Arithmetic Circuit Lower Bounds via Maximum-Rank of Partial Derivative Matrices*

Mrinal Kumar† Gaurav Maheshwari‡ Jayalal Sarma§

December 1, 2015

Abstract

We introduce the polynomial coefficient matrix and identify maximum rank of this matrix under variable substitution as a complexity measure for multivariate polynomials. We use our techniques to prove super-polynomial lower bounds against several classes of non-multilinear arithmetic circuits. In particular, we obtain the following results :

- As our first main result, we prove that any homogeneous depth-3 circuit for computing the product of d matrices of dimension $n \times n$ requires $\Omega(n^{d-1}/2^d)$ size. This improves the lower bounds in [NW95] for $d = \omega(1)$.
- As our second main result, we show that there is an explicit polynomial on n variables and degree at most $\frac{n}{2}$ for which any depth-3 circuit of product dimension at most $\frac{n}{10}$ (dimension of the space of affine forms feeding into each product gate) requires size $2^{\Omega(n)}$. This generalizes the lower bounds against diagonal circuits proved in [Sax08]. Diagonal circuits are of product dimension 1.
- We prove a $n^{\Omega(\log n)}$ lower bound on the size of product-sparse formulas. By definition, any multilinear formula is a product-sparse formula. Thus, this result extends the known super-polynomial lower bounds on the size of multilinear formulas [Raz06].
- We prove a $2^{\Omega(n)}$ lower bound on the size of partitioned arithmetic branching programs. This result extends the known exponential lower bound on the size of ordered arithmetic branching programs [Jan08].

*A preliminary version of this paper appeared in 40th International Colloquium on Automata, Languages and Programming (ICALP 2013).

†Department of Computer Science, Rutgers University. Email: mrinal.kumar@rutgers.edu. Part of this work was done while the author was at the Indian Institute of Technology Madras, Chennai, India.

‡Email: gaurav.m.iitm@gmail.com. The work was done while the author was with Indian Institute of Technology Madras, Chennai, India.

§Department of Computer Science & Engineering, Indian Institute of Technology Madras, Chennai, India. Email: jayalal@cse.iitm.ac.in

1 Introduction

Arithmetic circuits are a fundamental model of computation for polynomials. Establishing the limitations of polynomial sized arithmetic circuits is a central open question in the area of algebraic complexity (see [SY10] for a detailed survey). Unfortunately, very little is known in terms of lower bounds for general arithmetic circuits even after years of research. In the last two decades, this has led to a direction of research which aims to study restricted classes of arithmetic circuits with the hope that the tools and techniques developed in the process could possibly be adapted to make progress towards the problem of proving lower bounds for general circuits. Arithmetic Circuits of small depth(depth 3 and depth 4) and multilinear circuits are some of the most important classes studied in this regime.

In a surprising result Agrawal and Vinay [AV08] show that if a homogeneous polynomial in n variables of degree d (linear in n) can be computed by a homogeneous arithmetic circuits of size $2^{o(n)}$, then it can also be computed by homogeneous depth-4 circuits of size $2^{o(n)}$. The parameters of this result were further tightened by Koiran [Koi12] and Tavenas [Tav13]. Very recently, Gupta, Kamath, Kayal and Saptharishi [GKKS13b] proved a similar result for depth-3 circuits over fields of characteristic zero[1]. These results established a very direct connection between proving lower bounds for depth-3 and homogeneous depth-4 circuits and also somewhat explained the elusiveness of strong lower bounds for depth-3 and homogeneous depth-4 circuits.

For depth-3 circuits, the best known general result (over finite fields) is an exponential lower bound due to Grigoriev and Karpinski [GK98] and Grigoriev and Razborov [GR98]. Over fields of characteristic zero, obtaining such strong lower bounds is a long-standing open problem. The best known lower bound for depth three circuits over fields of characteristic zero are the quadratic lower bounds given by Shpilka and Wigderson [SW01].

For homogeneous depth-4 circuits, superpolynomial lower bounds were recently shown by Kumar and Saraf [KS13b], which were improved to exponential lower bounds by Kayal, Limaye, Saha and Srinivasan [KLSS14]. The main technical idea in both these results is to use an appropriate variant of the method of shifted partial derivatives introduced by Kayal [Kay12] and then used in multiple subsequent works on lower bounds for homogeneous depth four circuits [GKKS13a, FLMS13, KSS13, KS13a].

Another class of circuits which has been extensively studied is when the gates of the arithmetic circuits are restricted to compute multilinear polynomials. Super-polynomial lower bounds are known for the size of multilinear formulas computing the permanent or determinant polynomial [Raz09]. However, even under this restriction, proving super-polynomial lower bounds against arbitrary multilinear circuits is an open problem (see [SY10] and references there in). The parameter identified by [Raz06], which showed the limitations of multilinear formulas, was the rank of a matrix associated with the circuit - namely the partial derivatives matrix[2]. The method showed that there exists a partition of variables into two sets such that the rank of the partial derivatives matrix of any polynomial computed

[1] It is important to note that the depth-3 circuit constructed is highly non homogeneous

[2] An exponential sized matrix associated with the multilinear polynomial with respect to a partition of the variables into two sets. See Section 2 for the formal definition.

by the model is upper bounded by a function of the size of the circuit. But there are explicit polynomials for which the rank of the partial derivatives matrix is high. This program has been carried out for several classes of multilinear polynomials and several variants of multilinear circuits [DMPY12, Jan08, RY08, Raz06, Raz09, RSY08]. However, the partial derivatives matrix, in the form that was studied, was known to yield lower bounds only for multilinear circuits.

In this work, we generalize this framework to prove lower bounds against several classes of non-multilinear arithmetic circuits. This generalization also shows that the multilinearity restriction in the above proof strategy can possibly be eliminated from the circuit model side. Hence it can also be seen as an approach towards proving lower bounds against the general arithmetic circuits.

We introduce a variant of the partial derivatives matrix where the entries of the matrix are polynomials instead of constants - which we call the *polynomial coefficient matrix*. Instead of the rank of the partial derivatives matrix, we analyze the max-rank - the maximum rank of the polynomial coefficient matrix[3] under any substitution for the variables from the underlying field. We analyze how the max-rank changes under arithmetic operations. These tools are then combined to prove upper bounds on the max-rank of various restrictions of arithmetic circuits.

In [NW95], it was proved that any homogeneous depth-3 circuit for multiplying d $n \times n$ matrices (Iterated Matrix Multiplication, IMM_d^n) requires $\Omega\left(n^{d-1}/d!\right)$ size. We use our techniques to improve this result in terms of the lower bound. Our methods are completely different from [NW95] and this demonstrates the power of this method beyond the reach of the original partial derivatives matrix method due to Raz [Raz06]. As our first main result, we prove the following.

Theorem 1.1. *Any homogeneous depth-3 circuit for computing the product of d matrices of dimension $n \times n$ requires $\Omega(n^{d-1}/2^d)$ size.*

Notice that compared to the bounds in [NW95], our bounds are stronger when $d = \omega(1)$. Very recently, Gupta et al. [GKKS13a] studied the model of homogeneous circuits and proved a strong lower bound parameterized by the bottom fan-in. They studied depth-4 circuits ($\Sigma\Pi\Sigma\Pi$) and showed that if the fan-in of the bottom level product gate of the circuits is t, then any homogeneous depth-4 circuit computing the permanent (and the determinant) of $n \times n$ matrices must have size $2^{\Omega(\frac{n}{t})}$. In particular, this implies a $2^{\Omega(n)}$ lower bound for any depth-3 homogeneous circuit computing the permanent (and the determinant) of $n \times n$ matrices (n^2 variables). However, we remark that Theorem 1.1 is addressing the iterated matrix multiplication polynomial and hence is not directly subsumed by the above result. Moreover, the techniques used in [GKKS13a] are substantially different from ours.

