Electronic Colloquium on Computational Complexity, Report No. 153 (2016)

Lower Bounds for Projections of Power Symmetric Polynomials

Christian Engels[*] B. V. Raghavendra Rao[†] Karteek Sreenivasaiah[‡]

September 28, 2016

Abstract

The power symmetric polynomial on n variables of degree d is defined as $p_d(x_1, \ldots, x_n) = x_1^d + \cdots + x_n^d$. We study polynomials that are expressible as a sum of powers of homogenous linear projections of power symmetric polynomials. These form a subclass of polynomials computed by depth five circuits with summation and powering gates (i.e., $\sum \bigwedge \sum \bigwedge \sum$ circuits). We show $2^{\Omega(n)}$ size lower bounds for $x_1 \cdots x_n$ against the following models:

- Depth five $\sum \bigwedge \sum^{\leq n} \bigwedge^{\geq 21} \sum$ arithmetic circuits where the bottom $\sum$ gate is homogeneous;
- Depth four $\sum \bigwedge \sum^{\leq n} \bigwedge$ arithmetic circuits.

Together with the ideas in [Forbes, FOCS 2015] our lower bounds imply deterministic $n^{\mathsf{poly}(\log n)}$ black-box identity testing algorithms for the above classes of arithmetic circuits.

Our technique uses a measure that involves projecting the partial derivative space of the given polynomial to its multilinear subspace and then setting a subset of variables to 0.

1 Introduction

Arithmetic circuits were introduced by Valiant in [Val79] as a natural model for algebraic computation where he defined Algebraic Complexity classes based on various complexity measures of arithmetic circuits. In the same article, Valiant conjectured that the permanent polynomial, perm_n, does not have polynomial size arithmetic circuits. Following Valiant's work, there has been intensive efforts towards understanding the power and limitations of arithmetic circuits and other models of algebraic computation. Further, obtaining super polynomial size lower bounds for arithmetic circuits computing explicit polynomials has been a pivotal problem in Algebraic Complexity Theory. However, for general classes of

[*] Tokyo Institute of Technology, engels@is.titech.ac.jp, Supported by ELC project (KAKENHI No. 24106608)

[†] Indian Institute of Technology Madras, bvrr@cse.iitm.ac.in

[‡] Max-Planck-Institute for Informatics and Saarland University, karteek@mpi-inf.mpg.de, Supported by IMPECS post doctoral fellowship

ISSN 1433-8092

arithmetic circuits, the best known lower bound on the size is $\Omega(n \log d)$ for computing simultaneously a collection of n variate degree d polynomials [BS83].

Lack of progress on lower bounds against general arithmetic circuits lead researchers to focus on proving lower bounds against restricted classes of circuits. Grigoriev and Karpinski [GK98a] proved an exponential size lower bound for depth three circuits computing perm_n over finite fields which was further extended to functional fields by Grigoriev and Razborov [GK98b]. However, extending these results to infinite fields or depth four circuits remained elusive. Explaining the lack of progress, Agrawal and Vinay [AV08] (see also [Tav13, Koi12]) showed that proving exponential lower bounds against depth four arithmetic circuits is enough to resolve Valiant's conjecture. This was strengthened further to depth three circuits over infinite fields by Gupta et al. [GKKS13].

In a major attempt at breaking the barrier, Gupta et al. [GKKS14] obtained a $2^{\Omega(\sqrt{n})}$ size lower bound for depth four homogeneous circuits computing perm_n where the bottom fan-in is bounded by $O(\sqrt{n})$. This lower bound was achieved by a new complexity measure, the dimension of the shifted partial derivatives of the given polynomial. Using this complexity measure, Fournier et al. [FLMS14] obtained an exponential lower bound against depth four homogenous circuits computing the iterated matrix multiplication polynomial and hence implying that the techniques in [GKKS14] will not separate the class VP from VNP. Further, the ideas in [GKKS14, Kay12] have been generalized and applied to prove lower bounds against various classes of constant depth arithmetic circuits [KLSS14b, KLSS14a, KSS14, KS14, KS15a] for polynomials in VP as well as in VNP.

Despite several lower bound results against restricted class of arithmetic circuits, we have a limited set of complexity measures for arithmetic circuits. Nisan and Wigderson [NW95] were the first to use the space of partial derivatives to prove arithmetic circuit lower bounds. Later on, variants of partial derivative spaces and associated matrices were used to prove lower bounds to special classes of circuits such as multilinear formula (for e.g., [Raz04]) and depth three circuits (for e.g., [GK98a]). Kayal [Kay12] and Gupta et al. [GKKS14] introduced the notion of shifted partial derivatives, i.e., derivatives multiplied with monomials of certain degree. The dimension of the space of shifted partial derivatives and their projections were used extensively in subsequent work (see for e.g., [KS15a] and references therein). Chillara and Mukhopdhyay [CM14] obtained a combinatorial criteria based on the leading monomials of the space spanned by partial derivatives that would imply high dimension of the shifted partial derivatives.

More recently, the notion of evaluation dimension of polynomials was studied in [FS12] as a measure for arithmetic formulas. It is known that the rank of the partial derivative matrix of a polynomial, introduced in [Raz04] and extended in [KMS13], is equal to the evaluation dimension of the polynomial. However, the evaluation view of polynomials comes handier at times and is used extensively in proving lower bounds against read-once branching programs and restricted depth three circuits (see [Sap16] for details).

Since there are only a few techniques available for proving circuit lower bounds it is important to understand the strengths and limitations of existing approaches to improve our insight into Algebraic Complexity classes.

Our Model The power symmetric polynomial on n variables, of degree d is denoted by $p_d(x_1, \ldots, x_n)$ and given by

$$p_d(x_1, \ldots, x_n) = x_1^d + \ldots + x_n^d.$$

Power symmetric polynomials are a well studied class of polynomials. Kayal [Kay11] obtained a randomized polynomial time algorithm for testing affine equivalence to power symmetric polynomials. It can be seen that any polynomial can be written as a sum of homogeneous linear projections of power symmetric polynomials. Thus, *sum of homogeneous linear projections of power symmetric polynomials* can be viewed as a universal model of computation. This model is also referred to as diagonal depth three circuits or $\sum\bigwedge\sum$ circuits in the literature [Sap16]. Saxena [Sax08] obtained a non black-box deterministic polynomial time identity testing for sum of projections of power symmetric polynomials. Further, the arguments in [Kay12] imply that computing $x_1 \cdots x_n$ requires a sum of at least $\exp(\Omega(n))/n$ many projections of power symmetric polynomials. Combining this with the ideas in [For15a] gives a deterministic quasi-polynomial time black-box identity testing algorithm for polynomials that can be written as a sum of projections of power symmetric polynomials.

In this article, we study polynomials that build on power symmetric polynomials. In particular, we study polynomials that can be expressed as: (1) Sum of powers of power homogeneous symmetric polynomials and (2) Sum of powers of homogeneous projections of power symmetric polynomials. Models (1) and (2) correspond to $\sum\bigwedge\sum^{\leq n}\bigwedge$ circuits and $\sum\bigwedge\sum^{\leq n}\bigwedge\sum$ respectively.

