Super-polynomial lower bounds for depth-4 homogeneous arithmetic formulas

Neeraj Kayal * Nutan Limaye † Chandan Saha ‡ Srikanth Srinivasan §

Abstract

We show that any depth-4 homogeneous arithmetic formula computing the Iterated Matrix Multiplication polynomial $\mathrm{IMM}_{n,d}$ — the $(1,1)$-th entry of the product of d generic $n \times n$ matrices — has size $n^{\Omega(\log n)}$, if $d = \Omega(\log^2 n)$. Moreover, any depth-4 homogeneous formula computing the determinant polynomial Det_n — the determinant of a generic $n \times n$ matrix — has size $n^{\Omega(\log n)}$.

*Microsoft Research India. neeraka@microsoft.com

†Indian Institute of Technology Bombay. nutan@cse.iitb.ac.in

‡Indian Institute of Science. chandan@csa.iisc.ernet.in

§Indian Institute of Technology Bombay, srikanth@math.iitb.ac.in

1 Introduction

The problem of proving super-polynomial lower bounds for arithmetic circuits occupies a central position in complexity theory, much like the problem of proving super-polynomial lower bounds for boolean circuits. The model of arithmetic circuits is an algebraic analogue of the model of boolean circuits: An arithmetic circuit contains addition ($+$) and multiplication ($\times$) gates and it naturally computes a polynomial in the input variables over some underlying field. Proving super-polynomial arithmetic circuit lower bounds for an explicit family of polynomial, say the Permanent family, amounts to showing that $\mathsf{VP} \neq \mathsf{VNP}$ [25]. The complexity classes VP and VNP consist of families of polynomials and can be viewed as algebraic analogues of the classes P and NP respectively. Interestingly, it is known that $\mathsf{P} \neq \mathsf{NP}$ implies $\mathsf{VP} \neq \mathsf{VNP}$ [23]. The hope is that it might be possible to use algebraic and geometric insights along with the structure of arithmetic circuits to make progress towards settling the VP vs VNP question. Till date, research on arithmetic circuits has produced several interesting results that have enriched our understanding of the lower bound problem and the related problems on polynomial identity testing & reconstruction (or learning) of arithmetic circuits. The survey [22] gives an account of some of the results and outstanding open questions in this area.

Previous work on super-polynomial lower bounds. Raz [20] showed that any multilinear formula computing the determinant Det_n (or the permanent Perm_n) polynomial has $n^{\Omega(\log n)}$ size. This result was refined to show a super-polynomial gap between multilinear circuits and formulas [19]. A significantly better bound was later shown for bounded (i.e. constant) depth multilinear circuits [21]: A depth-d multilinear circuit computing Det_n or Perm_n has size $2^{n^{\Omega(1/d)}}$.

The study of constant depth circuits has gained momentum in the recent years after a striking connection was shown between lower bounds for general circuits and that for depth-4 & depth-3 formulas. Building on the *depth reduction* results of [26, 3], a string of works [2, 13, 24] arrived at the following result: A $2^{\omega(\sqrt{d}\log N)}$ size lower bound for depth-4 homogeneous formulas [1], computing a degree-d, N-variate polynomial (in a polynomial family), implies a super-polynomial lower bound for general circuits. Further, if the polynomial family belongs to VNP then such a lower bound would imply $\mathsf{VP} \neq \mathsf{VNP}$. A similar implication is true even for depth-3 formulas, although at the loss of the homogeneity condition - this is a surprising result due to [8].

The formal degree of a homogeneous formula is bounded by the degree of the computed polynomial - a feature that is quite effective in proving lower bounds using *partial derivatives* based methods. The approach of proving lower bounds by studying the space of partial derivatives of the computed polynomial was introduced by [18], who showed an exponential lower bound for homogeneous depth-3 formulas [2]. (For depth-3 formulas over fixed finite fields, an exponential lower bound was shown by [5, 6].) Indeed, the super-polynomial lower bounds obtained by [20, 19, 21], and also some others like [1], are based upon studying partial derivatives or associated matrices involving partial derivatives like the Jacobian or the Hessian.

The situation for depth-4 homogeneous formulas has been substantially improved by the recent work of [10, 7], followed by the work of [12] and [4]. These work have lead to a $2^{\Omega(\sqrt{d}\log N)}$ lower bound for depth-4 homogeneous formulas with bottom fan-in $O(\sqrt{d})$ (where d is the degree of the N-variate 'target' polynomial on which the lower bound is shown). Further, [12] and [4] together imply a super-polynomial separation between *algebraic branching programs* and *regular formulas* - two natural sub-models of arithmetic circuits [3]. A seemingly tempting

[1] with bottom fan-in bounded by $O(\sqrt{d})$

[2] Prior to this work, Nisan [17] showed an exponential lower bound for noncommutative arithmetic formulas

[3] In fact, a very recent work of [14] shows a super-polynomial separation between *general formulas* and *regular*

problem left open in these work is, if the lower bound of $2^{\Omega(\sqrt{d}\log N)}$ in the above statement could be improved to $2^{\omega(\sqrt{d}\log N)}$, a super-polynomial lower bound for general circuits would ensue immediately. Another recent work [15] has shown an exponential lower bound for depth-4 homogeneous formulas with constant top fan-in. At the heart of these results lies the study of the space of *shifted partial derivatives* of polynomials and an associated measure called the *dimension of the shifted partials* - a technique introduced in [10, 7]. Loosely speaking, the dimension of the shifted partials of a polynomial g refers to the dimension of the $\mathbb{F}$-linear vector space generated by the set of polynomials obtained by multiplying (shifting) the partial derivatives of g with monomials of suitable degrees.

Our results. In an attempt to understand the strength of the shifted partials method better, a recurring open problem stated in [12, 4, 14, 24] is to show a super-polynomial lower bound for homogeneous depth-4 formulas. Whether the shifted partial measure can be used to prove such a result or not is not exactly clear to us. This very recent work by [14] seems to suggest that the answer is likely in the negative. However, this does not rule out the possibility of using a different measure, perhaps closely related to the shifted partials, to achieve the same goal. It turns out that indeed it is possible to use a slightly modified (or augmented) version of the shifted partial measure to show a super-polynomial lower bound for depth-4 homogeneous formulas. For the ease of reference in this paper, we will call this modified measure the *shifted projected partials*. Loosely speaking, the idea is to *view the partials after 'projecting' them to an appropriate set of monomials.*

Our results are formally stated below.