We apply our method to depth-3 circuits where the space of the affine forms feeding into each product gate in the circuit is of limited dimension. Formally, a depth-3 $\Sigma\Pi\Sigma$ circuit

[3]When it is clear from the context, we drop the matrix as well as the partition. By the term, max-rank of a polynomial, we denote the maximum rank of the polynomial coefficient matrix corresponding to the polynomial with respect to the partition in the context.

C is said to be of product dimension r if for each product gate P in C, where $P = \Pi_{i=1}^{d} L_i$, where L_i is an affine form for each i, the dimension of the span of the set $\{L_i\}_{i\in[d]}$ is at most r. As our second main result, we prove exponential lower bounds on the size (in fact, the top fan in) of depth-3 circuits of bounded product dimension for computing an explicit polynomial.

Theorem 1.2. *There is an explicit polynomial on n variables and degree $\leq \frac{n}{2}$ for which any $\Sigma\Pi\Sigma$ circuit of product dimension at most $\frac{n}{10}$ requires size $2^{\Omega(n)}$.*

In [Sax08], the author studies diagonal circuits, which are depth-3 circuits where each product gate is an exponentiation gate. Clearly, such a product gate can be visualized as a product gate with the same affine form being fed into it multiple times. Thus, these circuits are of product dimension 1, and our lower bound result generalizes size lower bounds against diagonal circuits. Observe that $\Sigma\Pi\Sigma$ circuits of product dimension n are the usual unrestricted depth-3 circuits and hence, if we could improve the bound on the product dimension in Theorem 1.2 from $\frac{n}{10}$ to n, this would imply strong lower bounds for depth-3 circuits, which is a standing open problem.

Note that the product dimension of a depth-3 circuit is different from the dimension of the span of all affine forms computed at the bottom sum gates of a depth-3 circuit. It can be easily seen that, when this parameter, which we refer to as the total dimension of the circuit, is bounded, the model becomes non-universal.

For our next result, we generalize the model of syntactic multilinear formulas to product-sparse formulas. We formally define product-sparse formulas and full max-rank polynomials in Section 2. These formulas can compute non-multilinear polynomials as well. We prove the following lower bound on the size of product-sparse formulas using our methods.

Theorem 1.3. *Let X be a set of $2n$ variables, $\mathbb{F}$ be a field, and $f \in \mathbb{F}[X]$ be a full max-rank polynomial. Let Φ be any (s,d)-product-sparse formula of size $n^{\epsilon \log n}$, for a constant ϵ. If $sd = o(n^{1/8})$, then f cannot be computed by Φ.*

As our fourth result, we define partitioned arithmetic branching programs which are generalizations of ordered arithmetic branching programs. While ordered ABP can only compute multilinear polynomials, partitioned ABP is a non-multilinear model and thus, can compute non-multilinear polynomials too. We prove an exponential lower bound on the size of partitioned arithmetic branching programs extending results in [Jan08].

Theorem 1.4. *Let X be a set of $2n$ variables and $\mathbb{F}$ be a field. For any full max-rank homogeneous polynomial f of degree n over X and $\mathbb{F}$, the size of any partitioned arithmetic branching program computing f must be $2^{\Omega(n)}$.*

The rest of the paper is organized as follows. In section 2, we formally describe some of the preliminary definitions and notations and define the main parameter of our lower bounds - the polynomial coefficient matrix and prove the required properties with respect to arithmetic operations. Section 3 presents the lower bound result against depth-3 homogeneous circuits for computing iterated matrix multiplication. In section 4, we present an exponential lower

bound against $\Sigma\Pi\Sigma$ circuits of bounded product dimension. In section 5, we present a super-polynomial lower bound against product-sparse formulas. In section 6, we present an exponential lower bound against partitioned arithmetic branching programs.

2 Preliminaries

In this section, we define arithmetic circuits and the various restrictions of it that we study. For more detailed account of models and the results we refer the reader to the survey [SY10].

An arithmetic circuit Φ over the field $\mathbb{F}$ and the set of variables $X = \{x_1, x_2, \dots, x_n\}$ is a directed acyclic graph $G(V, E)$. The vertices of G with in-degree 0 are called *input* gates and are labelled by variables in X or constants from the field $\mathbb{F}$. The vertices of G with out-degree 0 are called *output* gates. Rest all vertices are referred to as internal vertices. Every internal vertex is either a plus gate or a product gate. We will study arithmetic circuits with a single output gate. Thus, the polynomial computed by the arithmetic circuit is the polynomial associated with the output gate. The size of Φ is defined to be the number of vertices in G.For a vertex $v \in V$, we denote the set of variables that occur in the subgraph rooted at v in G by X_v. An arithmetic circuit is called an *arithmetic formula* if the underlying undirected graph is acyclic i.e. fan-out of every vertex is at most one. A polynomial is said to be homogeneous if every monomial in it is of same degree. An arithmetic circuit is called *homogeneous* if every gate computes a homogeneous polynomial.

A $\Sigma\Pi\Sigma$ circuit is a levelled depth-3 circuit with a plus gate at the top, multiplication gates at the middle level and plus gates at the bottom level. The fan-in of the top plus gate is referred to as top fan-in. A $\Sigma\Pi\Sigma$ circuit is said to be *homogeneous* if the plus gate at the bottom level compute homogeneous linear forms only.

An important restricted model of arithmetic circuits is multilinear circuits. A polynomial $f \in \mathbb{F}[X]$ is called *multilinear* if the degree of every variable in f is at most one. An arithmetic circuit is called *multilinear* if the polynomial computed at every gate is multilinear. An arithmetic circuit is called *syntactic multilinear* if for every product gate v with children v_1 and v_2, $X_{v_1} \cap X_{v_2} = \phi$.

Let Φ be an arithmetic formula defined over the set of variables X and a field $\mathbb{F}$. For a product gate v in Φ with children v_1 and v_2, let us define the following properties:

Disjoint v is said to be *disjoint* if $X_{v_1} \cap X_{v_2} = \phi$.

Sparse v is said to be *s-sparse* if the number of monomials in the polynomial computed by at least one of its input gates is at most 2^s.

For any gate v, let us define the product-sparse depth of v to be equal to the maximum number of non-disjoint product gates in any path from a leaf to v.

Definition 2.1. *An arithmetic formula is said to be a (s, d)-product-sparse if every product gate v is either disjoint or s-sparse, where d is the product-sparse depth of the root node.*

Clearly, any syntactic multilinear formula is a $(s, 0)$-product-sparse formula for any s. Thus, proving lower bounds for product-sparse formulas will be a strengthening of known results.

An Arithmetic Branching Program (ABP) B is a levelled graph $G(V, E)$ in which V can be partitioned into levels $L_0, L_1, \ldots, L_d$ such that $L_0 = \{s\}$ and $L_d = \{t\}$ and the edges can only go between consecutive levels. The vertices s and t are called the *source* and *sink* respectively. The weight function w assigns affine forms to E. For a path p, the weight function can be extended by defining $w(p) = \prod_{e \in p} w(e)$. B computes the polynomial $\sum_p w(p)$ where p runs over all source-sink paths. B is said to be *homogeneous* if all edge labels are homogeneous linear forms and naturally computes a homogeneous polynomial. For any $i, j \in V$, $P_{i,j}$ denotes all paths from i to j in G, $X_{i,j}$ denotes the variables occuring in those paths and $f_{i,j}$ denotes the polynomial $\sum_{p \in P_{i,j}} w(p)$.

Definition 2.2. *Let B be a homogeneous arithmetic branching program defined over a field $\mathbb{F}$ and the set of variables $X = \{x_1, x_2, \ldots, x_{2n}\}$. B is said to be π-partitioned for a permutation $\pi : [2n] \to [2n]$ if there exists an $i = 2\alpha n$ for some constant α such that the following condition is satisfied, $\forall v \in L_i$:*

- *Either, $X_{s,v} \subseteq \{x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}\}$ and $|X_{v,t}| \leq 2n(1-\alpha)$.*
- *Or, $X_{v,t} \subseteq \{x_{\pi(n+1)}, x_{\pi(n+2)}, \ldots, x_{\pi(2n)}\}$ and $|X_{s,v}| \leq 2n(1-\alpha)$*

We say that B is partitioned with respect to the level L_i. B is said to be a partitioned arithmetic branching program if it is π-partitioned for some $\pi : [2n] \to [2n]$.