Our Results We begin with the analysis of the dimension of the shifted partial derivative spaces for our models in Section 3. We show, in Theorem 3.4, that this measure is low for the restriction of polynomials computed as in model (1), thereby concluding in Theorem 1.1 that the size of such polynomials computing $x_1 \cdots x_n$ has to be exponential in n:

Theorem 1.1. *Let $g = \sum_{i=1}^{s} f_i^{\alpha_i}$ where $f_i = p_{d_i}(x_{i_1}, \ldots, x_{m_i}, \ell_{i_1}, \ldots, \ell_{i_{r_i}})$, $m_i \leq \frac{1}{10}n$, $r_i \leq n^{\epsilon}$, $\alpha_i \leq 2^{o(n)}$ for all i where $0 < \epsilon < 1$. If $g = x_1 x_2 \ldots x_n$, then $s = 2^{\Omega(n)}$.*

On the other hand, we observe, in Lemma 1.2, that there are polynomials computed by $\sum\bigwedge\sum\bigwedge$ circuits which have a shifted partial derivative space of large dimension:

Lemma 1.2. *For $k \leq n \leq d$, $l = \Theta(d)$ and large enough $\alpha > 0$, we have:*

$$\dim\left(\mathbb{F}\text{-Span}\left\{\boldsymbol{x}^{\leq l}\partial^{=k}\left(p_d(x_1, \ldots, x_n)^{\alpha}\right)\right\}\right) = \Omega\left(\frac{\binom{n}{k}\binom{n+l}{l}}{l^c}\right)$$

for some constant $c > 0$.

Lemma 1.2 essentially implies that measures such as the ones considered in [GKKS14, Kay12] cannot be used to derive lower bounds against the size of polynomials computed by $\sum\bigwedge\sum\bigwedge$.[1] This leads us to our main result of the paper. We consider the dimension of Projected Multilinear Derivatives in Section 4 as a possible measure to overcome the

[1] Saptharishi in [Sap16] had mentioned this, however our results make it more precise.

limitations of the method of shifted partial derivatives. Projected multilinear derivative of a polynomial f is computed by first projecting the partial derivative space of f to its multilinear subspace and then setting a subset of variables to 0. The dimension of the resulting space of polynomials is our measure of complexity for polynomials. We show the following in Section 4:

Theorem 1.3. *Let $g = \sum_{i=1}^{s} f_i^{\alpha_i}$ where $f_i = p_{d_i}(\ell_{i_1}, \ldots, \ell_{i_n}) + \beta_i$, where for every i, either $d_i = 1$ or $d_i \geq 21$, and $\ell_{i_1}, \ldots, \ell_{i_n}$ are homogeneous linear forms. If $g = x_1 \cdot x_2 \cdots x_n$, then $s = 2^{\Omega(n)}$.*

Our proof involves upper bounding the dimension of projected multilinear derivative spaces of powers of homogeneous projections of p_d, and lower bounding the same measure for the polynomial $x_1 \cdots x_n$.

It may be noted that the arguments in [Kay12] immediately implies exponential lower bound for the monomial $x_1 \cdots x_n$ against $\sum \bigwedge \sum \bigwedge^{\leq 21} \sum$ circuits. However, due to the limitations in choice of parameters used in [Kay12] and those in the proof of Theorem 1.3, the two results though seemingly complementary, do not imply lower bound against general $\sum \bigwedge \sum \bigwedge \sum$ circuits.

Finally, using the ideas developed in [For15a], we obtain black-box deterministic quasi-polynomial time identity testing algorithm for the above mentioned restrictions of $\sum \bigwedge \sum \bigwedge \sum$ circuits (Corollary 5.1).

Related work Bera and Chakrabarti [BC15] proved an exponential lower bound for iterated matrix multiplication against homogeneous depth five circuits with small bottom fan-in. Kumar and Saptharishi [KS15b] obtained lower bounds against depth five circuits over finite fields. Both of these results used the dimension of shifted partial derivatives as the complexity measure for polynomials. Our results, even though they are for a sub-class of depth five arithmetic circuits, are incomparable to those in [BC15, FKS16]. Further, Kayal, Nair and Saha [KNS16] have defined a complexity measure based on the notion of skewed partial derivatives. Though the skewed derivatives defined in [KNS16] are similar to our notion of projected multilinear derivatives, they differ in the fact that we consider multilinear derivatives with respect to all possible multilinear monomials, rather than skewed derivatives. Further, Saptharishi [Sap16, p. 187] notes that allowing higher power at the bottom $\bigwedge \sum$ layer of $\sum \bigwedge \sum \bigwedge \sum$ circuits gives a $2^{O(\sqrt{n})}$ size upper bound to compute the polynomial $x_1 \cdots x_n$. Our result (Theorem 1.3) shows that the upper bound of $2^{O(\sqrt{n})}$ on the size of a $\sum \bigwedge \sum \bigwedge \sum$ circuit computing $x_1 \cdots x_n$ does not hold when the fan-in of the middle Σ gate is bounded by n and linear forms at the bottom layer are homogeneous, even when the bottom layer is allowed to have large degrees.

2 Preliminaries

An *arithmetic circuit* is a labelled directed acyclic graph. Vertices of zero in-degree are called *input* gates and are labelled by elements in $\mathbb{F} \cup \{x_1, \ldots, x_n\}$. Vertices of in-degree two or more are called *internal* gates and have their labels from $\{\times, +\}$. An arithmetic circuit has at least one vertex of zero out-degree called an *output* gate. We assume that an arithmetic circuit has exactly one output gate. A polynomial p_g in $\mathbb{F}[x_1, \ldots, x_n]$ can be associated with every gate g of an arithmetic circuit defined in an inductive fashion. Input gates compute their label. Let g be an internal gate with children $f_1, \dots, f_m$, then $p_g = p_{f_1}\ \mathsf{op}\ \cdots \mathsf{op}\ p_{f_m}$ where $\mathsf{op} \in \{+, \times\}$ is the label of g. The polynomial computed by the circuit is the polynomial at one of the output gates and denoted by p_C. The size of an arithmetic circuit is the number of gates in it and is denoted by size(C). We will sometimes denote a fan-in/degree bound on a layer as a superscript to the corresponding gate e.g., $\sum\bigwedge^{\leq n}\sum\bigwedge$ denotes the class of families of polynomials computed by depth four circuits with powering and sum gates, where the top most layer of powering gates have exponent bounded by n. Similarly $\sum\bigwedge\sum^{\leq n}\bigwedge^{\geq 21}\sum$ denotes the class of families of polynomials computed by depth five circuits with powering and sum gates, where the middle layer of sum gates have fan-in bounded from above n and the bottom most powering gates have degree at least 21.

We call a set $S \subseteq \mathbb{K}^n$ a hitting set for a class of circuits $\mathcal{C}$ with n inputs if for all n and for all circuits $C \in \mathcal{C}$ the following condition holds: Whenever C computes a non-zero polynomial then there exists an assignment $a \in S$ such that $C(a) \neq 0$.

We will later use the following inequality to bound the binomial coefficient. If not specified otherwise we use the logarithm to base two.

Proposition 2.1 ([Mac03]). *Let $r \leq n$. Then*

$$\log_2 \binom{n}{r} \approx nH(r/n)$$

where H is the binary entropy function: $H(p) = -p\log_2(p) - (1-p)\log_2(1-p)$ and $\approx$ is equality upto an additive $o(n)$ error.

We denote by $[n] = \{1, \dots, n\}$.

For a set of polynomials S, let $\mathcal{M}_{\leq d}(S)$ ($\mathcal{M}_{=d}(S)$) denote the set of all products of at most (exactly) d elements from S. Note that when S is a set of variables, $|\mathcal{M}_{\leq d}(S)| = \binom{|S|+d}{d}$. When the set S is clear from the context, we use $\mathcal{M}_{\leq d}$ ($\mathcal{M}_{=d}$) instead of $\mathcal{M}_{\leq d}(S)$ ($\mathcal{M}_{=d}(S)$) for the sake of brevity.

For a subset S of variables, let $\mathcal{X}_a^b(S)$ denote the set of all multilinear monomials of degree $a \leq d \leq b$ in variables from the set S, i.e.,

$$\mathcal{X}_a^b(S) = \{\prod_{x_i \in S} x_i^{\delta_i} \mid a \leq \sum_{i=1}^{n} \delta_i \leq b, \delta_i \in \{0,1\}\}.$$

Let $A \odot B$ for two sets A, B be defined as $\{a \cdot b \mid a \in A, b \in B\}$. Additionally, we define $A \cdot f$ for some polynomial f to be the set $\{a \cdot f \mid a \in A\}$.