Theorem 1. *A depth-4 homogeneous formula computing the Iterated Matrix Multiplication polynomial $IMM_{n,d}$ — the $(1,1)$-th entry of the product of d generic $n \times n$ matrices — has $n^{\Omega(\log n)}$ size, assuming $d = \Omega(\log^2 n)$. If $d \leqslant \epsilon \log^2 n$ for a sufficiently small $\epsilon > 0$ then any depth-4 homogeneous formula computing the $IMM_{n,d}$ polynomial has size $n^{\Omega(\sqrt{d})}$.*

Theorem 2. *A depth-4 homogeneous formula computing the determinant polynomial Det_n — the determinant of a generic $n \times n$ matrix — has size $n^{\Omega(\log n)}$.*

Subsequent work There has been quite some progress on this question since we submitted these results to STOC 2014. Independent of our work, Kumar and Saraf [16] give an $N^{\Omega(\log\log N)}$ lower bound for $\Sigma\Pi\Sigma\Pi$ homogeneous formulas computing an explicit polynomial (more formally, a polynomial in VNP) in N variables. Further, we [11] have been able to strengthen the lower bounds presented here by showing an $N^{\Omega(\sqrt{d})}$ lower bound for an explicit polynomial in N variables with $d = N^{\Omega(1)}$, yielding an *exponential* lower bound for homogeneous $\Sigma\Pi\Sigma\Pi$ formulas. In both these works, the explicit polynomials are variations of the Nisan-Wigderson polynomials introduced in [12].

The rest of the paper is devoted to proving Theorems 1 and 2.

2 Definitions and notations

The Iterated Matrix Multiplication polynomial. Fix any $n, d \in \mathbb{N}$ such that $n, d \geqslant 2$. Define sets of variables $X_1, \ldots, X_d$ as follows. If $p \in \{1, d\}$, $X_p = \left\{ x_j^{(p)} \,\middle|\, j \in [n] \right\}$ is a set of n variables; otherwise $X_p = \left\{ x_{j,k}^{(p)} \,\middle|\, j, k \in [n] \right\}$ is a set of n^2 variables. Let $X = \bigcup_{p \in [d]} X_p$

formulas.

and $N := |X| = (d-2)n^2 + 2n$. We think of X_1 and X_d as row and column vectors of variables respectively and of X_p ($p \in [d]\backslash\{1,d\}$) as $n \times n$ matrices of variables. Now, we define the $\mathrm{IMM}_{n,d}(X)$ polynomial as the (unique entry of) the product of the matrices $X_1 \cdots X_d$. Formally,

$$\mathrm{IMM}_{n,d}(X) = \sum_{j_1,\ldots,j_{d-1}} x^{(1)}_{j_1} x^{(2)}_{j_1,j_2} \cdots x^{(d-1)}_{j_{d-2},j_{d-1}} x^{(d)}_{j_{d-1}}$$

An alternate, combinatorial and quite useful way of looking the above polynomial is through the lens of *Algebraic Branching Programs* (ABPs) (see, e.g., [22]). Consider a homogeneous ABP $\mathcal{A}$ defined over vertex sets $V_0, \ldots, V_d$ where $V_0 = \{v^{(0)}\}$, $V_d = \{v^{(d)}\}$, and $V_p = \{v^{(p)}_i \mid i \in [n]\}$ for $p \in [d-1]$. The ABP contains all possible edges between V_p and V_{p+1} for $p \in \{0, \ldots, d-1\}$. Each edge e is labelled with a *distinct* variable from X: the edge $e = (v^{(0)}, v^{(1)}_j)$ is labelled with $x^{(1)}_j$; $e = (v^{(p)}_i, v^{(p+1)}_j)$ is labelled with $x^{(p+1)}_{i,j}$; finally, $e = (v^{(d-1)}_i, v^{(d)})$ is labelled with $x^{(d)}_j$. The ABP computes a polynomial by summing over all paths ρ from $v^{(0)}$ to $v^{(d)}$ the monomial which is obtained by multiplying the variables labelling the edges along the path. It is easily verified that the polynomial computed this way is $\mathrm{IMM}_{n,d}$.

Throughout, we omit mention of the set of variables X if the values of n and d are fixed. Recall that a monomial over the variables in X is said to be *multilinear* if it is not divisible by x^2 for any $x \in X$. Given a monomial $\mathbf{x^i}$, we define the *matrix support of* $\mathbf{x^i}$ — denoted $\mathrm{MSupp}(\mathbf{x^i})$ — to be the set of all $p \in [d]$ such that m is divisible by some $x \in X_p$. We call a monomial $\mathbf{x^i}$ *set-multilinear* if it is multilinear and furthermore, it is divisible by exactly one variable in X_p for each $p \in \mathrm{MSupp}(\mathbf{x^i})$.

Depth-4 arithmetic formulas. We recall some basic definitions regarding arithmetic circuits and formulas; for a more thorough introduction, see the excellent survey [22]. Let Y be a finite set of variables. An arithmetic formula C over $\mathbb{F}[Y]$ is a rooted tree the leaves of which are labelled by variables in Y and elements of the field $\mathbb{F}$ and internal nodes (called *gates*) by $+$ and $\times$. This computes a polynomial $f \in \mathbb{F}[Y]$ in a natural way. By the *size* of a formula, we mean the number of vertices in the tree, and by the *depth* of a formula, we mean the longest root-to-leaf path in the tree. Our focus here is on *depth-4 formulas*, which are formulas that can be written as sums of products of sums of products, otherwise known as $\Sigma\Pi\Sigma\Pi$ formulas. We will prove lower bounds for *homogeneous* $\Sigma\Pi\Sigma\Pi$ formulas which are $\Sigma\Pi\Sigma\Pi$ formulas such that each node computes a homogeneous polynomial (i.e. a polynomial whose every monomial has the same degree). Given a $\Sigma\Pi\Sigma\Pi$ formula, the layer 0 nodes will refer to the leaf nodes, the layer 1 nodes to the Π-gates just above the leaf nodes, etc. The *top fan-in* refers to the fan-in of the root node on layer 4. We also consider variants of $\Sigma\Pi\Sigma\Pi$ formulas with bounds on the fan-ins of the Π gates. By $\Sigma\Pi^{[D]}\Sigma\Pi^{[t]}$ formulas, we mean $\Sigma\Pi\Sigma\Pi$ formulas where the fan-ins of the layer 1 and layer 3 Π gates are *at most* t and D respectively.

