}_{(n,2t)}|_{\{x=0|x\in Y_2\}}$ is indeed a copy of $H^{i}_{(n,t)}$ for every i, and the same holds for $H^{(i)}_{(n,2t)}|_{\{x=0|x\in Y_1\}}$. Hence, $\widehat{H_{(n,2t)}}$ is defined over Y_1 for $i\in A$, and over Y_2 for $i\in B$. Thus, the partition φ naturally induces a partition φ' of Y.

Let $q'_i = \widehat{H_{(n,2t)}}(p_i)$, $m'_i = \widehat{H_{(n,2t)}}(m_i)$. Now we argue that $m'_1,\ldots,m'_R$ are linearly independent, since $m_1,\ldots,m_R$ are linearly independent. Suppose not, and let $\alpha_1,\ldots,\alpha_R\in\mathbb{F}$ be such that $\sum_{i=1}^{R}\alpha_i m'_i = 0$. Since $\widehat{H_{n,2t}}$ is a linear map from V to W, we have $\widehat{H_{(n,2t)}}(\sum_{i=1}^{R}\alpha_i m_i) = \sum_{i=1}^{R}\alpha_i\widehat{H_{(n,2t)}}(m_i) = \sum_{i=1}^{R}\alpha_i m'_i = 0$, a contradiction to the fact that $\widehat{H_{(n,2t)}}$ is a copy of $H_{n,t}$ and is a hitting set generator for degree k polynomials.

From the above observations, we have that the polynomials $q'_1,\ldots,q'_R$ are linearly independent. Since each of the q'_is correspond to multiple rows in the matrix $M_{h^{\varphi'}}$, we have $\mathsf{rank}(M_{h^{\varphi'}}) \ge R$. □

4. Conclusion

We have showed that the SV-generator with suitable parameters preserves the rank of partial derivative matrix of the polynomial with suitable partition of the variables. The main hurdle in generalizing our technique to arbitrary hitting set generators for degree k polynomials is the lack of structure of the generators under substitution of variables. It would be interesting to see if general hitting sets preserve the rank of partial derivative matrix, or rather any complexity measure.

Finally, it will be interesting to see if hitting set generators can reduce the complexity of a polynomial. More precisely, suppose $\mathcal{C}_1$ and $\mathcal{C}_2$ are algebraic complexity classes. Let G be a family of hitting set generators for $\mathcal{C}_1$. If $\mathcal{C}_2 \subset \mathcal{C}_1$, is it possible that $G(f) \in \mathcal{C}_2$ for every $f \in \mathcal{C}_1$?

Acknowledgments. We thank anonymous reviewers for a detailed feed back on an earlier version of the draft and for pointing out some impreciseness in the proofs and statements.

[1] A. Shpilka, I. Volkovich, Improved polynomial identity testing for read-once formulas, in: RANDOM, Springer, 2009, pp. 700–713.

[2] R. Raz, Multi-linear formulas for permanent and determinant are of super-polynomial size, J. ACM 56 (2) (2009) 8:1–8:17. `doi:10.1145/1502793.1502797`.

[3] Ø. Ore, über höhere kongruenzen, Norsk Mat. Forenings Skrifter 1 (7) (1922) 15.

[4] R. A. Demillo, R. J. Lipton, A probabilistic remark on algebraic program testing, Information Processing Letters 7 (4) (1978) 193 – 195. `doi:https://doi.org/10.1016/0020-0190(78)90067-4`.

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

[6] R. Zippel, Probabilistic algorithms for sparse polynomials, Springer, 1979.

[7] V. Kabanets, R. Impagliazzo, Derandomizing polynomial identity tests means proving circuit lower bounds, Computational Complexity 13 (1-2) (2004) 1–46. `doi:10.1007/s00037-004-0182-6`.

[8] M. Agrawal, V. Vinay, Arithmetic circuits: A chasm at depth four, in: FOCS, 2008, pp. 67–75.

[9] N. Saxena, Progress on polynomial identity testing, Bulletin of the EATCS 99 (2009) 49–79.

[10] N. Saxena, Progress on polynomial identity testing - II, Electronic Colloquium on Computational Complexity (ECCC) 20 (2013) 186.

[11] R. G. Downey, M. R. Fellows, Fundamentals of Parameterized Complexity, Texts in Computer Science, Springer, 2013.

[12] M. Müller, Parameterized randomization, Ph.D. thesis, Albert-Ludwigs-Universität Freiburg im Breisgau (2008).

[13] A. Chauhan, B. V. R. Rao, Parameterized analogues of probabilistic computation, in: CALDAM, 2015, pp. 181–192. doi:10.1007/978-3-319-14974-5_18.

[14] A. Shpilka, I. Volkovich, Read-once polynomial identity testing, in: STOC, 2008, pp. 507–516, see also ECCC TR-2010-011.

[15] M. Anderson, D. van Melkebeek, I. Volkovich, Deterministic polynomial identity tests for multilinear bounded-read formulae, Computational Complexity 24 (4) (2015) 695–776. doi:10.1007/s00037-015-0097-4.

[16] D. Minahan, I. Volkovich, Complete derandomization of identity testing and reconstruction of read-once formulas, TOCT 10 (3) (2018) 10:1–10:11.

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

[18] N. Saxena, Diagonal circuit identity testing and lower bounds, in: ICALP, Springer, 2008, pp. 60–71.

[19] N. Nisan, Lower bounds for non-commutative computation, in: STOC, ACM, 1991, pp. 410–418.

[20] N. Nisan, A. Wigderson, Lower bounds on arithmetic circuits via partial derivatives, Computational Complexity 6 (3) (1996) 217–234.

[21] M. Kumar, G. Maheshwari, J. Sarma, Arithmetic circuit lower bounds via maxrank, in: ICALP, Springer, 2013, pp. 661–672.