We now introduce the main tool used in the paper and prove its properties. Let $Y = \{y_1, y_2, \ldots, y_m\}$ and $Z = \{z_1, z_2, \ldots, z_m\}$ be two sets of variables. Let $f \in \mathbb{F}[Y, Z]$ be a multilinear polynomial. Define L_f to be the $2^m \times 2^m$ *partial derivatives matrix* as follows: for monic multilinear monomials $p \in \mathbb{F}[Y], q \in \mathbb{F}[Z]$, define $L_f(p, q)$ to be the coefficient of the monomial pq in f. Let us denote the rank of L_f by $\text{rank}(L_f)$. We extend the partial derivatives matrix to non-multilinear polynomials.

Definition 2.3 (Polynomial Coefficient Matrix)**.** *For $f \in \mathbb{F}[Y, Z]$, define M_f to be the $2^m \times 2^m$* polynomial coefficient matrix *with each entry from $\mathbb{F}[Y, Z]$ defined as follows. For monic multilinear monomials p and q in Y and Z respectively, $M_f(p, q) = G$ if and only if f can be uniquely written as $f = pq(G) + Q$, where $G, Q \in \mathbb{F}[Y, Z]$ such that G does not contain any variable other than those present in p and q, Q does not have any monomial m which is divisible by pq and which contains only variables that are present in p and q.*

We now consider the following simple example for clarity. Let P be the bivariate polynomial defined as

$$P(x_1, x_2) = x_1^2 \cdot x_2 + x_1 + 1$$

Now, consider the partition of the variables into Y and Z defined as $Y = \{x_1\}$ and $Z = \{x_2\}$. The matrix M_P is a 2×2 matrix with rows indexed by ϕ, x_1 and columns indexed by ϕ, x_2.

The entries of the matrix are as follows: $M_P(\phi,\phi) = 1$, $M_P(\phi, x_2) = 0$, $M_P(x_1,\phi) = 1$ and $M_P(x_1, x_2) = x_1$.

Observe that we can write, $f = \sum_{p,q} M_f(p,q)pq$ and for a multilinear polynomial f, M_f is same as L_f. For any function $S : Y \cup Z \to \mathbb{F}$, let us denote by $M_f|_S$ the matrix obtained by substituting each variable x by $S(x)$ at each entry in M_f. Let us define max-rank$(M_f) = \max_{S:Y\cup Z\to\mathbb{F}} \{\text{rank}(M_f|_S)\}$. The following proposition bounds the max-rank of the matrix (similar bounds on the rank of partial derivatives matrix for some cases have been proved in [RSY08]).

Proposition 2.4. *Let $f, g \in \mathbb{F}[Y, Z]$, $h \in \mathbb{F}[Y]$ and $w \in F[Z]$.*

2.4.1 If f contains variables $Y' \subseteq Y$ and $Z' \subseteq Z$ only, then max-rank$(M_f) \leq 2^a$ *where* $a = \min\{|Y'|, |Z'|\}$.

2.4.2 max-rank$(M_{f+g}) \leq$ max-rank$(M_f) +$ max-rank(M_g).

2.4.3 Let $Y_1, Y_2 \subseteq Y$ and $Z_1, Z_2 \subseteq Z$ such that $Y_1 \cap Y_2 = \phi$ and $Z_1 \cap Z_2 = \phi$. If $f \in \mathbb{F}[Y_1, Z_1]$ and $g \in \mathbb{F}[Y_2, Z_2]$, then max-rank$(M_{fg}) =$ max-rank$(M_f) \cdot$ max-rank(M_g).

2.4.4 max-rank$(M_{fh}) \leq$ max-rank(M_f) *and* max-rank$(M_{fw}) \leq$ max-rank(M_f).

2.4.5 If g is a linear form, then max-rank$(M_{fg}) \leq 2 \cdot$ max-rank(M_f).

2.4.6 If g can be expressed as $\sum_{i\in[r]} h_i w_i$ where $h_i \in \mathbb{F}[Y]$ and $w_i \in \mathbb{F}[Z]$, then max-rank$(M_{fg}) \leq r \cdot$ max-rank(M_f).

2.4.7 If g has r monomials, then max-rank$(M_{fg}) \leq r \cdot$ max-rank(M_f).

Proof. Let us prove each of the cases separately.

2.4.1 In the polynomial coefficient matrix M_f, the number of non-zero rows or non-zero columns will be at most 2^a. Thus, rank of M_f for any substitution would be at most 2^a. Hence, max-rank$(M_f) \leq 2^a$.

2.4.2 It is easy to observe that $M_{f+g} = M_f + M_g$. Let max-rank$(M_{f+g}) =$ rank$(M_{f+g}|_S)$ for some substitution S. Then,

$$\begin{aligned}
\text{max-rank}(M_{f+g}) &= \text{rank}(M_{f+g}|_S) \\
&= \text{rank}(M_f|_S + M_g|_S) \\
&\leq \text{rank}(M_f|_S) + \text{rank}(M_g|_S) \\
&\leq \text{max-rank}(M_f) + \text{max-rank}(M_g).
\end{aligned}$$

2.4.3 We think of M_f as a $2^{|Y_1|} \times 2^{|Z_1|}$ matrix and M_g as a $2^{|Y_2|} \times 2^{|Z_2|}$ matrix as all the other entries are zero. Similarly, we can think of M_{fg} as a $2^{|Y_1\cup Y_2|} \times 2^{|Z_1\cup Z_2|}$ matrix. Since f and g are defined over disjoint set of variables, we have $M_{fg} = M_f \otimes M_g$ where $\otimes$ denotes the tensor product of two matrices.

Let max-rank(M_{fg}) = rank$(M_{fg}|_S)$ for some substitution S. Then,

$$\begin{aligned}
\text{max-rank}(M_{fg}) &= \text{rank}(M_{fg}|_S) \\
&= \text{rank}((M_f \otimes M_g)|_S) \\
&= \text{rank}(M_f|_S \otimes M_g|_S) \\
&= \text{rank}(M_f|_S) \cdot \text{rank}(M_g|_S) \\
&\leq \text{max-rank}(M_f) \cdot \text{max-rank}(M_g) \ .
\end{aligned}$$

To see the other side of the inequality, let max-rank(M_f) = rank$(M_f|_{S_1})$ and max-rank(M_g) = rank$(M_g|_{S_2})$ for some substitutions $S_1 : Y_1 \cup Z_1 \to \mathbb{F}$ and $S_2 : Y_2 \cup Z_2 \to \mathbb{F}$. Let us define $S : Y \cup Z \to \mathbb{F}$ as the following:

$$S(x) = \begin{Bmatrix} S_1(x) & , & x \in Y_1 \cup Z_1 \\ S_2(x) & , & x \in Y_2 \cup Z_2 \\ 0 & , & otherwise \end{Bmatrix}$$

Thus,

$$\begin{aligned}
\text{max-rank}(M_{fg}) &\geq \text{rank}(M_{fg}|_S) \\
&= \text{rank}((M_f \otimes M_g)|_S) \\
&= \text{rank}(M_f|_{S_1} \otimes M_g|_{S_2}) \\
&= \text{rank}(M_f|_{S_1}) \cdot \text{rank}(M_g|_{S_2}) \\
&= \text{max-rank}(M_f) \cdot \text{max-rank}(M_g) \ .
\end{aligned}$$

2.4.4 Consider $h \in \mathbb{F}[Y]$. Let us first analyze the simplest case when $h = y$ for some $y \in Y$. Let us consider a row in M_{yf} which is indexed by the multilinear monomial p in the set of variables Y. Every monomial of the polynomial yf will be divisible by y, thus if p is not divisible by y then all the entries in this row will be zero. Let us consider such a multilinear monomial p in the set of variables Y which is divisible by y and a multilinear monomial q in the set of variables Z. Then, observe that

$$M_{yf}(p, q) = yM_f(p, q) + M_f(p/y, q)$$

Before proceeding further, we sketch the proof of this observation. Observe that we can decompose the polynomial f as

$$f = pq \cdot M_f(p, q) + \frac{pq}{y} \cdot M_f(p/y, q) + R$$

This is because every monomial of f falls into one of the following three sets:

- It is divisible by pq and contains no variables outside the support of pq.
- It is divisible by $\frac{pq}{y}$ and contains no variables outside the support of $\frac{pq}{y}$.