The measure. Let f be a polynomial in $\mathbb{F}[x_1, \ldots, x_N]$ of degree d. Let S_1 and S_2 be certain fixed subsets of monomials in the N variables. For a polynomial $g = \sum_{\mathbf{i}} c_{\mathbf{i}} \mathbf{x^i}$, where $c_{\mathbf{i}} \in \mathbb{F}$, define $\pi_{S_1}(g) := \sum_{\mathbf{x^i} \in S_1} c_{\mathbf{i}} \mathbf{x^i}$ i.e. $\pi_{S_1}(g)$ is the projection of g onto the monomials in S_1. Consider the vector space $\mathcal{V}_{k,\ell}(f)$, which we call the space of the shifted projected partials of f [4] and is defined to be

$$\mathrm{span}_{\mathbb{F}}\{\mathbf{x^i} \cdot \pi_{S_1}\left(\frac{\partial^k f}{\partial x_{j_1} \ldots \partial x_{j_k}}\right) : |\mathbf{i}| \leqslant \ell \text{ and } \prod_{q \in [k]} x_{j_q} \in S_2\}. \tag{1}$$

[4] borrowing notations and terminologies from [12] and [4]

The measure is the dimension of this space, denoted by $\mu_{k,\ell}(f) := \dim(\mathcal{V}_{k,\ell}(f))$. The choices of S_1 and S_2 used for $\mathrm{IMM}_{n,d}$ will be made precise in Section 3. The parameters k and ℓ will also be fixed in the analysis later. Since S_1 and S_2 are fixed, it is easy to verify that the measure obeys the subadditivity property.

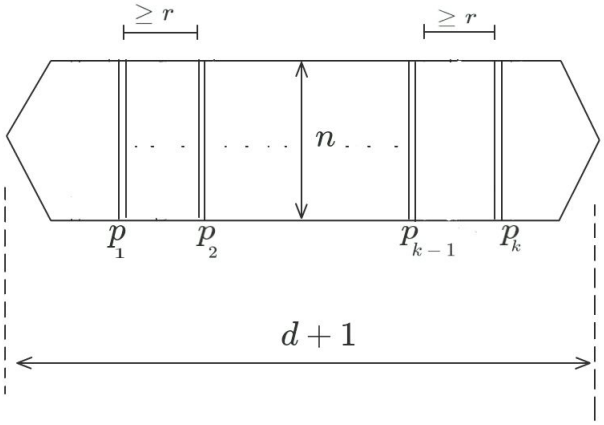
Lemma 3 (Subadditivity Lemma)**.** *For any $f, g \in \mathbb{F}[X]$, we have $\mu_{k,\ell}(f+g) \leqslant \mu_{k,\ell}(f)+\mu_{k,\ell}(g)$.*

3 Preliminaries

Throughout this section, we fix some $n, d \in \mathbb{N}$ and work with $X = \bigcup_{p\in[d]} X_p$, the set of variables over which $\mathrm{IMM}_{n,d}$ is defined.

3.1 The derivatives

We define the derivative operators as in [4]. Let $X_1, X_2, \ldots, X_d$ be the matrices that define $\mathrm{IMM}_{n,d}$. Let k be a parameter which will be fixed later and $r = \lfloor \frac{d}{k+1} \rfloor - 1$. We choose evenly spaced k indices $p_1, p_2, \ldots, p_k$, i.e. $p_1, p_2, \ldots, p_k$ are chosen so that for all $1 \leqslant q \leqslant k+1$, $p_q - (p_{q-1}+1)) \geqslant r$, where $p_0 = 0$ and $p_{k+1} = d+1$. Now we choose one variable each from the matrices $X_{p_1}, X_{p_2}, \ldots, X_{p_k}$, say $x^{(p_1)}_{i_1,j_1}, x^{(p_2)}_{i_2,j_2}, \ldots, x^{(p_k)}_{i_k,j_k}$, respectively and take derivatives with respect to them - this defines the set S_2 in Equation (1). More precisely, for any $I = (i_1, j_1, \ldots, i_k, j_k) \in [n]^{2k}$, let m_I denote the monomial $x^{(p_1)}_{i_1,j_1} x^{(p_2)}_{i_2,j_2} \ldots x^{(p_k)}_{i_k,j_k}$ and for a polynomial $F \in \mathbb{F}[X]$, let $\partial_I F$ denote $\left(\frac{\partial^k F}{\partial x^{(p_1)}_{i_1,j_1} \ldots \partial x^{(p_k)}_{i_k,j_k}} \right)$. Then S_2 is the set $\{m_I \mid I \in [n]^{2k}\}$.



3.2 Restriction applied to $\mathrm{IMM}_{n,d}(X)$

We will define a restriction as in Section 6 of [4]. Fix $p'_1, \ldots, p'_{k+1} \in [d]$ such that for each $q \in [k+1]$, we have $\min\{p'_q - (p_{q-1}+1), p_q - (p'_q+1)\} \geqslant \lfloor \frac{r-1}{2} \rfloor$, where $p_0, \ldots, p_{k+1}, r$ are as defined in Section 3.1. Recall that S_n is standard notation for the set of all bijections from the set $[n]$ to itself. Let $P' = \{p_q \mid q \in [k]\} \cup \{p'_q \mid q \in [k+1]\}$. For $j_1, j_d \in [n]$ and tuple of bijections $B = (\phi_p \in S_n : p \in [d] \backslash (P' \cup \{1, d\}))$, we define the restriction $\tau = \tau_{j_1,j_d,B}$ as follows:

For $x \in X$

$$\tau(x) = \begin{cases} 0 & \text{if } x = x_j^{(1)} \text{ for } j \neq j_1, \\ 0 & \text{if } x = x_j^{(d)} \text{ for } j \neq j_d, \\ 0 & \text{if } x = x_{i,j}^{(p)} \text{ for } p \in [d] \backslash (P' \cup \{1, d\}) \text{ and } \phi_p(i) \neq j, \\ x & \text{otherwise.} \end{cases}$$

We denote by $\mathcal{R}$ the set of all such restrictions. Given a restriction $\sigma \in \mathcal{R}$ and a polynomial $f \in \mathbb{F}[X]$, we denote by $f|_\sigma$ the polynomial $f(\sigma(x) : x \in X)$. Let $\tau_0 = \tau_{1,1,B_0}$ where B_0 is a tuple of identity permutations and let $F = \mathrm{IMM}_{n,d}|_{\tau_0}$.