The notion of *shifted partial derivatives* is given as follows. For $f \in \mathbb{F}[x_1, \dots, x_n]$ let $\partial^{=k} f$ denote the set of all partial derivatives of f of order k.

For $l \geq 0$, the (k, l) shifted partial derivative space of f denoted by $\mathbb{F}\text{-Span}\left\{\boldsymbol{x}^{\leq l}\partial^{=k} f\right\}$ and is defined as

$$\mathbb{F}\text{-Span}\left\{\boldsymbol{x}^{\leq l}\partial^{=k} f\right\} \triangleq \mathbb{F}\text{-Span}\left\{\mathbf{m} \cdot \partial^{=k} f \;\mid\; \mathbf{m} \in \mathcal{M}_{\leq \ell}(x_1, \dots, x_n)\right\}$$

where

$$\mathbb{F}\text{-Span}\{S\} \triangleq \{\alpha_1 f_1 + \cdots + \alpha_m f_m \mid f_i \in S \text{ and } \alpha_i \in \mathbb{F} \text{ for all } i \in [m]\}.$$

We restate the well known lower bound for the dimension of the space of shifted partial derivatives $x_1 \cdots x_n$:

Proposition 2.2 ([Kay12])**.** $\dim \left(\mathbb{F}\text{-Span}\left\{\boldsymbol{x}^{\leq l}\partial^{=k} x_1 \cdots x_n\right\}\right) \geq \binom{n}{k} \cdot \binom{n-k+l}{l}$.

For $k \geq 1$, the kth order multilinear derivative space of f, denoted by $\partial^{=k}_{\mathsf{ML}} f$, is defined as:

$$\partial^{=k}_{\mathsf{ML}} f \triangleq \{\frac{\partial^k f}{\partial x_{i_1} \cdots \partial x_{i_k}} \mid i_1 < \ldots < i_k \in \{1, \ldots, n\}\}.$$

Note that $\partial^{=k}_{\mathsf{ML}} f \subseteq \partial^{=k} f$ with equality when f is a multilinear polynomial.

3 Dimension of Shifted Partial Derivatives

This section is devoted to the analysis of the dimension of the shifted partial derivative space of polynomials that are computed by restricted classes of $\sum \bigwedge \sum \bigwedge \sum$ circuits. We begin by showing that there are powers of power symmetric polynomials that have shifted partial derivative space within a polynomial factor of the shifted partial derivative space of $x_1 x_2 \cdots x_n$ as given in Proposition 2.2.

Proof of Lemma 1.2

We re-state Lemma 1.2 for readability:

Lemma 1.2. *For $k \leq n \leq d$, $l = \Theta(d)$ and large enough $\alpha > 0$, we have:*

$$\dim \left(\mathbb{F}\text{-Span}\left\{\boldsymbol{x}^{\leq l}\partial^{=k}\left(p_d(x_1, \ldots, x_n)^\alpha\right)\right\}\right) = \Omega\left(\frac{\binom{n}{k}\binom{n+l}{l}}{l^c}\right).$$

for some constant $c > 0$.

Remark. Note that the lower bound above is not interesting for small values d, and hence the bound $d \geq n$ is necessary, though, this may not be tight. More precisely, if $d = O(1)$, it follows from [Kay12] that

$$]\dim \left(\mathbb{F}\text{-Span}\left\{\boldsymbol{x}^{\leq l}\partial^{=k}\left((x_1^d + \cdots + x_n^d)^\alpha\right)\right\}\right)$$

is upper bounded by $\binom{n+dk-k+l}{dk-k+l}$ for any k. In this case however, our lower bound in Lemma 1.2 is exponentially smaller than $\binom{n+dk-k+l}{dk-k+l}$ since $l = \Theta(d)$.

Proof. Let $f = x_1^d + \cdots + x_n^d$. Then $\forall S \subseteq \{1, \ldots, n\}$ with $|S| = k$, we have: $\frac{\partial^k f^\alpha}{\partial S} = f^{\alpha-k} \cdot \prod_{i \in S} x_i^{d-1}$. Recall that

$$\begin{aligned}
\mathbb{F}\text{-Span}\left\{\boldsymbol{x}^{\leq l}\partial^{=k} f\right\} &= \mathbb{F}\text{-Span}\left\{\mathbf{m} \cdot \partial^{=k} f \mid \mathbf{m} \in \mathcal{M}_{\leq l}(x_1, \ldots, x_n)\right\} \\
&\supseteq \mathbb{F}\text{-Span}\left\{\mathbf{m} \cdot \partial^{=k}_{\mathsf{ML}} f \mid \mathbf{m} \in \mathcal{M}_{\leq l}(x_1, \ldots, x_n)\right\} \\
&= \mathbb{F}\text{-Span}\left\{\mathbf{m} \cdot f^{\alpha-k} \cdot \prod_{i \in S} x_i^{d-1} \;\middle|\; \begin{array}{c} \mathbf{m} \in \mathcal{M}_{\leq l}(x_1, \ldots, x_n), \\ S \subset \{1, \ldots, n\} \text{ with } |S| = k \end{array}\right\}.
\end{aligned}$$

Thus $\dim\left(\mathbb{F}\text{-Span}\left\{\boldsymbol{x}^{\leq l}\partial^{=k}\left(f^{\alpha}\right)\right\}\right)$ is lower bounded by the number of monomials in the set

$$\Gamma_{k,l,d} \triangleq \{\prod_{i\in S} x_i^{d-1} \mid S \subseteq \{1,\ldots,n\}, |S| = k\} \odot \mathcal{M}_{\leq l}(\{x_1,\ldots,x_n\})\}.$$

We now lower bound $|\Gamma_{k,l,d}|$. Let $\mathcal{N}_{k,d} = \{\prod_{i\in S} x_i^{d-1} \mid |S| = k\}$.

Consider the map $\varphi : \mathcal{N}_{k,d} \times \mathcal{M}_{\leq l} \to \Gamma_{k,l,d}$ where $(m_1, m_2) \mapsto m_1 \cdot m_2$. Note that if $d-1 \geq l$ and $d \geq n$, the map φ is injective and hence $|\Gamma_{k,l,d}| \geq |\mathcal{N}_{k,d}||\mathcal{M}_{\leq l}| = \binom{n}{k} \cdot \binom{n+l}{l}$. We now argue that if $l \in \Theta(d)$, any element in $\Gamma_{k,l,d}$ has at most $l^{O(1)}$ many pre-images under φ, which completes the proof.

Let $\gamma = x_{i_1}^{d-1} \cdots x_{i_k}^{d-1} \cdot m \in \Gamma_{k,l,d}$ where $i_1 < i_2 < \cdots < i_k$ and $m \in \mathcal{M}_{\leq l}$. To bound the number of pre-images of γ, let $\varphi(x_{j_1} \cdots x_{j_k}, m') = \gamma$. Since degree of m' is l, by comparing the degrees, it must hold that $|\{i_1, \ldots i_k\} \triangle \{j_1, \ldots, j_k\}| \leq l/(d-1)$. Therefore $|\varphi^{-1}(x_{i_1}^{d-1} \cdots x_{i_k}^{d-1} \cdot m)| \leq \binom{l}{l/(d-1)} \leq l^{O(1)}$, this completes the proof. □

Recall that by Proposition 2.2

$$\binom{n}{k}\binom{n-k+l}{l} \leq \dim\left(\mathbb{F}\text{-Span}\left\{\boldsymbol{x}^{\leq l}\partial^{=k} x_1 \cdots x_n\right\}\right) \leq \binom{n}{k}\binom{n+l}{l}.$$

Thus, Lemma 1.2 implies that the shifted partial derivative measure and Proposition 2.2 cannot be used in proving lower bounds for the monomial $x_1 \cdots x_n$ against general $\Sigma \wedge \Sigma \wedge \Sigma$ circuits. Nevertheless, it is worthwhile to look for subclasses of power symmetric polynomials of high degree where the dimension of the shifted partial derivative space is small. The *arity* of a polynomial f is the number of variables f depends on. It was shown in [KS16] that certain projections of the shifted partial derivatives of any product of sub-linear arity polynomials is low. We consider homogeneous projections of power symmetric where we allow arity to be bounded by $n/10$.