- Everything which does not fall in item 1 and item 2.

Since y divides p and p is multilinear, the sets in item 1 and item 2 above are disjoint. For every monomial α in item 3, observe that $y \cdot \alpha$ cannot be both divisible by pq and not contain a variable outside the support of pq, else α would fall in item 1 or item 2. Therefore, $y \cdot \alpha$ cannot contribute to $M_{yf}(p,q)$. Moreover, for every monomial α in item 1, its contribution to $M_{yf}(p,q)$ is precisely y times its contribution to $M_f(p,q)$ and for every monomial in item 2, its contribution to $M_{yf}(p,q)$ is equal to its contribution to $M_f(p/y,q)$. Therefore, it follows that $M_{yf}(p,q) = yM_f(p,q) + M_f(p/y,q)$.

Thus, rows in M_{yf} are a linear combination of rows in M_f. Hence, max-rank$(M_{yf}) \leq$ max-rank(M_f). For a subset $S \subseteq Y$, we denote the monomial $\Pi_{y \in S} y$ by y^S. Let us analyze the case when $h = y^S$. Consider a row of M_{fg} indexed by the multilinear monomial p in the set of variables Y. If p is not divisible by y^S, then all the entries in this row will be zero. Otherwise, for any multilinear monomial q in the variables Z, we can write, $M_{y^S f} = \sum_{S' \subseteq S} y^{S \setminus S'} M_f(p/y^{S'}, q)$. Thus, rows in $M_{y^S f}$ are a linear combination of rows in M_f. Similarly, we can show that for any monomial m in the variables Y, rows in M_{mf} are a linear combination of rows in M_f.

Now consider any $h = \sum_{i \in [r]} m_i \in \mathbb{F}[Y]$ where r is the number of monomials in h and each m_i is a distinct monomial. Thus, $M_{fh} = \sum_{i \in [r]} M_{m_i f}$. Thus, each row in M_{fh} is a linear combination of rows in M_f. Hence, max-rank$(M_{fh}) \leq$ max-rank(M_f).

2.4.5 Since g is a linear form in the variables $Y \cup Z$, g can be expressed as $g = g_1 + g_2$ where $g_1 \in \mathbb{F}[Y]$ and $g_2 \in \mathbb{F}[Z]$ and the proof follows from the properties 2.4.2 and 2.4.4.

2.4.6 Since $M_{fg} = \sum_{i \in [r]} M_{fh_i w_i}$, using item 4, we obtain a proof.

2.4.7 Each monomial m_i of g can be written as $g_i h_i$ such that g_i is a monomial in the variables Y and h_i is a monomial in the variables Z. Thus, the proof follows using item 6.

□

Full Rank Polynomials: Let $X = \{x_1, \cdots, x_{2n}\}, Y = \{y_1, \cdots, y_n\}$, and $Z = \{z_1, \cdots, z_n\}$ be the sets of variables and $f \in \mathbb{F}[X]$. The polynomial f is said to be a *full rank* polynomial if for any partition $A : X \to Y \cup Z$, rank$(L_{f^A}) = 2^n$, where f^A is the polynomial obtained from f after substituting $A(x)$ for every occurrence of variable x for every variable x.

We say that f is a *full max-rank* polynomial if max-rank$(M_{f^A}) = 2^n$ for any partition A. Any full rank polynomial is also a full max-rank polynomial. Many full rank polynomials have been studied in the literature [Jan08, Raz06, Raz09].

3 Lower Bounds against Homogeneous Depth-3 Circuits

Let Φ be a homogeneous $\Sigma\Pi\Sigma$ circuit with top fan-in k defined over the set of variables X and the field $\mathbb{F}$ computing a homogeneous polynomial $f = \sum_{i=1}^{k} P_i$, where $P_i = \prod_{j=1}^{deg(P_i)} l_{i,j}$, each $l_{i,j}$ is a linear form and $deg(P_i)$ is the fan-in of the i^{th} multiplication gate. For a partition $A : X \to Y \cup Z$, denote by Φ^A the circuit obtained after replacing every variable x by $A(x)$ and the corresponding polynomial by f^A. We prove the following upper bound on the max-rank(M_{f^A}).

Lemma 3.1. *Let Φ be a homogeneous $\Sigma\Pi\Sigma$ circuit as defined above and the degree of f be d. Then, for any partition $A : X \to Y \cup Z$,* max-rank$(M_{f^A}) \leq k \cdot 2^d$.

Proof. Let us denote by $l_{i,j}^A$ and P_i^A the polynomials obtained after substitution of x by $A(x)$ in the polynomials $l_{i,j}$ and P_i respectively.

Since each $l_{i,j}$ is a homogeneous linear form, a multiplication gate P_i computes a homogeneous polynomial of degree $deg(P_i)$. Thus if $deg(P_i) \neq d$, then the multiplication gate P_i does not contribute any monomial in the output polynomial f. Hence, it can be assumed without loss of generality that $deg(P_i) = d$ for all $i \in [k]$.

Since $l_{i,j}$ is a homogeneous linear form, max-rank$(M_{l_{i,j}^A}) \leq 2$. Thus, using Proposition 2.4.5,$\forall i \in [k]$: max-rank$(M_{P_i^A}) \leq 2^d$. Hence, using Proposition 2.4.2, max-rank$(M_{f^A}) \leq \sum_{i\in[k]}$ max-rank$(M_{P_i^A}) \leq k \cdot 2^d$. □

In [NW95], it was proved that any homogeneous $\Sigma\Pi\Sigma$ circuit for multiplying d $n \times n$ matrices requires $\Omega(n^{d-1}/d!)$ size. We prove a better lower bound using our techniques. Formally, let $X^1, X^2, \ldots, X^d$ be disjoint sets of variables of size n^2 each, with $X = \cup_{i\in[d]} X^i$. The variables in X^i will be denoted by x_{jk}^i for $j, k \in [n]$. We will be looking at the problem of multiplying d $n \times n$ matrices $A^1, A^2, \ldots, A^d$ where $(j, k)^{th}$ entry of matrix A^i, denoted by A_{jk}^i, is defined to be equal to x_{jk}^i for all $i \in [d]$ and $j, k \in [n]$. The output polynomial, that we are interested in, is the $(1, 1)^{th}$ entry of $\prod_{i\in[d]} A^i$ denoted by f. We also refer to f by IMM_d^n. The polynomial f is clearly a homogeneous multilinear polynomial of degree d. Moreover, any monomial in f contains one variable each from the sets $X^1, X^2, \ldots, X^d$.

We first prove an important lemma below.

Lemma 3.2. *For the polynomial f as defined above, there exists a bijective partition $B : X \to Y \cup Z$ such that* max-rank$(M_{f^B}) = n^{d-1}$.

Proof. We fix some notations first. For $i < j$, let us denote the set $\{i, i + 1, \ldots, j\}$ by $[i, j]$. Let us also denote the pair $((k, i), (k + 1, j))$ by e_{ijk} for any i, j, k. Construct a directed graph $G(V, E)$ on the set of vertices $V = [0, d - 1] \times [1, n]$ and consisting of edges $E = \{e_{ijk} \mid i, j \in [1, n], k \in [0, d - 1]\}$. Note that the edges e_{ijk} and e_{jik} are two distinct edges for fixed values of i, j, k when $i \neq j$. Let us also define a weight function $w : E \to X$ such that $w(e_{ijk}) = x_{ij}^{k+1}$.