3.3 Measure $\mu_{k,\ell}$ applied to a restriction of $\mathrm{IMM}_{n,d}(X)$

Just as in [4], we work with the special restriction $F = \mathrm{IMM}_{n,d}|_{\tau_0}$ for the ease of presentation. The lower bound on the measure given by Lemma 4 (below) holds for every restriction τ applied to $\mathrm{IMM}_{n,d}$ i.e. for every $\mathrm{IMM}_{n,d}|_\tau$. In [4] it was proved that the dimension of the shifted partials space of F is *large*. It turns out that the measure $\mu_{k,\ell}(F)$ is exactly equal to the the dimension of the shifted partials space of F, if the set S_1 in Equation (1) is defined as follows.

The projection π_{S_1}: The map π_{S_1} becomes well defined once we specify the set S_1. Let $p_1, p_2, \ldots, p_k$ be as defined in Section 3.1. The set S_1 is defined as the set of all set-multilinear monomials which are supported on variables in $X \backslash \left(\cup_q X_{p_q}\right)$. We can now prove this lemma formally.

Lemma 4. *Let $k, \ell \in \mathbb{N}$ be arbitrary parameters such that $20k < d < \ell$ and $k \geqslant 2$. Then,*

$$\mu_{k,\ell}(F) \geqslant M \cdot \binom{N+\ell}{\ell} - M^2 \cdot \binom{N+\ell-d/40}{\ell-d/40},$$

where $M = \left\lfloor n^{1.5k} \right\rfloor$.

The proof of this lemma follows that of [4, Lemma 11] closely. For completeness, the entire proof is presented in the appendix.

4 Lower bounds for certain $\Sigma\Pi\Sigma\Pi$ formulas

In this section, we prove a lower bound for certain variants of $\Sigma\Pi\Sigma\Pi$ formulas that we define below. Fix n and d and let X be the set of input variables to $\mathrm{IMM}_{n,d}$. Let Z denote the set $\bigcup_{p \in P'} X_p$ — where P' is as defined in Section 3 — and $Y = X \backslash Z$. Let $\mathcal{J}$ denote the ideal generated by all the *non*-set-multilinear monomials over X.

Given $X' \subseteq X$ and $f \in \mathbb{F}[X]$, we denote by $\deg_{X'}(f)$ the degree of f seen as a polynomial over the variables in X' with coefficients from $\mathbb{F}[X \backslash X']$.

Definition 5 ($\Sigma\Pi^{[D]}\Sigma\Pi_Y^{[t]}$ formulas)**.** *An $\Sigma\Pi\Sigma\Pi$ formula C is said to be an $\Sigma\Pi^{[D]}\Sigma\Pi_Y^{[t]}$ formula if the fan-ins of its layer 3 multiplication gates are bounded by D, and the layer 1 Π gates in C compute monomials $\mathbf{x^i}$ s.t. $\deg_Y(\mathbf{x^i}) \leqslant t$.*

The main result of this section is the following:

Lemma 6. *For large enough $n, d \in \mathbb{N}$, any $D \in \mathbb{N}$ and $t, k \in \mathbb{N}$ such that $t \geqslant 4$ and $kt \leqslant d/1000$, the following holds. Let C be a $\Sigma\Pi^{[D]}\Sigma\Pi_Y^{[\lfloor t/2 \rfloor]}$ formula such that $C = \mathrm{IMM}_{n,d}|_\sigma \pmod{\mathcal{J}}$ for some $\sigma \in \mathcal{R}$. Then, the top fan-in of C is at least $\frac{1}{4 \cdot 2^d} \left(\frac{n^{1.25}k}{eD}\right)^k$.*

The proof of the above combines Lemma 4 along with an upper bound on the dimension of the shifted projected partial derivative space of C. To be precise, we prove the following:

Lemma 7. *For any $n, d, D, k, \ell \geqslant 2$, we have the following. Let C be a $\Sigma\Pi^{[D]}\Sigma\Pi_Y^{[t]}$ formula over the variables in X of top fan-in s and let f be any polynomial from $\mathcal{J}$. Then, we have*

$$\mu_{k,\ell}(C+f) \leqslant s \cdot 2^d \cdot \binom{D}{k} \cdot \binom{N+\ell+(t+1)k}{\ell+(t+1)k}$$

Assuming the above lemma, let us finish the proof of Lemma 6. We will need the following technical facts (see [4, Section 3] for the proof of Fact 9).

Fact 8. *For any integers N, ℓ, r such that $r < \ell$, we have*

$$\left(\frac{N+\ell}{\ell}\right)^r \leqslant \frac{\binom{N+\ell}{\ell}}{\binom{N+\ell-r}{\ell-r}} \leqslant \left(\frac{N+\ell-r}{\ell-r}\right)^r.$$

Fact 9. *For any integers $n, d \geqslant 2$, $N = (d-2)n^2 + 2dn$ and $t \geqslant 1$, there exists an integer $\ell > d$ such that $n^{1/16} \leqslant \left(\frac{N+\ell}{\ell}\right)^t \leqslant n^{1/4}$.*

of Lemma 6. [4, Claim 14] observe that all the polynomials $\mathrm{IMM}_{n,d}|_\sigma$ are equivalent in the sense that they can be transformed to one another by permuting the variables in each X_p ($p \in [d]$) suitably, which also preserves the ideal $\mathcal{J}$. Thus, it suffices to prove the lemma for $F = \mathrm{IMM}_{n,d}|_{\tau_0}$ only.

By Fact 9, we can fix $\ell \in \mathbb{N}$ such that $n^{1/16} \leqslant \left(\frac{N+\ell}{\ell}\right)^t \leqslant n^{1/4}$. For this choice of ℓ, we first lower bound $\mu_{k,\ell}(F)$ using Lemma 4, which tells us that

$$\mu_{k,\ell}(F) \geqslant M \cdot \binom{N+\ell}{\ell} - M^2 \binom{N+\ell-d/40}{\ell-d/40} \tag{2}$$

where $M = \lfloor n^{1.5k} \rfloor$.