Proof of Theorem 1.1

We can now build the ingredients for the proof of Theorem 1.1. We begin with a simple upper bound on the dimension of the derivatives of powers of projections of p_d onto low-dimensional sub-spaces:

Lemma 3.1. *Let* $f = p_d(\ell_1, \ldots, \ell_t)$ *and* $d \geq k$. *Then* $\dim\left(\mathbb{F}\text{-Span}\left\{\partial^{\leq k} f^{\alpha}\right\}\right) \leq (k+1)(dk)^r$ *where* $r = \dim(\mathbb{F}\text{-Span}\{\ell_1, \ldots, \ell_t\})$.

Proof. Without loss of generality, assume that $\ell_1, \ldots, \ell_r$ is a basis for $\mathbb{F}\text{-Span}\{\ell_1, \ldots, \ell_t\}$, $r \leq t$. Observe that

$$\partial^{\leq k} f^{\alpha} \subseteq \mathbb{F}\text{-Span}\left\{f^{\alpha-i} \cdot \ell_1^{\beta_1} \cdots \ell_r^{\beta_r} \mid \sum_{j=1}^{r} \beta_j \leq dk\right\}_{i\in\{1,\ldots,k\}}$$

and therefore, $\dim\left(\mathbb{F}\text{-Span}\left\{\partial^{\leq k} f^{\alpha}\right\}\right) \leq (k+1)(dk)^r$ as required. □

Now, we bound the dimension of shifted partial derivatives of powers of the power symmetric polynomial:

Lemma 3.2. *Let $f = p_d(x_{j_1}, \ldots, x_{j_m})$ for some $j_1, \ldots, j_m \in \{1, \ldots, n\}$. Then for any $\alpha, l, k \geq 1$*

$$\dim\left(\mathbb{F}\text{-Span}\left\{\boldsymbol{x}^{\leq l}\partial^{=k} f^\alpha\right\}\right) \leq (k+1)\binom{n+m+k+l}{k+l}.$$

Proof. Let $i_1 < i_2 < \ldots < i_k \in \{1, \ldots, n\}$. Note that

$$\frac{\partial^k f^\alpha}{\partial x_{i_1} \cdots \partial x_{i_k}} = \begin{cases} f^{\alpha-k} x_{i_1}^{d-1} \cdots x_{i_k}^{d-1} & \text{if } \{i_1 \ldots, i_k\} \subseteq \{j_1, \ldots, j_m\}, \\ 0 & \text{otherwise.} \end{cases}$$

Now, relabelling the powers $x_{j_1}^{d-1}, \ldots, x_{j_m}^{d-1}$ as new variables $y_1, \ldots, y_m$ and shifting the resulting polynomials by monomials of degree at most l we get:

$$\mathbb{F}\text{-Span}\left\{\boldsymbol{x}^{\leq l}\partial^{=k} f^\alpha\right\} \subseteq \mathbb{F}\text{-Span}\left\{\bigcup_{0 \leq i \leq k} f^{\alpha-i} \cdot S|_{y_1 = x_{j_1}^{d-1}, \ldots, y_m = x_{j_m}^{d-1}}\right\}$$

where $S = \mathcal{M}_{=k+l}(\{x_1, \ldots, x_n, y_1, \ldots, y_m\})$, the set of all monomials of degree at most $k+l$ in the variables $\{x_1, \ldots, x_n, y_1, \ldots, y_m\}$. Therefore,

$$\dim\left(\mathbb{F}\text{-Span}\left\{\boldsymbol{x}^{\leq l}\partial^{=k} f^\alpha\right\}\right) \leq (k+1) \cdot \binom{n+m+k+l}{k+l}. \qquad \square$$

Combining Lemmas 3.1 and 3.2 with the sum and product rules for partial derivatives, we get:

Lemma 3.3. *Let $d > k$, $\ell_1, \ldots \ell_t$ be linear forms in $\mathbb{F}[x_1, \ldots, x_n]$, $f = p_d(x_{j_1}, \ldots, x_{j_m}, \ell_1, \ldots, \ell_t)$ and $\dim(\mathbb{F}\text{-Span}\{\ell_1, \ldots, \ell_t\}) = r$. Then we have*

$$\dim\left(\mathbb{F}\text{-Span}\left\{\boldsymbol{x}^{\leq l}\partial^{=k} f^\alpha\right\}\right) \leq \alpha(k+1)^2(dk)^r k\binom{m+n+k+l}{k+l}.$$

Proof. We have $f^\alpha = \sum_{i=0}^{\alpha} \binom{\alpha}{i} p_d(x_{j_1}, \ldots, x_{j_m})^i p_d(\ell_1, \ldots, \ell_t)^{\alpha-i}$, then by sub-additivity,

$$\begin{aligned} &\dim\left(\mathbb{F}\text{-Span}\left\{\boldsymbol{x}^{\leq l}\partial^{=k} f^\alpha\right\}\right) \leq \sum_{i=0}^{\alpha} \dim\left(\mathbb{F}\text{-Span}\left\{\boldsymbol{x}^{\leq l}\partial^{=k}\left(p_d(x_{j_1}, \ldots, x_{j_m})^i p_d(\ell_1, \ldots, \ell_t)^{\alpha-i}\right)\right\}\right) \\ &\leq \sum_{i=0}^{\alpha}\sum_{j=0}^{k} \dim\left(\mathbb{F}\text{-Span}\left\{\boldsymbol{x}^{\leq l}\partial^{=j} p_d(x_{j_1}, \ldots, x_{j_m})^i\right\}\right) \dim\left(\partial^{\leq k-j}\mathbb{F}\text{-Span}\left\{p_d(\ell_1, \ldots, \ell_t)^{\alpha-i}\right\}\right) \\ &\leq \alpha(k+1)(dk)^r k^2\,(k+1)\binom{n+m+k+l}{k+l} \text{ by Lemma 3.1 and Lemma 3.2.} \end{aligned}$$

For the penultimate inequality, note that

$$\begin{aligned} &\mathbb{F}\text{-Span}\left\{\boldsymbol{x}^{\leq l}\partial^{=k} p_d(x_{j_1}, \ldots, x_{j_m})^i p_d(\ell_1, \ldots, \ell_t)^{\alpha-i}\right\} \\ &\subseteq \mathbb{F}\text{-Span}\left\{\bigcup_{j=0}^{k} \boldsymbol{x}^{\leq l}\partial^{=j} p_d(x_1, \ldots, x_m)^i \odot \partial^{\leq k-j}(p_d(\ell_1, \ldots, \ell_t)^{\alpha-i})\right\}. \qquad \square \end{aligned}$$

Finally, using sub-additivity of shifted partial derivatives and Lemma 3.3 we get the following upper bound on the dimension.

Theorem 3.4. *Let $d > k$ and $g = \sum_{i=1}^{s} f_i^{\alpha_i}$ where $f_i = p_{d_i}(x_{i_1}, \ldots, x_{i_{m_i}}, \ell_{i_1}, \ldots, \ell_{i_{r_i}})$ and $\ell_{i_1}, \ldots, \ell_{i_{m_i}}$ are linear forms in $x_1, \ldots, x_n$. Then*

$$\dim\left(\mathbb{F}\text{-Span}\left\{\boldsymbol{x}^{\leq l}\partial^{=k} g\right\}\right) \leq s\alpha(k+1)^2(dk)^r \binom{n+m+k+l}{k+l}$$

where $m = \max_i m_i$ and $r = \max_i\{\dim(\mathbb{F}\text{-Span}\left\{\ell_{i_1}, \ldots, \ell_{i_{r_i}}\right\})\}$.