It is easy to observe that the above graph encodes the matrices $A^1, A^2, \ldots, A^d$. The weights on the edges are the variables in the matrices. For example, a variable x_{ij}^{k+1} in the matrix A^{k+1} is the weight of the edge e_{ijk}. Let us denote the set of paths in G from the vertex $(0,1)$ to the vertex $(d,1)$ by $\mathcal{P}$. Let us extend the weight function and define $w(p) = \prod_{e \in p} w(e)$ for any path $p \in \mathcal{P}$. Since, all paths in $\mathcal{P}$ are of length equal to d, the weights corresponding to each of these paths are monomials of degree d.

Let us define the partition $B : X \to Y \cup Z$ as follows: all the variables in odd numbered matrices are assigned variables in Y and all the variables in even numbered matrices are assigned variables in Z. Let us denote the variable assigned by B to x_{ij}^{2k-1} by y_{ij}^{2k-1} and the variable assigned to x_{ij}^{2k} by z_{ij}^{2k}.

It follows from the matrix multiplication properties that for any path $p \in \mathcal{P}$, the monomial $w(p)$ is a monomial in the output polynomial. Each such path is uniquely specified once we specify the odd steps in the path. Now, specifying odd steps in the path corresponds to specifying a variable from each of the odd numbered matrices. To count number of such ways, let us first consider the case when d is even. There are $d/2$ odd numbered matrices and we have n^2 ways to choose a variable from each of these $d/2$ matrices except for the first matrix for which we can only choose a variable from the first row since our output polynomial is the $(1,1)^{th}$ entry. Thus, there are n^{d-1} number of ways to specify one variable each from the odd numbered matrices, the number of such paths is also n^{d-1}. We get the same count for the case when d is odd using a similar argument. Since once the odd steps are chosen, there is only one way to choose the even steps, all these n^{d-1} monomials give rise to non-zero entries in different rows and columns in the matrix M_{f^B}. Hence, the matrix is an identity block of dimension n^{d-1} upto a permutation of rows and columns and thus it has rank n^{d-1}. □

Theorem 3.3. *Any homogeneous $\Sigma\Pi\Sigma$ circuit for computing the product of d $n \times n$ matrices requires $\Omega(n^{d-1}/2^d)$ size.*

Proof. Let Φ be a homogeneous $\Sigma\Pi\Sigma$ circuit computing f. Then, using Lemma 3.1, for any partition A, max-rank$(M_{f^A}) \leq k \cdot 2^d$. From Lemma 3.2, we know that there exists a partition B such that max-rank$(M_{f^B}) = n^{d-1}$. Hence, $k \geq n^{d-1}/2^d$. □

It is worth noting that there exists a depth-2 circuit of size n^{d-1} computing IMM_d^n polynomial. As observed in Lemma 3.2, there are n^{d-1} monomials in the IMM_d^n polynomial. Hence, the sum of monomials representation for IMM_d^n will have top fan-in equal to n^{d-1}. We remark that when the number of matrices is a constant, the upper and lower bounds for IMM_d^n polynomial asymptotically match.

4 Lower Bounds against Depth-3 Circuits of Bounded Product Dimension

If a depth-3 circuit is not homogeneous, the fan-in of a product gate can be arbitrarily larger than the degree of the polynomial being computed. Hence the techniques in the previous

section fails to give non-trivial size lower bounds. In this section, we study depth-3 circuits with bounded product dimension - where the affine forms feeding into every product gate are from a linear vector space of small dimension and prove exponential size lower bounds for such circuits.

We will first prove an upper bound on the max-rank of the polynomial coefficient matrix for the polynomial computed by a depth-3 circuit of product dimension r, parameterized by r. Let C be a $\Sigma\Pi\Sigma$ circuit of product dimension r and top fan-in k computing a polynomial f.

Let us consider a circuit C_d in which the root gate is a plus gate with fan-in k and all the gates at the second layer compute the homogeneous component of degree d of the polynomial computed at the corresponding product gate in C.

Observation 4.1. *If C computes a homogeneous polynomial f of degree d, then C_d computes the same polynomial as C.*

Proof. Let us denote the polynomials computed at the product gates in C by P^j, where $j \in [k]$. We know that $f = \Sigma_{j\in[k]} P^j$. Let us expand the polynomial P^j as a sum of the homogeneous polynomials. Thus, $P^j = \Sigma_r P^j_r$, where P^j_r is the homogeneous component of degree r in P^j. Thus, $f = \Sigma_{j\in[k]}\Sigma_r P^j_r$. If f is a homogeneous polynomial of degree d, then in the above summation, all terms except $r = d$ cancels each other. Hence, $f = \Sigma_{j\in[k]} P^j_d$. By definition, the polynomial computed by C_d is also $\Sigma_{j\in[k]} P^j_d$. Hence, C_d computes the same polynomial as of C. □

It is clear that proving a lower bound on the top fan-in of circuit C_d suffices to imply the same lower bound on the top fan-in of circuit C computing a homogeneous polynomial. The bounded product-dimension of C proves useful to upper bound the max-rank of the polynomial coefficient matrix of the polynomial computed by C_d.

Let P be a product gate in C of fan-in s and g be the polynomial computed at P. Let us denote the corresponding gate in C_d by P_d and the polynomial computed at P_d by g_d. The polynomial g can be written as $\Pi_{i\in[s]} L_i$, where each L_i is an affine form for each i. Since the dimension of the span of the set $\{L_i\}_{i\in[s]}$ is at most r, it can be assumed without loss of generality that $L_1, L_2, \ldots, L_r$ form its basis. Let l_i be the homogeneous component of L_i for each i. Clearly the set $\{l_i\}_{i\in[r']}$ spans the set $\{l_i\}_{i\in[s]}$ for some $r' \leq r$. To simplify the notation, we will refer to r' as r. Clearly, the polynomial g_d can be written as a sum of products of d linear forms from the set $\{l_i\}_{i\in[r]}$. We now use the following lemma to simplify the product terms in g_d.

Lemma 4.2. *([Shp01]) Let $X = \{x_1, x_2, \ldots, x_d\}$. Any monomial of degree d in X can be written as a linear combination of d^{th} power of some 2^d linear forms in X. Further, each of the 2^d linear forms in the expression corresponds to $\Sigma_{i\in S} x_i$ for a subset S of $[d]$.*

The above lemma can be extended in the following manner.

Lemma 4.3. *Let $\mathcal{L} = \{l_1, l_2, \ldots, l_r\}$ be a set of homogeneous linear forms. Any polynomial which is a sum of products of d linear forms from $\mathcal{L}$ can be written as a linear combination of d^{th} powers of at most $\binom{d+r}{r}$ homogeneous linear forms.*

Proof. Consider any polynomial f which can be written as a sum of products of d linear forms from $\mathcal{L}$. If we treat $\mathcal{L}$ as the set of variables, then any product term q in f is a monomial of degree d. Applying Lemma 4.2, q can be written as $q = \Sigma_{i=1}^{2^d} l'_i$, where l'_i is a linear combination of the linear forms present in q for every i. In general, each l'_i can be written as $l'_i = \Sigma_{i\in[r]}\gamma_i l_i$ for non-negative integers γ_i satisfying $\Sigma_{i\in[r]}\gamma_i \leq d$. Now, each of the product terms in f can be expanded in a similar fashion into d^{th} powers of linear forms, each from the set $\{\Sigma_{i\in[r]}\gamma_i l_i : \gamma_i \in \mathbb{Z}^{\geq 0} \wedge \Sigma_{i\in[r]}\gamma_i \leq d\}$. The number of such distinct linear forms is at most $\binom{d+r}{r}$. Hence, the lemma follows. □

Using above lemma, the polynomial g_d can be written as a linear combination of d^{th} powers of at most $\binom{d+r}{r}$ homogeneous linear forms.

We now bound the max-rank of the power of a homogeneous linear form which in turn will give us a bound for g_d due to the subadditivity of max-rank.