Note that for our setting of parameters, we have

$$\begin{aligned}\frac{M\binom{N+\ell}{\ell}}{M^2\binom{N+\ell-d/40}{\ell-d/40}} &\geqslant \frac{1}{n^{1.5k}} \cdot \left(\frac{N+\ell}{\ell}\right)^{d/40} \qquad \text{(by Fact 8)} \\ &\geqslant \frac{(n^{1/16t})^{d/40}}{n^{1.5k}} \geqslant n^{\Omega(k)} \geqslant 2\end{aligned}$$

for large enough n. Thus, using the above and (2), we obtain that

$$\mu_{k,\ell}(F) \geqslant \frac{M}{2} \cdot \binom{N+\ell}{\ell} \tag{3}$$

Now, since $C = F \pmod{\mathcal{J}}$, we have $F = C + f$ for some polynomial $f \in \mathcal{J}$. Then, Lemma 7 and Inequality (3) above together imply that

$$\begin{aligned}s &\geqslant \frac{M}{2 \cdot 2^d \cdot \binom{D}{k}} \cdot \frac{\binom{N+\ell}{\ell}}{\binom{N+\ell+([t/2]+1)k}{\ell+([t/2]+1)k}} \geqslant \frac{1}{2 \cdot 2^d} \frac{n^{1.5k}/2}{(\frac{eD}{k})^k} \cdot \frac{\binom{N+\ell}{\ell}}{\binom{N+\ell+tk}{\ell+tk}} \\ &\geqslant \frac{1}{4 \cdot 2^d} \frac{n^{1.5k}}{(\frac{eD}{k})^k} \cdot \frac{1}{\left(\frac{N+\ell}{\ell}\right)^{tk}} \qquad \text{(by Fact 8)} \\ &\geqslant \frac{1}{4 \cdot 2^d} \left(\frac{n^{1.5}k}{eD \cdot \left(\frac{N+\ell}{\ell}\right)^t}\right)^k \geqslant \frac{1}{4 \cdot 2^d} \left(\frac{n^{1.5}k}{eD \cdot n^{1/4}}\right)^k \quad \text{(by choice of } \ell) \\ &\geqslant \frac{1}{4 \cdot 2^d} \left(\frac{n^{1.25}k}{eD}\right)^k,\end{aligned}$$

which implies the lemma. □

All that remains is to prove Lemma 7, which is done below.

4.1 Proof of Lemma 7

Fix C and f as in the statement of the lemma. By Lemma 3, we know that $\mu_{k,\ell}(C+f) \leqslant \mu_{k,\ell}(C) + \mu_{k,\ell}(f)$. The latter term is handled first.

Claim 10. *For every $g \in \mathcal{J}$ and every $I \in [n]^{2k}$, we have $\pi_{S_1}(\partial_I g) = 0$. In particular, $\mu_{k,\ell}(g) = 0$.*

Proof. By linearity, it suffices to prove the above for every monomial $\mathbf{x^i} \in \mathcal{J}$. Since $\mathbf{x^i}$ is non-set multilinear, there exists some $p \in [d]$ and $x, y \in X_p$ (possibly equal) such that $xy | \mathbf{x^i}$. There are two cases to consider:

- $p \notin \{p_1, \ldots, p_k\}$: In this case, it is easy to see that $xy | \partial_I \mathbf{x^i}$ as well and hence $\pi_{S_1}(\partial_I \mathbf{x^i}) = 0$.
- $p \in \{p_1, \ldots, p_k\}$: Either x and y are distinct or $x = y$. In the former case, we note that since we derive w.r.t. at most one of x or y, it must be the case that either $x | \partial_I \mathbf{x^i}$ or $y | \partial_I \mathbf{x^i}$. In the latter case, since we derive at most once w.r.t. x, we have $x | \partial_I \mathbf{x^i}$. In either case, $\pi_{S_1}(\partial_I \mathbf{x^i}) = 0$.

□

Thus, we only need to bound $\mu_{k,\ell}(C)$. Assume that $C = \sum_{i=1}^{s} C_i$, where each C_i is a $\Pi^{[D]}\Sigma\Pi_Y^{[t]}$ formula. By Lemma 3, it suffices to show that for each $i \in [s]$, we have

$$\mu_{k,\ell}(C_i) \leqslant 2^d \cdot \binom{D}{k} \cdot \binom{N + \ell + (t+1)k}{\ell + (t+1)k} \tag{4}$$

Let $i \in [s]$ be fixed for the rest of the proof. We may assume that the top fan-in of C_i is exactly D and hence $C_i = \prod_{p \in [D]} Q_p$ where $\deg_Y(Q_p) \leqslant t$ for each $p \in [d]$. Consider any $I \in [n]^{2k}$. By the product rule for differentiation, we can see that $\partial_I C_i$ can be written as

$$\partial_I(C_i) = \sum_{A \subseteq [D] : |A| = D-k} \left(\prod_{p \in A} Q_p \right) \cdot Q'_{I,A}$$

where for each A, $Q'_{I,A}$ satisfies $\deg_Y(Q'_{I,A}) \leqslant tk$. Let Q_A denote $\prod_{p \in A} Q_p$. Hence we have

$$\left\{ \partial_I(C_i) \;\middle|\; I \in [n]^{2k} \right\} \subseteq$$
$$\operatorname{span}_{\mathbb{F}} \left\{ Q_A \cdot \mathbf{x^j} \;\middle|\; A \subseteq [D], |A| = D-k, \deg_Y(\mathbf{x^j}) \leqslant tk \right\}$$

Thus, we have by linearity,

$$\left\{ \pi_{S_1}(\partial_I(C_i)) \;\middle|\; I \in [n]^{2k} \right\} \subseteq$$
$$\operatorname{span}_{\mathbb{F}} \left\{ \pi_{S_1}(Q_A \cdot \mathbf{x^j}) \;\middle|\; |A| = D-k, \deg_Y(\mathbf{x^j}) \leqslant tk \right\}$$

Now, by the definition of π_{S_1}, $\pi_{S_1}(Q_A \cdot \mathbf{x^j}) = 0$ if either $\mathbf{x^j}$ is non-set-multilinear or it is divisible by a variable in $\bigcup_{q \in [k]} X_{p_q}$. Thus, in the expression above, we may range only over $\mathbf{x^j}$ that are set-multilinear and not divisible by any $x \in \bigcup_{q \in [k]} X_{p_q}$. In particular, this implies that