Combining the previous theorem with the lower bound from Proposition 2.2 as usual, gives us the size lower bound.

Theorem 1.1. *Let $g = \sum_{i=1}^{s} f_i^{\alpha_i}$ where $f_i = p_{d_i}(x_{i_1}, \ldots, x_{m_i}, \ell_{i_1}, \ldots, \ell_{i_{r_i}})$, $m_i \leq \frac{1}{10}n$, $r_i \leq n^\epsilon$ and $\alpha_i \leq 2^{n^\delta}$ for all i, for some $0 < \delta, \epsilon < 1$. If $g = x_1 x_2 \ldots x_n$, then $s = 2^{\Omega(n)}$.*

Proof. Let $m = \max_i m_i$. Using Proposition 2.2 and Theorem 3.4

$$s \geq \frac{\binom{n}{k}\binom{n-k+l}{l}}{\alpha(k+1)^2(dk)^r\binom{n+m+k+l}{k+l}}$$

where $\alpha = \max_i \alpha_i$. Taking the logarithm and using that $2\log(k+1) \leq 2\log dk$ when $d \geq 2$ gives us

$$\log s \geq \log\binom{n}{k} + \log\binom{n-k+l}{l} - \left(\log\alpha + \log\binom{n+m+k+l}{k+l} + (r+2)\log dk\right).$$

Note that $(r+2)\log dk = o(n)$. Now, using the approximation of binomial coefficients in Proposition 2.1 and setting $k = n/10$ and $l = 10n$ we get $\log s \geq 0.001n$. This proves the required bound as $d = 1$ is a degenerate case. □

4 Projected Multilinear Derivatives and Proof of Theorem 1.3

This section is devoted to the proof of Theorem 1.3. Our proof follows the standard two step approach for proving arithmetic circuit lower bounds: First, define a sub-additive measure that is low for every polynomial computed in the model. Second, show that the measure is exponentially larger for a specific polynomial p. Hence allowing us to conclude that any circuit in the model that computes p requires exponential size.

The dimension of the space of partial derivatives, space of shifted partial derivatives, their projection and the evaluation dimension are the most commonly used measure in the literature (see [Sap16] for a good exposition). We consider yet another variant of the space of partial derivatives, viz, *projected multilinear derivatives*. We begin with the definition of the measure.

The Complexity Measure

Let $f \in \mathbb{F}[x_1, \ldots, x_n]$. For $S \in \{1, \ldots, n\}$, let $\pi_S : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{F}[x_1, \ldots, x_n]$, be the projection map that sets all variables in S to zero, i.e., for every $f \in \mathbb{F}[x_1, \ldots, x_n]$ let $\pi_S(f) = f(x_i = 0 \mid i \in S)$. Let π_{m} denote the projection that projects a polynomial into its multilinear component, i.e., if $f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha \prod_{i=1}^n x_i^{\alpha_i}$, then $\pi_{\mathsf{m}}(f) = \sum_{\alpha \in \{0,1\}^n} c_\alpha \prod_{i=1}^n x_i^{\alpha_i}$.

Let $S \subseteq \{1, \ldots, n\}$ and $1 \leq k \leq n$. We define the complexity measure Projected Multilinear Derivatives (PMD) of a polynomial f of order k with respect to S as:

$$\mathrm{PMD}_S^k(f) \triangleq \dim(\mathbb{F}\text{-Span}\left\{\pi_S(\pi_{\mathsf{m}}(\partial_{\mathsf{ML}}^{=k} f))\right\}).$$

We omit the subscript S when either S is clear from the context, or when it refers to an unspecified set S.

Similar to other well established measures, PMD^k is sub-additive.

Lemma 4.1. *For any $S \subseteq \{1 \ldots, n\}$, $k \geq 1$, and polynomials f and g:*

$$\mathrm{PMD}_S^k(f + g) \leq \mathrm{PMD}_S^k(f) + \mathrm{PMD}_S^k(g).$$

Proof. Note that $\partial_{\mathsf{ML}}^{=k}(f + g) = \partial_{\mathsf{ML}}^{=k}(f) + \partial_{\mathsf{ML}}^{=k}(g)$, where for any two sets A and B, $A + B = \{a + b \mid a \in A, b \in B\}$. Therefore, $\mathbb{F}\text{-Span}\left\{\pi_S(\pi_{\mathsf{m}}(\partial_{\mathsf{ML}}^{=k}(f + g)))\right\} \subseteq \mathbb{F}\text{-Span}\left\{\pi_S(\pi_{\mathsf{m}}(\partial_{\mathsf{ML}}^{=k} f))\right\} \oplus \mathbb{F}\text{-Span}\left\{\pi_S(\pi_{\mathsf{m}}(\partial_{\mathsf{ML}}^{=k} g))\right\}$ where $\oplus$ denotes the direct sum of vector spaces. Hence $\mathrm{PMD}_S^k(f + g) \leq \mathrm{PMD}_S^k(f) + \mathrm{PMD}_S^k(g)$. □

Upper and Lower Bounds for the Measure

We obtain an upper bound on the dimension of projected multilinear derivatives of powers of power symmetric polynomials and their homogeneous projections. To begin with, we observe that in the case of powers of power symmetric polynomials the dimension of projected multilinear derivatives is either 0 or 1 for suitable values of k.

Lemma 4.2. *For any $\beta_0, \beta_1, \ldots, \beta_n \in \mathbb{F}, \alpha, d \in \mathbb{N}$ and for any $S \subseteq \{1, \ldots, n\}$ with $|S| + k > n$, we have $\mathrm{PMD}_S^k((\sum_{i=1}^n \beta_i x_i^d + \beta_0)^\alpha) \leq 1$.*

Proof. Let $f = \sum_{i=1}^n \beta_i x_i^d + \beta_0$. For any $T \subseteq \{x_1, \ldots, x_n\}$ with $|T| = k$, $\frac{\partial^k f^\alpha}{\partial T} = \left(\gamma \prod_{x_i \in T} \beta_i x_i^{d-1}\right) f^{\alpha - k}$ for some $\gamma \in \mathbb{F}$. Note that for any monomial M such that $\mathrm{support}(M) \cap S \neq \emptyset$, we have $\pi_S(M) = 0$. The condition $k + |S| > n$ implies that $T \cap S \neq \emptyset$ for any $T \subseteq \{x_1, \ldots, x_n\}$ with $|S| = k$. This means that S has at least one variable index in common with every monomial of the derivative $\frac{\partial^k f^\alpha}{\partial T}$ provided $d \geq 2$. Therefore $\mathrm{PMD}_S^k(f^\alpha) = 0$ when $d = 2$. For the case when $d = 1$, we have $\pi_S(\pi_{\mathsf{m}}(\partial_{\mathsf{ML}}^{=k}(f^\alpha))) \subseteq \mathbb{F}\text{-Span}\left\{f^{\alpha - k}\right\}$ and hence $\mathrm{PMD}_S^k(f^\alpha) = 1$. □

It might seem that the argument in Lemma 4.2 would immediately generalize to the case when the variables are replaced with homogeneous linear forms. However, the argument above fails even when the degree of the power symmetric polynomial is two (i.e., $d = 2$). Let $f = \ell_1^2 + \cdots + \ell_n^2 + \beta$ where $\ell_1, \ldots, \ell_n$ are homogeneous linear functions such that each of the ℓ_i depends on all of the variables and $\beta \neq 0$. It is not hard to see that the space of the kth order derivatives of f^α i.e., $\partial_{\mathsf{ML}}^k f$ is contained in the span of $\{f^{\alpha-k}\prod_{i=1}^{n}\ell_i^{\gamma_i} \mid \sum_i \gamma_i \le k\}$. Even after applying the projections π_{m} and π_S for any $S \subseteq \{1,\ldots,n\}$, with $|S| = (n/2)+1$, obtaining a bound on PMD^k better than the bound of $x_1\cdots x_n$ seems to be difficult. The reason is that every multilinear monomial of degree $|n/2-1-k|$ appears in at least one of the projected multilinear derivatives of d^α.