Lemma 4.4. *Given a linear form l over a set of variables X and any positive integer t, the* max-rank *of l^t is at most $t+1$ for any partition of the set X of variables into Y and Z.*

Proof. Partition the linear form l into two parts, $l = l_y + l_z$, where l_y consists of all variables in l from the set Y and l_z consists of the variables which come from the set Z. By the binomial theorem, $l^t = \Sigma_{i=0}^{t}\binom{t}{i} l_y^i l_z^{t-i}$. Now, l_y^i is a polynomial just in Y variables and hence its max-rank can be bounded above by 1, and multiplication by l_z^{t-i} does not increase the max-rank any further, by Proposition 2.4.4. Hence, the max-rank of each term in the sum is at most 1 and there are at most $t+1$ terms, so, by using the subadditivity of max-rank, we get an upper bound of $t+1$ on the max-rank of the sum. □

We are now ready to prove an upper bound on the max-rank of the polynomial computed at the root gate of the circuit C_d.

Lemma 4.5. *Let C_d be an arithmetic circuit as defined above which computes a polynomial f_d over the set of variables X. Then, for any partition $A : X \to Y \cup Z$,* max-rank$(M_{f_d^A}) \leq k(d+1)\binom{d+r}{r}$.

Proof. Let us consider a gate P_d at the second layer in C_d computing a polynomial g_d. Let us denote by g_d^A the polynomial obtained after applying the partition A on each occurrence of variables from X in g_d. It follows from Lemma 4.3 that the polynomial g_d can be written as a linear combination of d^{th} powers of at most $(d+1)\binom{d+r}{r}$ homogeneous linear forms. From Lemma 4.4, the max-rank of d^{th} power of any linear form is at most $d+1$ for any partition. Hence, using the sub-additivity property of max-rank,

$$\text{max-rank}(M_{g_d^A}) \leq (d+1)\binom{d+r}{r}.$$

From the construction of C_d, the polynomial f_d is the sum of k polynomials computed at the second layer gates in C_d. Hence, using the sub-additivity property of max-rank again,

$$\text{max-rank}(M_{f_d^A}) \leq k(d+1)\binom{d+r}{r}.$$

□

In the following theorem, we use the above lemma to derive a size lower bound against the depth-3 circuits of bounded product-dimension.

Theorem 4.6. *There is an explicit polynomial in n variables and degree $\frac{n}{2}$ for which any $\Sigma\Pi\Sigma$ circuit C of product dimension at most $\frac{n}{10}$ requires size $2^{\Omega(n)}$.*

Proof. We describe the explicit polynomial f first. Let X be a set of n variables. Let us fix an equal sized partition A of X into Y and Z. Let us order all subset of Y and Z of size exactly $\frac{n}{4}$ in any order, say $S_1, S_2, \ldots, S_w$ and $T_1, T_2, \ldots, T_w$, where $w = \binom{n/2}{n/4}$. Let us define the polynomial f^A over the set of variables $Y \cup Z$ as follows: $f^A(Y, Z) = \Sigma_{i=1}^{w} \Pi_{y \in S_i} \Pi_{z \in T_i} yz$. The polynomial f over the set of variables X can be obtained by replacing variables in Y and Z in the polynomial f^A by $A^{-1}(Y)$ and $A^{-1}(Z)$ respectively. The polynomial f as defined is homogeneous and of degree $\frac{n}{2}$. The polynomial coefficient matrix of f^A is simply the diagonal submatrix, and the rank is at least $\binom{n/2}{n/4} \geq \frac{2^{\frac{n}{2}}}{\sqrt{n}}$.

Now we prove the size lower bound. Let C be a $\Sigma\Pi\Sigma$ circuit of product dimension at most r computing f. Let the top fan-in of C be k. Since f is homogeneous, let us consider the circuit C_d as described above which computes the same polynomial f where d is the degree of f. From Lemma 4.5, we know that,

$$\text{max-rank}(M_{f^A}) \leq k(d+1)\binom{d+r}{r}$$

This implies that,

$$k \geq \frac{\frac{2^{\frac{n}{2}}}{\sqrt{n}}}{\binom{d+r}{r}(d+1)}$$

For $d = \frac{n}{2}$, $r = \frac{n}{10}$, and a constant $c > 0$,

$$k \geq 2^{cn}.$$

□

Universality of Depth 3 Circuits with Product Dimension 1: It can be easily seen that the polynomial f can be computed by a $\Sigma\Pi\Sigma$ circuit of product-dimension 1. Applying Lemma 4.3 to each of the product gates in sum of product representation of f, a $\Sigma\Pi\Sigma$ circuit can be constructed in which the middle layer product gates are feeded by same linear form d times, and thus are of product-dimension 1.

An Impossibility result for Total Dimension Measure: Consider the trivial depth-2 circuit for any polynomial, where each monomial is computed by the product gate. Viewing this as a depth-3 circuit, the total dimension of the circuit is bounded above by n, since there are only n variables. Can we have a circuit with a smaller total dimension r computing the

same polynomial? We show that this is not always possible if $r = \alpha.n$ for a sufficiently small constant $\alpha < 1$. In particular, we show that even for $r = \frac{n}{10}$, the circuit cannot compute the polynomial that we constructed in the proof of Theorem 4.6 irrespective of the size of the circuit. As a first step, using the ideas developed in this section, we prove the following upper bound for the max-rank of such circuits.

Lemma 4.7. *If the total dimension of a $\Sigma\Pi\Sigma$ circuit is r, then the* max-rank *of the polynomial of degree d computed by the circuit is bounded above by $\binom{d+r}{r}(d+1)$.*

Proof. Observe that if the span of all the affine forms occurring in a $\Sigma\Pi\Sigma$ circuit is r (spanned by the basis $L_1, L_2, \ldots, L_r$), then each of the product gates in the circuit can be decomposed into sum of power of homogeneous linear forms as in Lemma 4.3. Moreover, each of these homogeneous linear forms will be of the form $\Sigma_i \alpha_i l_i$, where $\alpha_i \in \mathbb{Z}^{\geq 0} \wedge \Sigma_i \alpha_i \leq d$ and l_i is the homogeneous part of L_i for each i in $[r]$. Consequently, the max-rank of the circuit is bounded by $\binom{d+r}{r}(d+1)$ by Lemma 4.4 and the sub-additivity of max-rank. □

Thus, a $\Sigma\Pi\Sigma$ circuit of total dimension bounded by r, can compute the polynomial f described in the proof of Theorem 4.6, only if

$$\binom{d+r}{r}(d+1) \geq \frac{2^{\frac{n}{2}}}{\sqrt{n}} .$$

This in turn implies that for $r \leq \frac{n}{10}$, such circuits cannot compute the polynomial f irrespective of the number of gates they use.

5 Lower Bounds against Product-sparse Formulas

Let $Y = \{y_1, y_2, \ldots, y_m\}$ and $Z = \{z_1, z_2, \ldots, z_m\}$. Let Φ be a (s, d)-product-sparse formula defined over the field $\mathbb{F}$ and the variables $Y \cup Z$. For a node v, let us denote by Φ_v the sub-circuit rooted at v, and denote by Y_v and Z_v, the set of variables in Y and Z that appear in Φ_v respectively. Let us define, $a(v) = \min\{|Y_v|, |Z_v|\}$ and $b(v) = (|Y_v| + |Z_v|)/2$. We say that a node v is k-unbalanced if $b(v) - a(v) \geq k$. Let γ be a simple path from a leaf to the node v. We say that γ is k-unbalanced if it contains at least one k-unbalanced node. We say that γ is central if for every u, u_1 on the path γ such that there is an edge from u_1 to u in Φ, $b(u) \leq 2b(u_1)$. v is said to be k-weak if every central path that reaches v is k-unbalanced.

We prove that if v is k-weak then the max-rank of the matrix M_v can be bounded. The proof goes via induction on $|\Phi_v|$ and follows the same outline as that of [Raz09]. It only differs in the case of non-disjoint product gates which we include in full detail below. The proofs of the rest of cases is easy to see.