$\deg_Z(\mathbf{x}^{\mathbf{j}}) \leqslant k$ (recall that $Z = \bigcup_{p\in P'} X_p$) and hence $|\mathbf{j}| = \deg_Y(\mathbf{x}^{\mathbf{j}}) + \deg_Z(\mathbf{x}^{\mathbf{j}}) \leqslant tk + k = (t+1)k$. Thus, we get

$$\begin{aligned}&\left\{\pi_{S_1}(\partial_I(C_i)) \;\middle|\; I \in [n]^{2k}\right\} \subseteq \\ &\operatorname{span}_{\mathbb{F}}\left\{\pi_{S_1}(Q_A \cdot \mathbf{x}^{\mathbf{j}}) \;\middle|\; |A| = D-k, \mathbf{x}^{\mathbf{j}} \in \mathcal{M}_X^{sm}, |\mathbf{j}| \leqslant (t+1)k\right\} \end{aligned} \tag{5}$$

where we use $\mathcal{M}_X^{sm}$ to denote the set of all set-multilinear monomials over X.

To analyze the above, decompose Q_A further as

$$Q_A = Q_A^{nsm} + \sum_{B\subseteq[d]} Q_A^B$$

where Q_A^{nsm} is the sum of all the *non*-set-multilinear monomials in Q_A (with the same coefficients) and Q_A^B (for each $B \subseteq [d]$) is a linear-combination of set-multilinear monomials $\mathbf{x}^{\mathbf{i_1}}$ appearing in Q_A such that $\operatorname{MSupp}(\mathbf{x}^{\mathbf{i_1}}) = B$.

Since non-set-multilinear monomials lie in the kernel of π_{S_1} we have for any $\mathbf{x}^{\mathbf{j}} \in \mathcal{M}_X^{sm}$,

$$\begin{aligned}\pi_{S_1}(Q_A \cdot \mathbf{x}^{\mathbf{j}}) &= \pi_{S_1}(Q_A^{nsm} \cdot \mathbf{x}^{\mathbf{j}}) + \sum_{B\subseteq[d]} \pi_{S_1}(Q_A^B \cdot \mathbf{x}^{\mathbf{j}}) \\ &= 0 + \sum_{B\subseteq[d]} \pi_{S_1}(Q_A^B \cdot \mathbf{x}^{\mathbf{j}}) \end{aligned} \tag{6}$$

What follows is a crucial observation: for any $B \subseteq [d]$ and any $\mathbf{x}^{\mathbf{j}} \in \mathcal{M}_X^{sm}$,

$$\pi_{S_1}(Q_A^B \cdot \mathbf{x}^{\mathbf{j}}) = \begin{cases} 0, & \text{if } B \cap \{p_1, \ldots, p_k\} \neq \varnothing, \\ 0, & \text{if } \operatorname{MSupp}(\mathbf{x}^{\mathbf{j}}) \cap \{p_1, \ldots, p_k\} \neq \varnothing, \\ 0, & \text{if } \operatorname{MSupp}(\mathbf{x}^{\mathbf{j}}) \cap B \neq \varnothing, \\ Q_A^B \cdot \mathbf{x}^{\mathbf{j}}, & \text{otherwise.} \end{cases}$$

In particular, along with (6), this implies that for any $\mathbf{x}^{\mathbf{j}} \in \mathcal{M}_X^{sm}$, the polynomial $\pi_{S_1}(Q_A \cdot \mathbf{x}^{\mathbf{j}})$ lies in $\operatorname{span}_{\mathbb{F}}\left\{Q_A^B \cdot \mathbf{x}^{\mathbf{j}} \;\middle|\; B \subseteq [d]\right\}$. Plugging this into (5)

$$\begin{aligned}&\left\{\pi_{S_1}(\partial_I(C_i)) \;\middle|\; I \in [n]^{2k}\right\} \subseteq \\ &\operatorname{span}_{\mathbb{F}}\left\{Q_A^B \cdot \mathbf{x}^{\mathbf{j}} \;\middle|\; |A| = D-k, |\mathbf{j}| \leqslant (t+1)k, B \subseteq [d]\right\}\end{aligned}$$

We are now ready to bound $\mu_{k,\ell}(C_i)$. By linearity once more, we have

$$\begin{aligned}\mathcal{V}_{k,\ell}(C_i) &= \left\{\mathbf{x}^{\mathbf{i}} \cdot \pi_{S_1}(\partial_I(C_i)) \;\middle|\; I \in [n]^{2k}, |\mathbf{i}| \leqslant \ell\right\} \\ &\subseteq \operatorname{span}_{\mathbb{F}}\left\{Q_A^B \cdot \mathbf{x}^{\mathbf{i}+\mathbf{j}} \;\middle|\; |A| = D-k, |\mathbf{j}| \leqslant (t+1)k, B \subseteq [d], |\mathbf{i}| \leqslant \ell\right\} \\ &= \operatorname{span}_{\mathbb{F}}\left\{Q_A^B \cdot \mathbf{x}^{\mathbf{i}} \;\middle|\; |A| = D-k, |\mathbf{i}| \leqslant \ell + (t+1)k, B \subseteq [d]\right\}\end{aligned}$$

Therefore, by the definition of $\mu_{k,\ell}$, we get

$$\begin{aligned}\mu_{k,\ell}(C_i) &= \dim(\mathcal{V}_{k,\ell}(C_i)) \\ &\leqslant \left|\left\{Q_A^B \cdot \mathbf{x}^{\mathbf{i}} \;\middle|\; |A| = D-k, |\mathbf{i}| \leqslant \ell + (t+1)k, B \subseteq [d]\right\}\right| \\ &\leqslant (\#\text{ of choices for } B) \cdot (\#\text{ of choices for } A) \\ &\quad \cdot (\#\text{ of monomials of degee} \leqslant \ell + (t+1)k) \\ &= 2^d \cdot \binom{D}{k} \cdot \binom{N + \ell + (t+1)k}{\ell + (t+1)k}\end{aligned}$$

This finishes the proof of Lemma 7.