A natural approach to overcome the above difficulty could be to obtain a basis for the projected multilinear derivatives of f^α consisting of a small set of monomials and a small set of products of powers of the linear forms which are all multiplied by suitable powers of f, similar to the proof of Lemma 4.2. Surprisingly, as shown below in Lemma 4.3, the approach works when the degree $d \ge 21$, although it requires an involved combinatorial argument.

Lemma 4.3. *Let $f = (\ell_1^d + \ldots + \ell_n^d + \beta)$ for some scalar β, and let $Y = \{\ell_i^{d-j} \mid 1 \le i \le n, 1 \le j \le d\}$. Let $\lambda = 1/4+\varepsilon$ for some $0 < \varepsilon < 1/4$. Then, for $k = 3n/4$ and any $S \subseteq \{1,\ldots,n\}$ with $|S| = n/2+1$, we have:*

$$\pi_S(\pi_{\mathsf{m}}(\partial_{\mathsf{ML}}^{=k} f^\alpha) \subseteq \mathbb{F}\text{-Span}\left\{\pi_S(\pi_{\mathsf{m}}(\mathcal{F}\odot\left(\mathcal{X}_{\lambda n}^{n/2-1}(\overline{S})\cup\mathcal{M}_{\le(1+\varepsilon)n/d}(Y)\right)))\right\}$$

where $\mathcal{F} = \cup_{i=1}^{k} f^{\alpha-i}$ and $\overline{S} = \{1,\ldots,n\}\setminus S$.

Proof. Let $T \subseteq \{x_1,\ldots,x_n\}$ with $|T| = k$, let $f_T^{(k)}$ denote kth order partial derivative of f with respect to T. Note that

$$f_T^{(k)} \in \mathbb{F}\text{-Span}\left\{\ell_j^{d-k} \mid 1 \le j \le n\right\}.$$

Let L_i denote $\{\ell_j^{d-i} \mid 1 \le j \le n\}$ so that $f_T^{(k)} \in \mathbb{F}\text{-Span}\{L_k\}$. Then,

$$\frac{\partial^k f^\alpha}{\partial T} \in \mathbb{F}\text{-Span}\left\{f^{\alpha-i}\odot D_i^T(f) \mid 1 \le i \le k\right\} \qquad (1)$$

where $D_i^T(f) = \left\{\prod_{r=1}^{i} f_{T_r}^{(t_r)} \;\mid\; T_1\cup\ldots\cup T_i = T, \;\text{ where } t_r = |T_r| > 0, 1 \le r \le i\right\}$. Intuitively, the set D_i^T contains one polynomial for each possible partition of T into i many parts. The polynomial corresponding to a particular partition is the product of the derivatives of f with respect to each of the parts.

Now, the following claim bounds the span of D_i^T:

Claim 1. *For any $1 \le i \le k$: $D_i^T \subseteq \mathbb{F}\text{-Span}\left\{\bigodot_{r=1}^{k} L_r^{\odot j_r} \;\mid\; 1\cdot j_1+\cdots+k\cdot j_k = k\right\}$.*

Proof. Let $T_1,\ldots,T_i$ be a partition of T and let j_r denote the number of parts with cardinality r. Then

$$\prod_{|T_j|=r} f_{T_j}^{(r)} \in \mathbb{F}\text{-Span}\left\{\bigodot_{|T_j|=r} L_r\right\} = \mathbb{F}\text{-Span}\left\{L_r^{\odot j_r}\right\}.$$

Thus, $\prod_{r=1}^{i} f_{T_r}^{(t_r)} \in \mathbb{F}\text{-Span}\left\{\bigodot_{r=1}^{k} L_r^{\odot j_r}\right\}$. Since, $\sum_{r=1}^{k} r\cdot j_r = k$ for any partition $T_1\cup\ldots\cup T_i$ of T, the claim follows. □

Continuing from (1), we have:

$$\begin{aligned}\frac{\partial^k f^\alpha}{\partial T} &\in \mathbb{F}\text{-Span}\left\{f^{\alpha-i}\odot D_i^T(f) \mid 1\le i\le k\right\} \subseteq \mathbb{F}\text{-Span}\left\{\mathcal{F}\odot\{D_i^T(f) \mid 1\le i\le d\}\right\}\\ &\subseteq \mathbb{F}\text{-Span}\left\{\mathcal{F}\odot\left\{\bigodot_{r=1}^{d} L_r^{\odot j_r} \mid 1\cdot j_1+\cdots+d\cdot j_d=k\right\}\right\}. \qquad (2)\end{aligned}$$

To conclude the proof, it is enough to obtain a set of polynomials that span the right-hand side in (2) that satisfy the properties stated in the Lemma.

Claim 2.

$$\pi_S(\pi_{\mathsf{m}}\left(\left\{\bigodot_{r=1}^{d} L_r^{\odot j_r} \mid 1\cdot j_1+\cdots+d\cdot j_d=k\right\}\right) \subseteq \mathbb{F}\text{-Span}\left\{\mathcal{X}_{\lambda n}^{n/2-1}(\bar{S})\cup\mathcal{M}_{\le(1+\varepsilon)n/d}(Y)\right\}.$$

Proof. Note that the polynomials in L_j are homogeneous non-constant polynomials of degree $d-j$, and hence the set $\bigodot_{r=1}^{d} L_r^{\odot j_r}$ consists of homogeneous polynomials of degree: $\deg(\bigodot_{r=1}^{d} L_r^{\odot j_r}) = \sum_{r=1}^{d} j_r(d-r)$, where $\deg(\bigodot_{r=1}^{d} L_r^{\odot j_r})$ denotes the degree of polynomials in $\bigodot_{r=1}^{d} L_r^{\odot j_r}$. The remaining argument is split into three cases depending on the value of $\deg(\bigodot_{r=1}^{d} L_r^{\odot j_r})$:

Case 1: $\deg(\bigodot_{r=1}^{d} L_r^{\odot j_r}) > n/2$, then $\pi_S(\pi_{\mathsf{m}}(\bigodot_{r=1}^{d} L_r^{\odot j_r})) = \{0\}$.

Case 2: $\lambda n \le \deg(\bigodot_{r=1}^{d} L_r^{\odot j_r})) \le n/2$. In this case $\pi_S(\pi_{\mathsf{m}}(\bigodot_{r=1}^{d} L_r^{\odot j_r}))$ is trivially spanned by set of all multilinear monomials in the set of variables $\{x_j \mid j\notin S\}$ of degree at least λn and at most $n/2$. However, since $|S| = n/2-1$, we have $\pi_S(\pi_{\mathsf{m}}(\bigodot_{r=1}^{d} L_r^{\odot j_r})) \subseteq \mathbb{F}\text{-Span}\left\{\mathcal{X}_{\lambda n}^{n/2-1}(\bar{S})\right\}$.