Lemma 5.1. *Let Φ be a (s, d)-product-sparse formula over the set of variables $Y \cup Z$, and let v be a node in Φ. Denote the product-sparse depth of v by $d(v)$. If v is k-weak,* max-rank$(M_v) \leq 2^{s \cdot d(v)} \cdot |\Phi_v| \cdot 2^{b(v) - k/2}$.

Proof. Consider the case when v is a s-sparse product gate with children v_1 and v_2. Without loss of generality it can be assumed that v is not disjoint.

Let us suppose that the product-sparse depth of v is d. Without loss of generality, assume that v_2 computes a sparse polynomial having at most 2^s number of monomials. Thus using Proposition 2.4.7,

$$\text{max-rank}(M_v) \leq 2^s \cdot \text{max-rank}(M_{v_1}) \tag{1}$$

Clearly, product-sparse depth of v_1 is at most $d-1$. Consider the following cases:

Case 1 : If $b(v) \leq 2b(v_1)$, then v_1 is also k-weak. Therefore, by induction hypothesis, $\text{max-rank}(M_{v_1}) \leq 2^{s(d-1)} \cdot |\Phi_{v_1}| \cdot 2^{b(v_1)-k/2} \leq 2^{s(d-1)} \cdot |\Phi_v| \cdot 2^{b(v)-k/2}$. Thus, using Equation 1,

$$\text{max-rank}(M_v) \leq 2^{sd} \cdot |\Phi_v| \cdot 2^{b(v)-k/2} \ .$$

Case 2 : If $b(v) > 2b(v_1)$, then $b(v_1) < b(v)/2 < b(v) - k/2$ since $b(v) \geq k$. Therefore using Proposition 2.4.1,

$$\text{max-rank}(M_{v_1}) \leq 2^{a(v_1)} \leq 2^{b(v_1)} < 2^{b(v)-k/2}$$

Therefore,

$$\text{max-rank}(M_v) \leq 2^s \cdot 2^{b(v)-k/2} \leq 2^{sd} \cdot |\Phi_v| \cdot 2^{b(v)-k/2} \ .$$

□

Now, to prove a lower bound for (s,d)-product-sparse formulas computing a full max-rank polynomial, we only need to show that there exists a partition that makes the formula k-weak with suitable values of s, d and k.

In [Raz06], Raz proved that for syntactic multilinear formulas of size at most $n^{\epsilon \log n}$, where ϵ is a small enough universal constant, there exists such a partition that makes the formula k-weak for $k = n^{1/8}$. We observe that this result also holds for product-sparse formulas, the proof given in [Raz06] is not specific to just syntactic multilinear formulas and holds for any arithmetic formula. We state the lemma again for completeness sake for the case of product-sparse formulas.

Lemma 5.2. *([Raz06]) Let $n = 2m$. Let Φ be a (s,d)-product-sparse formula over the set of variables $X = \{x_1, \ldots, x_n\}$, such that every variable in X appears in Φ, and such that $|\Phi| \leq n^{\epsilon \log n}$, where ϵ is a small enough universal constant. Let A be a random partition of the variables in X into $\{y_1, \ldots, y_m\} \cup \{z_1, \ldots, z_m\}$. Then with probability of at least $1 - n^{-\Omega(\log n)}$ the formula Φ^A is k-weak, for $k = n^{1/8}$.*

With above lemma, the following theorem is easy to derive.

Theorem 5.3. *Let X be a set of $2n$ variables and let $f \in \mathbb{F}[X]$ be a full max-rank polynomial. Let Φ be any (s,d)-product-sparse formula of size $n^{\epsilon \log n}$ for a constant ϵ (same as in [Raz06]). If $sd = o(n^{1/8})$, then f cannot be computed by Φ.*

Proof. Assume for a contradiction that Φ computes f. Using Lemma 5.2, for a random partition A, with probability of at least $1 - n^{-\Omega(\log n)}$, the formula Φ^A is k-weak for $k = n^{1/8}$. By Lemma 5.1, max-rank$(M_{\Phi^A}) \leq 2^{sd} \cdot |\Phi^A| \cdot 2^{n-k/2} < 2^n$. Since f is a full max-rank polynomial, it cannot be computed by Φ. Assume for a contradiction that Φ computes f. Using Raz's result, there exists a partition A such that the formula Φ^A is k-weak for $k = n^{1/8}$. By Lemma 5.1, max-rank$(M_{\Phi^A}) \leq 2^{sd} \cdot |\Phi^A| \cdot 2^{n-k/2} < 2^n$. Since f is a full max-rank polynomial, it cannot be computed by Φ. □

6 Lower Bounds against Partitioned Arithmetic Branching Programs

In the preliminaries section, we defined partitioned arithmetic branching programs which are a generalization of ordered ABPs. By definition, any polynomial computed by a partitioned ABP is homogenous. In [Jan08], a full rank homogenous polynomial was constructed. Thus, to prove lower bounds for partitioned ABP, we only need to upper bound the max-rank of the polynomial coefficient matrix for any polynomial being computed by a partitioned ABP. Now we prove such an upper bound and use it to prove exponential lower bound on the size of partitioned ABPs, thus extending result in [Jan08].

Theorem 6.1. *Let X be a set of $2n$ variables and $\mathbb{F}$ be a field. For any full max-rank homogenous polynomial f of degree n over X and $\mathbb{F}$, the size of any partitioned ABP computing f must be $2^{\Omega(n)}$.*

Proof. Let B be a π-partitioned ABP computing f for a permutation $\pi : [2n] \to [2n]$. Let $L_0, L_1, \ldots, L_n$ be the levels of B. Consider any partition A that assigns all n y-variables to $\{x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}\}$ and all n z-variables to $\{x_{\pi(n+1)}, x_{\pi(n+2)}, \ldots, x_{\pi(2n)}\}$. Let us denote by f^A the polynomial obtained from f after substituting each variable x by $A(x)$. Let B is partitioned with respect to the level L_i for $i = 2\alpha n$. We can write, $f = f_{st} = \sum_{v \in L_i} f_{s,v} f_{v,t}$. Consider a node $v \in L_i$. By definition, there are following two cases:

Case 1: $X_{s,v} \subseteq \{x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}\}$ and $|X_{v,t}| \leq 2n(1-\alpha)$. Thus, $f^A_{s,v} \in \mathbb{F}[Y]$. Hence, using Proposition 2.4.4 and 2.4.1,

$$\text{max-rank}(M_{f^A_{s,v} f^A_{v,t}}) \leq \text{max-rank}(M_{f^A_{v,t}}) \leq 2^{|X_{v,t}|/2} \leq 2^{n(1-\alpha)} .$$

Case 2: $X_{v,t} \subseteq \{x_{\pi(n+1)}, x_{\pi(n+2)}, \ldots, x_{\pi(2n)}\}$ and $|X_{s,v}| \leq 2n(1-\alpha)$. Thus, $f^A_{v,t} \in \mathbb{F}[Z]$. Hence, again using Proposition 2.4.4 and 2.4.1,

$$\text{max-rank}(M_{f^A_{s,v} f^A_{v,t}}) \leq \text{max-rank}(M_{f^A_{s,v}}) \leq 2^{|X_{s,v}|/2} \leq 2^{n(1-\alpha)} .$$

Thus, in any case, max-rank$(M_{f^A_{s,v} f^A_{v,t}}) \leq 2^{n(1-\alpha)}$ for all $v \in L_i$. Using Proposition 2.4.2,

$$\text{max-rank}(M_{f^A}) \leq |L_i| \cdot 2^{n(1-\alpha)} .$$

Since f is a full max-rank polynomial, we get $|L_i| \geq 2^{\alpha n}$. □

7 Variants of Maximum Rank Measure

Motivated by the applicability of the new measure, we study variants of the same in this section. A natural measure that can be considered for a matrix with polynomial entries is the dimension of the space spanned by the polynomials.