5 Lower bounds for $\Sigma\Pi\Sigma\Pi$ homogeneous formulas

In this section, we prove Theorems 1 and 2. The idea of the proof is to show that if $\mathrm{IMM}_{n,d}$ or Det_n has a small $\Sigma\Pi\Sigma\Pi$ homogeneous formula, then there is a restriction $\sigma \in \mathcal{R}$ such that $\mathrm{IMM}_{n,d}|_\sigma$ has a small $\Sigma\Pi^{[D]}\Sigma\Pi^{[t]}_Y$ formula $\pmod{\mathcal{J}}$ (for suitably chosen t and k). We then appeal to Lemma 6 to get the result. We first prove a restriction lemma for $\mathrm{IMM}_{n,d}$.

Lemma 11. *For all large enough $n, d \in \mathbb{N}$, any $D, t, k \geqslant 1$, we have the following. If $\mathrm{IMM}_{n,d}$ has a $\Sigma\Pi^{[D]}\Sigma\Pi$ formula of size $\mathfrak{s} < n^{t/10}$, then there is a restriction $\sigma \in \mathcal{R}$ and a $\Sigma\Pi^{[D]}\Sigma\Pi^{[\lceil t/2 \rceil]}_Y$ formula C' of size at most $\mathfrak{s}$ such that $C' = \mathrm{IMM}_{n,d}|_\sigma \pmod{\mathcal{J}}$. Moreover, if C is also homogeneous, then we can find a homogeneous C' satisfying the above.*

Proof. We show that a random $\sigma \in \mathcal{R}$ will meet our requirements with good probability. Formally, choose $j_1, j_d \in [d]$ and $B = (\phi_p \in S_n : p \in [d] \backslash (P' \cup \{1, d\}))$ each independently and uniformly at random and set $\sigma = \tau_{j_1, j_d, B}$ as defined in Section 3. Note that for $p \in [d] \backslash P'$, each variable $x \in X_p$ is set to 0 with probability $1 - 1/n$; moreover, the restrictions in $X_p, X_{p'}$ for $p \neq p'$ are independent.

Let C_1 be the formula obtained by setting all variables $x \in X$ to $\sigma(x)$ and removing Π-gates at layer 1 which have an input set to 0; clearly, C_1 is a $\Sigma\Pi^{[D]}\Sigma\Pi$ formula that computes $\mathrm{IMM}_{n,d}|_\sigma$. We call a $\sigma \in \mathcal{R}$ *good* if every gate g at layer 1 in C computing a *set-multilinear* monomial such that $\deg_Y(g) > \lceil t/2 \rceil$ has as input some variable that is set to 0 by σ and hence removed from C_1. We claim that σ is good with probability at least $1/2$.

To see this, consider any gate g at layer 1 in C computing a set-multilinear monomial $\mathbf{x^i}$ such that $\deg_Y(g) = |\mathrm{MSupp}(\mathbf{x^i}) \cap ([d] \backslash P')| > \lceil t/2 \rceil$. We can factor $\mathbf{x^i}$ as $(\prod_{p \in \mathrm{MSupp}(\mathbf{x^i}) \cap ([d] \backslash P')} x_p) \cdot \mathbf{x^j}$ for some monomial $\mathbf{x^j}$. Then, g survives in C_1 iff no variable x_p ($p \in \mathrm{MSupp}(\mathbf{x^i}) \cap ([d] \backslash P')$) is set to 0 by σ. Since the probability that each such x_p is not set to 0 is at most $1/n$ and this event is independent for distinct p, the probability that g survives in C_1 is at most $\frac{1}{n^{t/2}}$. Taking a union bound over all such g — of which there are at most $\mathfrak{s}$ many — we see that the probability that any such g survives in C_1 is at most $\mathfrak{s} \cdot \frac{1}{n^{t/2}} \leqslant 1/2$ for large n since $\mathfrak{s} < n^{t/10}$.

Now, fix any good σ and $C_1 = C|_\sigma$ which computes $\mathrm{IMM}_{n,d}|_\sigma$. Let C' denote the formula obtained from C_1 by removing all gates g at layer 1 such that $\deg_Y(g) > \lceil t/2 \rceil$. By our choice of σ, all such gates compute non-set-multilinear monomials in $\mathcal{J}$. Thus, $C' = \mathrm{IMM}_{n,d}|_\sigma \pmod{\mathcal{J}}$ as claimed in the lemma statement. Moreover, it is clear that C' has size at most the size of C which is $\mathfrak{s}$.

Finally, note that C' was obtained from C by removing some of the monomials computed at layer 1 in C. If C is homogeneous, then we can assume w.l.o.g. that all the monomials feeding into a Σ-gate at layer 2 have the same degree. It thus follows that if C was a homogeneous formula, then so is C'. □

We now prove the lower bound for $\mathrm{IMM}_{n,d}$.

of Theorem 1. We first fix the parameters that we will be using. Choose t, k such that $t = \min\{\lfloor \sqrt{d} \rfloor, \lfloor \log n / 5000 \rfloor\}$ and $d/4000 \leqslant kt \leqslant d/2000$. Let C be a homogeneous formula of size $\mathfrak{s}$ computing $\mathrm{IMM}_{n,d}$. Note that since C is homogeneous, it is in particular a $\Sigma\Pi^{[d]}\Sigma\Pi$ formula. If $\mathfrak{s} \geqslant n^{t/10}$, then we have the claimed lower bound and thus we are done.

Otherwise, we can use Lemma 11 and obtain a restriction $\sigma \in \mathcal{R}$ and a *homogeneous* $\Sigma\Pi^{[d]}\Sigma\Pi^{[\lceil t/2 \rceil]}_Y$ formula C' of size at most $\mathfrak{s}$ such that $C' = \mathrm{IMM}_{n,d}|_\sigma \pmod{\mathcal{J}}$. Note that, in particular, the *top fan-in* s of C' is at most $\mathfrak{s}$.