Case 3: $\deg(\bigodot_{r=1}^{d} L_r^{\odot j_r})) < \lambda n$, i.e., $\sum_{r=1}^{d} j_r(d-r) \le \lambda n$. Recall that we have $\sum_{r=1}^{d} r\cdot j_r = k = 3n/4$. Thus

$$\begin{aligned}\sum_{r=1}^{d} j_r(d-r) &= \sum_{r=1}^{d} dj_r - \sum_{r=1}^{d} r\cdot j_r. \quad \text{Therefore}\\ \sum_{r=1}^{d} d\cdot j_r &\le \sum_{r=1}^{d} r\cdot j_r + \lambda n \quad \text{(By Assumption of Case 3)}\\ &= k+\lambda n = (\lambda+3/4)n = (1+\varepsilon)n.\end{aligned}$$

Therefore,

$$\sum_{r=1}^{d} j_r \le (1+\varepsilon)n/d.$$

Hence, in this case, $\pi_S(\pi_{\mathsf{m}}(\bigodot_{r=1}^{d} L_r^{\odot j_r}))$ is spanned by set of all product of at most $(1+\varepsilon)n/d$ polynomials of the form ℓ_i^{d-j}, i.e., $\pi_S(\pi_{\mathsf{m}}(\bigodot_{r=1}^{d} L_r^{\odot j_r})) \subseteq \mathbb{F}\text{-Span}\left\{\mathcal{M}_{\le(1+\varepsilon)n/d}(Y)\right\}$. □

Claim 2 completes the proof of Lemma 4.3. □

Using Lemma 4.3 above and choosing suitable parameters k and S we obtain the following upper bound on the dimension of projected multilinear derivatives of powers of homogeneous projections of power symmetric polynomials:

Theorem 4.4. *Let $f = (\ell_1^d + \ldots + \ell_n^d + \beta)$. For $d \geq 21$, and any $S \subseteq \{1, \ldots, n\}, |S| = n/2 + 1$*

$$\mathrm{PMD}_S^k(f^\alpha) \leq k \cdot n \cdot 2^{0.498n}.$$

Proof. By Lemma 4.3,

$$\pi_S(\pi_{\mathsf{m}}(\partial_{\mathsf{ML}}^{=k} f^\alpha)) \subset \mathbb{F}\text{-Span}\left\{\pi_S(\pi_{\mathsf{m}}(\{f^{\alpha-i}\}_{i=1}^k \odot \left\{\mathcal{X}_{\lambda n}^{n/2-1}(\bar{S}) \cup \mathcal{M}_{\leq(1+\epsilon)n/d}(Y)\right\}))\right\}$$

Recall that $\lambda = \frac{1}{4} + \varepsilon$. We choose $\varepsilon = 1/50$ and hence $\lambda = 0.27$. We have:

$$\mathrm{PMD}_S^k(f^\alpha) \leq k \cdot (|\mathcal{X}_{\lambda n}^{n/2-1}(\bar{S})| + |\mathcal{M}_{\leq(1+\epsilon)n/d}(Y)|).$$

Now, since $1/4 < \lambda < 1/2$, we have

$$\begin{aligned}|\mathcal{X}_{\lambda n}^{n/2-1}(\bar{S})| &\leq (n/2 - 1 - \lambda n) \cdot \binom{n/2-1}{\lambda n} \leq c(n/2) \cdot \binom{n/2}{\lambda n} \\ &\leq (cn/2) \cdot 2^{\frac{n}{2} \cdot \mathcal{H}(2\lambda)} \leq (n/2) \cdot 2^{0.498n}.\end{aligned}$$

Where c is an absolute constant. We bound $|\mathcal{M}_{\leq(1+\epsilon)n/d}(Y)|$ as follows:

$$\begin{aligned}|\mathcal{M}_{\leq(1+\epsilon)n/d}(Y)| = \binom{dn + (1+\varepsilon)n/d}{(1+\varepsilon)n/d} &\leq 2^{(dn+(1+\varepsilon)n/d)\mathcal{H}\left(\frac{(1+\varepsilon)n/d}{dn+(1+\varepsilon)n/d}\right)} \\ &= 2^{n(d+(1+\varepsilon)/d)\mathcal{H}\left((1+\varepsilon)/(d^2+(1+\epsilon))\right)} \leq 2^{0.4955n} \quad \text{for } d \geq 21.\end{aligned}$$

For the last inequality, note that for fixed n and ε, $(d + (1+\varepsilon))\mathcal{H}((1+\varepsilon)/(d^2 + (1+\epsilon))$ is a monotonically decreasing function of d, with $\lim_{d\to\infty}(d+(1+\varepsilon))\mathcal{H}((1+\varepsilon)/(d^2+(1+\epsilon)) = 0$. Therefore, the bound holds for $d \geq 21$.

This completes the proof. □

Now, it remains to establish a lower bound on the dimension of projected multilinear derivatives of the polynomial $x_1 \cdots x_n$. This follows from a relatively simple argument and is shown below:

Lemma 4.5. *For any $S \subseteq \{1, \ldots, n\}$ with $|S| = n/2 + 1$ and $k = 3n/4$ we have*

$$\mathrm{PMD}_S^k(x_1 \cdots x_n) \geq \binom{n/2-1}{n/4} \geq 2^{n/2}/n^2.$$

Proof. $\partial_{\mathsf{ML}}^{=k}(x_1 \cdots x_n) \subseteq \mathbb{F}\text{-Span}\left\{x_{i_1} \cdots x_{i_{n/4}} \mid i_1 < i_2 < \cdots < i_{n/4} \leq n.\right\}$. As for any k element subset $T \subseteq \{1, \ldots, n\}$ such that $\overline{T} \cap S = \emptyset$, $\pi_S(\pi_{\mathsf{m}}(\frac{\partial^k}{\partial T}(x_1 \cdots x_n))) = \prod_{i \notin T} x_i$. Thus, we have:

$$\pi_S(\pi_{\mathsf{m}}(\partial_{\mathsf{ML}}^{=k}(x_1 \cdots x_n))) = \mathbb{F}\text{-Span}\left\{\prod_{i \in T} x_i \ \mid \ T \subseteq \overline{S}, |T| \leq n/4\right\}$$

Therefore, $\mathrm{PMD}_S^k(x_1 \cdots x_n) \geq \binom{n/2-1}{n/4} \geq 2^{n/2}/n^2$. The last inequality follows from Stirling's approximation of binomial coefficients. □

Proof of Theorem 1.3

Theorem 1.3. *Let $g = \sum_{i=1}^{s} f_i^{\alpha_i}$ where $f_i = p_{d_i}(\ell_{i_1}, \ldots, \ell_{i_n}) + \beta_i$, where for every i, either $d_i = 1$ or $d_i \geq 21$, and $\ell_{i_1}, \ldots, \ell_{i_n}$ are homogeneous linear forms. If $g = x_1 \cdots x_n$, then $s = 2^{\Omega(n)}$.*

Proof. Let $S = \{1, \ldots, n/2+1\}$ and $k = 3n/4$. Then by Theorem 4.4 we have $\mathsf{PMD}_S^k(f_i) \leq 2^{0.498n}$. By the sub-additivity of PMD_S^k (Lemma 4.1), we have $\mathsf{PMD}_S^k(\sum_{i=1}^{s} f_i^{\alpha_i}) \leq s \cdot 2^{0.498n}$. Since $\mathsf{PMD}_S^k(x_1 \cdots x_n) \geq 2^{n/2}/n^2$, we conclude $s \geq 2^{0.01n}$, as required. □

5 Black Box Polynomial Identity Testing

Forbes [For15b] showed that lower bound for $x_1 \cdots x_n$ against any model using a measure that is invariant under projections using zero substitutions can be translated into quasi polynomial time deterministic black-box PIT algorithm. Using the ideas from [For15b], we obtain deterministic quasi polynomial time identity testing algorithm from the lower bounds obtained in Sections 3 and 4.

Let $\mathcal{C}_1$ be the class of all circuits of the form $g = \sum_{i=1}^{s} f_i^{\alpha_i}$ where we define $f_i = p_{d_i}(x_{i_1}, \ldots, x_{i_{m_i}}, \ell_{i_1}, \ldots, \ell_{i_{r_i}})$ and $m_i \leq \frac{1}{2}n$, $r_i \leq n^{\epsilon}$ and $s \in \mathsf{poly}(n)$. Let $\mathcal{C}_2$ be the class of all circuits of the form $g = \sum_{i=1}^{s} f_i^{\alpha_i}$ where $f_i = p_{d_i}(\ell_{i_1}, \ldots, \ell_{i_n}) + \beta_i$ and $d_i \geq 21$ and $\ell_{i_1}, \ldots, \ell_{i_n}$ are homogeneous linear forms.