Let P be a polynomial in n variables and Y and Z be a partition of the set of all variables. For the Polynomial Partial Derivative Matrix M (of order $2^{|Y|} \times 2^{|Z|}$), we define the linear rank of this matrix as the maximum number of linearly independent rows or columns of M, where the constants involved in the linear combination come from the underlying field $\mathbb{F}$.

Linear Rank vs Max Rank of M : Let $C = \{c_1, c_2, \ldots, c_t\}$ be some vectors over a polynomial ring $\mathbb{F}[x]$. We now aim to compare the linear rank and the max rank of these vectors. We will denote by Q the vector $\sum_i \lambda_i c_i$ for indeterminates λ_i. Clearly, each entry of Q is a polynomial over the ring $\mathbb{F}[x][\lambda]$.

Claim 7.1. *For the matrix M, the linear rank is at least the max rank of M.*

Proof. Let the vectors in C be independent with respect to max rank. This implies that there is a substitution S for x such that for any λ, Q is not the all zeros vector. This in turn implies that for no λ, Q has all entries identically zero, which tells us that the vectors in C are independent with respect to linear rank. □

The converse of this observation is not true. Indeed, even though the vectors in C may be independent with respect to the linear rank, there may not be a unique substitution which gives us a non zero Q for every choice of λ. However, we prove that for sufficiently large $\mathbb{F}$, a high linear rank will imply a high max rank.

Claim 7.2. *For sufficiently large $\mathbb{F}$, for the matrix M, max rank is at least the linear rank.*

Proof. Let the vectors in C be independent with respect to linear rank. This means that for any choice of λ, Q is not the all zero vector. Now, if possible, let the vectors in C be dependent with respect to max rank. This means that for any substitution for variables in x, there is a choice of λ such that Q becomes an all zero vector for these substitions. Therefore, the number of zeros of polynomial entries in Q is at least as many as the number of ways of substituting the values of variables in x. More precisely, we apply the following observation. Let P be a polynomial over a field $\mathbb{F}$ and variables x and λs such that the degree of P in any of the λ variables in 1 and there are t of them. A trivial hitting set for this polynomial has size $\Pi_i(d_i + 1)2^t$. Therefore, if $\mathbb{F}^n \geq \Pi_i(d_i + 1)2^t$, then we know that P is identically zero. We just require our $\mathbb{F}$ to be large enough. So, for large enough $\mathbb{F}$, this will contradict the fact that the vectors in C are independent with respect to linear rank. □

This observation gives us the conclusion that for sufficiently large fields, linear rank and max rank are equivalent.

Proposition 7.3. *For large enough fields, the linear rank of the Polynomial Partial Derivative Matrix is equal to the max rank of the Polynomial Partial Derivative Matrix.*

8 Conclusion

We have introduced the polynomial coefficient matrix as a generalization of coefficient matrix for non-multilinear polynomials. The heart of our technique is the notion of max-rank of the polynomial coefficient matrix. Using the notion of max-rank instead of rank of the coefficient matrix as a complexity measure for polynomials, we have been able to generalize the known lower bounds on the multilinear models to certain non-multilinear models - most notably to improve the known lower bounds against homogeneous depth-3 circuits and to derive lower bounds against depth-3 circuits with product dimension $\frac{n}{10}$. Noting that it suffices to prove lower bounds against depth-3 circuits of product dimension n to derive lower bounds against arbitrary arithmetic circuits, one of the main open problems that arises from this work is to close this gap between n and $\frac{n}{10}$.

References

[AV08] Manindra Agrawal and V. Vinay. Arithmetic Circuits: A Chasm at Depth Four. In *Proceedings of Symposium on Foundations of Computer Science(FOCS)*, pages 67–75, 2008.

[DMPY12] Zeev Dvir, Guillaume Malod, Sylvain Perifel, and Amir Yehudayoff. Separating Multilinear Branching Programs and Formulas. In *Proceedings of Symposium on Theory of Computing (STOC)*, pages 615–624, 2012.

[FLMS13] Hervé Fournier, Nutan Limaye, Guillaume Malod, and Srikanth Srinivasan. Lower bounds for depth 4 formulas computing iterated matrix multiplication. *Electronic Colloquium on Computational Complexity (ECCC)*, 20:100, 2013.

[GK98] Dima Grigoriev and Marek Karpinski. An Exponential Lower Bound for Depth 3 Arithmetic Circuits. In *Proceedings of Symposium on Theory of Computing (STOC)*, pages 577–582, 1998.

[GKKS13a] A. Gupta, P. Kamath, N. Kayal, and R. Saptharishi. Approaching the chasm at depth four. *In Proceedings of CCC*, 2013.

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

[GR98] D. Grigoriev and A. Razborov. Exponential Complexity Lower Bounds for Depth 3 Arithmetic Circuits in Algebras of Functions over Finite Fields. In *Proceedings of Symposium on Foundations of Computer Science(FOCS)*, pages 269–278, 1998.

[Jan08] Maurice J. Jansen. Lower Bounds for Syntactically Multilinear Algebraic Branching Programs. In *Proceedings of Mathematical Foundations of Computer Science(MFCS)*, pages 407–418, 2008.

[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.

[KLSS14] Neeraj Kayal, Nutan Limaye, Chandan Saha, and Srikanth Srinivasan. An exponential lower bound for homogeneous depth four arithmetic formulas. *Electronic Colloquium on Computational Complexity (ECCC)*, 2014.

[Koi12] Pascal Koiran. Arithmetic Circuits: The Chasm at Depth Four Gets Wider. *Theor. Comput. Sci.*, 448:56–65, 2012.

[KS13a] Mrinal Kumar and Shubhangi Saraf. Lower bounds for depth 4 homogenous circuits with bounded top fanin. *Electronic Colloquium on Computational Complexity (ECCC)*, 20:68, 2013.

[KS13b] Mrinal Kumar and Shubhangi Saraf. Superpolynomial lower bounds for general homogeneous depth 4 arithmetic circuits. *CoRR*, abs/1312.5978, 2013.

[KSS13] Neeraj Kayal, Chandan Saha, and Ramprasad Saptharishi. A super-polynomial lower bound for regular arithmetic formulas. *Electronic Colloquium on Computational Complexity (ECCC)*, 20:91, 2013.

[NW95] N. Nisan and A. Wigderson. Lower Bounds on Arithmetic Circuits via Partial Derivatives. In *Proceedings of Symposium on Foundations of Computer Science(FOCS)*, pages 16–25, 1995.

[Raz06] Ran Raz. Separation of Multilinear Circuit and Formula Size. *Theory of Computing*, 2(1):121–135, 2006.

[Raz09] Ran Raz. Multi-linear Formulas for Permanent and Determinant are of Super-polynomial Size. *Journal of ACM*, 56:8:1–8:17, April 2009.

[RSY08] Ran Raz, Amir Shpilka, and Amir Yehudayoff. A Lower Bound for the Size of Syntactically Multilinear Arithmetic Circuits. *SIAM Journal of Computing*, 38(4):1624–1647, 2008.

[RY08] R. Raz and A. Yehudayoff. Lower Bounds and Separations for Constant Depth Multilinear Circuits. In *Proceedings of Conference on Computational Complexity*, pages 128–139, june 2008.

[Sax08] Nitin Saxena. Diagonal Circuit Identity Testing and Lower Bounds. In *International Colloquium on Automata, Languages and Programming(ICALP)*, pages 60–71, 2008.

[Shp01] Amir Shpilka. Affine Projections of Symmetric Polynomials. In *Proceedings of Conference on Computational Complexity*, pages 160–171, 2001.

[SW01] Amir Shpilka and Avi Wigderson. Depth-3 Arithmetic Circuits over Fields of Characteristic Zero. *Computational Complexity*, 10(1):1–27, 2001.

[SY10] Amir Shpilka and Amir Yehudayoff. Arithmetic Circuits: A Survey of Recent Results and Open Questions. *Foundations and Trends in Theoretical Computer Science*, 5(3-4):207–388, March 2010.

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