Corollary 5.1. *There is a deterministic $n^{O(\log s)}$ time algorithm that given a multilinear polynomial $g \in \mathcal{C}_1 \cup \mathcal{C}_2$ with $\deg(g)$ tests if $g \equiv 0$.*

Proof (Sketch): The proof is a generalization of the arguments in Forbes [For15b] to projected multilinear derivatives. (See Proposition 4.18 in [For15b]). The argument when $g \in \mathcal{C}_1$ is exactly the same as in [For15b]. For the case when $g \in \mathcal{C}_2$, we argue that if $g \not\equiv 0$, then the trailing monomial in g will have at most $O(\log s)$ variables. Recall that trailing monomial of g, denoted by $\mathrm{TM}(g)$ is the smallest monomial with non-zero coefficient in g with respect to the lexicographic ordering induced by $x_1 > x_2 > \cdots > x_n$. Suppose S is the set of variables in $\mathrm{TM}(g)$. Since g is multilinear, we have $g|_{\overline{S} \to 0} = \prod_{i \in S} x_i$. Then, by Theorem 1.3 we have $s \geq 2^{\Omega(|S|)}$, and hence $|S| \leq c \log s$ for some constant $c > 0$. Now, testing if $g \equiv 0$ can be done by the following algorithm:

1. For all $S \subseteq \{1, \ldots, n\}$ with $|S| \leq c \log s$ do steps 2 & 3.
2. Let $g' \triangleq g(x_j = 0 \mid j \notin S)$.
3. For $a_S \in \{0,1\}^{|S|}$, if $g'(a_S) \neq 0$ then reject and halt.
4. Accept and halt.

Now, testing if $g \equiv 0$ can be done in time $n^{O(\log s)}$ by enumerating all $S \subseteq \{1, \ldots, n\}$, with $|S| \leq c \log s$, and testing if $g|_{\overline{S} \to 0} \equiv 0$. □

References

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

[BC15] Suman K. Bera and Amit Chakrabarti. A depth-five lower bound for iterated matrix multiplication. In *30th Conference on Computational Complexity, CCC 2015, June 17-19, 2015, Portland, Oregon, USA*, pages 183–197, 2015.

[BS83] Walter Baur and Volker Strassen. The complexity of partial derivatives. *Theor. Comput. Sci.*, 22:317–330, 1983.

[CM14] Suryajith Chillara and Partha Mukhopadhyay. Depth-4 lower bounds, determinantal complexity: A unified approach. In *31st International Symposium on Theoretical Aspects of Computer Science (STACS 2014), STACS 2014, March 5-8, 2014, Lyon, France*, pages 239–250, 2014.

[FKS16] Michael A. Forbes, Mrinal Kumar, and Ramprasad Saptharishi. Functional lower bounds for arithmetic circuits and connections to boolean circuit complexity. *Electronic Colloquium on Computational Complexity (ECCC)*, 23:45, 2016.

[FLMS14] Hervé Fournier, Nutan Limaye, Guillaume Malod, and Srikanth Srinivasan. Lower bounds for depth 4 formulas computing iterated matrix multiplication. In *STOC*, pages 128–135, 2014.

[For15a] Michael A. Forbes. Deterministic divisibility testing via shifted partial derivatives. 2015.

[For15b] Michael A. Forbes. Deterministic divisibility testing via shifted partial derivatives. In *FOCS*. IEEE Computer Society, 2015.

[FS12] Michael A. Forbes and Amir Shpilka. Quasipolynomial-time identity testing of non-commutative and read-once oblivious algebraic branching programs. *CoRR*, abs/1209.2408, 2012.

[GK98a] Dima Grigoriev and Marek Karpinski. An exponential lower bound for depth 3 arithmetic circuits. In *STOC*, pages 577–582, 1998.

[GK98b] Dima Grigoriev and Marek Karpinski. An exponential lower bound for depth 3 arithmetic circuits. In Jeffrey Scott Vitter, editor, *STOC*, pages 577–582. ACM, 1998.

[GKKS13] Ankit Gupta, Pritish Kamath, Neeraj Kayal, and Ramprasad Saptharishi. Arithmetic circuits: A chasm at depth three. In *54th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2013, 26-29 October, 2013, Berkeley, CA, USA*, pages 578–587, 2013.

[GKKS14] Ankit Gupta, Pritish Kamath, Neeraj Kayal, and Ramprasad Saptharishi. Approaching the chasm at depth four. *J. ACM*, 61(6):33:1–33:16, 2014.

[Kay11] Neeraj Kayal. Efficient algorithms for some special cases of the polynomial equivalence problem. In *SODA*, pages 1409–1421, 2011.

[Kay12] Neeraj Kayal. An exponential lower bound for the sum of powers of bounded degree polynomials. *Electronic Colloquium on Computational Complexity (ECCC)*, 19:81, 2012.

[KLSS14a] Neeraj Kayal, Nutan Limaye, Chandan Saha, and Srikanth Srinivasan. An exponential lower bound for homogeneous depth four arithmetic formulas. In *FOCS*, pages 61–70. IEEE Computer Society, 2014.

[KLSS14b] Neeraj Kayal, Nutan Limaye, Chandan Saha, and Srikanth Srinivasan. Super-polynomial lower bounds for depth-4 homogeneous arithmetic formulas. In David B. Shmoys, editor, *STOC*, pages 119–127. ACM, 2014.

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

[KNS16] Neeraj Kayal, Vineet Nair, and Chandan Saha. Separation between read-once oblivious algebraic branching programs (roabps) and multilinear depth three circuits. In *33rd Symposium on Theoretical Aspects of Computer Science, STACS 2016, February 17-20, 2016, Orléans, France*, pages 46:1–46:15, 2016.

[Koi12] Pascal Koiran. Arithmetic circuits: The chasm at depth four gets wider. *Theor. Comput. Sci.*, 448:56–65, 2012.

[KS14] Mrinal Kumar and Shubhangi Saraf. On the power of homogeneous depth 4 arithmetic circuits. In *FOCS*, pages 364–373, 2014.

[KS15a] Neeraj Kayal and Chandan Saha. Multi-k-ic depth three circuit lower bound. In *STACS*, pages 527–539, 2015.

[KS15b] Mrinal Kumar and Ramprasad Saptharishi. An exponential lower bound for homogeneous depth-5 circuits over finite fields. *CoRR*, abs/1507.00177, 2015.

[KS16] Mrinal Kumar and Shubhangi Saraf. Sums of products of polynomials in few variables: Lower bounds and polynomial identity testing. In *31st Conference on Computational Complexity, CCC 2016, May 29 to June 1, 2016, Tokyo, Japan*, pages 35:1–35:29, 2016.

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

[Mac03] David J. C. MacKay. *Information Theory, Inference and Learning Algorithms*. Cambridge University Press, 2003.

[NW95] Noam Nisan and Avi Wigderson. Lower bounds for arithmetic circuits via partial derivatives (preliminary version). In *FOCS*, pages 16–25, 1995.

[Raz04] Ran Raz. Multi-linear formulas for permanent and determinant are of super-polynomial size. In *STOC*, pages 633–641, 2004.

[Sap16] Ramprasad Saptharishi. A survey of lower bounds in arithmetic circuit complexity. Version 2.1.3, `https://github.com/dasarpmar/lowerbounds-survey/releases`, 2016.

[Sax08] Nitin Saxena. Diagonal circuit identity testing and lower bounds. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *ICALP*, volume 5125 of *Lecture Notes in Computer Science*, pages 60–71. Springer, 2008.

[Tav13] Sébastien Tavenas. Improved bounds for reduction to depth 4 and depth 3. In *MFCS*, pages 813–824, 2013.

[Val79] Leslie G. Valiant. Completeness classes in algebra. In *STOC*, pages 249–261, 1979.