Since C' is $\Sigma\Pi^{[d]}\Sigma\Pi^{[\lceil t/2 \rceil]}_Y$, each input polynomial f to a Π-gate g at layer 3 in C' satisfies $\deg_Y(f) \leqslant \lceil t/2 \rceil$. We now apply the following transformation to C': if any Π-gate g at layer

3 in C' has two inputs f_1, f_2 such that $\deg_Y(f_1), \deg_Y(f_2) < t/4$, then we replace them by a brute force $\Sigma\Pi_Y^{[\lceil t/2 \rceil]}$ formula computing their homogeneous product $f_1 f_2$. This process clearly ensures that the formula remains $\Sigma\Pi^{[d]}\Sigma\Pi_Y^{[\lceil t/2 \rceil]}$ and moreover, does not increase the top fan-in of C'. We repeatedly apply this transformation to C' until we have an equivalent homogeneous formula C'' of top fan-in at most s that moreover has the property that any Π-gate at layer 3 has at most one input f such that $\deg_Y(f) < t/4$. In particular, this last property along with the homogeneity of C'' ensures that any layer 3 Π-gate in C'' has fan-in at most $4d/t + 1 \leqslant 5d/t$. Hence, C'' is a $\Sigma\Pi^{[\lfloor 5d/t \rfloor]}\Sigma\Pi_Y^{[\lceil t/2 \rceil]}$ formula of top fan-in at most s such that $C'' = \mathrm{IMM}_{n,d}|_\sigma \pmod{\mathcal{J}}$.

Lemma 6 tells us that by our choice of k and t and for large enough n, we have

$$\begin{aligned}\mathfrak{s} \geqslant s &\geqslant \frac{1}{4 \cdot 2^d} \cdot \left(\frac{nkt}{5ed}\right)^k \geqslant \frac{1}{4 \cdot 2^d} \cdot \left(\frac{n}{60000}\right)^k \geqslant \frac{n^{d/4500t}}{4 \cdot 2^d} \\ &\geqslant \max\left\{\frac{n^{\Omega(\sqrt{d})}}{4 \cdot 2^d}, 2^{\Omega(d)}\right\}.\end{aligned}$$

Note that the above lower bound is $n^{\Omega(\sqrt{d})}$ when $d < \epsilon \log^2 n$ for a small enough $\epsilon > 0$; for $d = \Omega(\log^2 n)$, the above is $n^{\Omega(\log n)}$. Thus, we have the theorem. □

We now turn to the lower bound for Det_n. We first need a lemma due to Valiant [25]. Given parameters $n_1, d_1 \geqslant 2$, we let $X(n_1, d_1)$ denote the set of variables over which the polynomial IMM_{n_1,d_1} is defined.

Lemma 12. *For any $n_1, d_1 \in \mathbb{N}^+$ and any $n \geqslant n_1 d_1$, there is an $n \times n$ matrix M whose entries are either 0, 1, or variables from $X(n_1, d_1)$ such that $\mathrm{Det}_n(M) = \mathrm{IMM}_{n_1,d_1}$.*

of Theorem 2. For large enough n, we can fix n_1 and $d_1 = \Theta(\log^2 n_1)$ such that $n/2 \leqslant n_1 d_1 \leqslant n$. Set $t = \lfloor \log n_1/25000 \rfloor$ and $k \geqslant 10$ such that $d_1/4000 \leqslant kt \leqslant d_1/2000$.

Assume that C is a homogeneous $\Sigma\Pi\Sigma\Pi$ formula of size $\mathfrak{s}$ for the polynomial $\mathrm{Det}_n(y_{i,j} : i, j \in [n])$. In particular, note that C is a $\Sigma\Pi^{[n]}\Sigma\Pi$ formula. If $\mathfrak{s} \geqslant n_1^{t/10} = n^{\Omega(\log n)}$, then we have the claimed lower bound and we are done. Otherwise, we can use Lemma 12 to transform C into an $\Sigma\Pi^{[n]}\Sigma\Pi$ formula C_1 of size at most $\mathfrak{s}$ for IMM_{n_1,d_1} by substituting each $y_{i,j}$ by $M_{i,j}$ throughout C. Now, we can apply Lemma 11 to C_1 and obtain a restriction $\sigma \in \mathcal{R}$ and a $\Sigma\Pi^{[n]}\Sigma\Pi_Y^{[\lceil t/2 \rceil]}$ formula C' of size at most $\mathfrak{s}$ such that $C' = \mathrm{IMM}_{n_1,d_1}|_\sigma \pmod{\mathcal{J}}$. Note in particular that the top fan-in s of C' is at most $\mathfrak{s}$.

Lemma 6 tells us that for large enough n we have

$$\begin{aligned}s &\geqslant \frac{1}{4 \cdot 2^{d_1}} \cdot \left(\frac{n_1^{1.25}}{en}\right)^k \geqslant \frac{1}{4 \cdot 2^{d_1}} \cdot \left(\frac{n_1^{1.25}}{2en_1d_1}\right)^k \geqslant \frac{n^{k/5}}{4 \cdot 2^{d_1}} \\ &\geqslant \frac{n_1^{d_1/20000t}}{4 \cdot 2^{d_1}} = 2^{\Omega(d_1)} = n_1^{\Omega(\log n_1)} = n^{\Omega(\log n)},\end{aligned}$$

and since $s \leqslant \mathfrak{s}$, we have the theorem. □

6 Discussion

Our work uses an augmentation of the shifted partial measure (namely, shifted projected partials) to show a super-polynomial lower bound for homogeneous depth-4 formulas. It is natural to wonder if one might be able to use some other 'shifted partials inspired' measure(s) to prove

super-polynomial lower bounds for other interesting classes of arithmetic circuits, like homogeneous formulas or multilinear circuits. As mentioned in the introduction, we have been able to improve the quasipolynomial lower bound presented here to an exponential lower bound for an explicit polynomial in VNP. It would be interesting to prove such a lower bound for a polynomial in VP.

References

[1] Manindra Agrawal, Chandan Saha, Ramprasad Saptharishi, and Nitin Saxena. Jacobian hits circuits: hitting-sets, lower bounds for depth-d occur-k formulas & depth-3 transcendence degree-k circuits. In *STOC*, pages 599–614, 2012.

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

[3] Eric Allender, Jia Jiao, Meena Mahajan, and V. Vinay. Non-Commutative Arithmetic Circuits: Depth Reduction and Size Lower Bounds. *Theor. Comput. Sci.*, 209(1-2):47–86, 1998.

[4] 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.

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

[6] Dima Grigoriev and Alexander A. Razborov. Exponential complexity lower bounds for depth 3 arithmetic circuits in algebras of functions over finite fields. In *FOCS*, pages 269–278, 1998.

[7] Ankit Gupta, Pritish Kamath, Neeraj Kayal, and Ramprasad Saptharishi. Approaching the chasm at depth four. In *Proceedings of the Conference on Computational Complexity (CCC)*, 2013.

[8] Ankit Gupta, Pritish Kamath, Neeraj Kayal, and Ramprasad Saptharishi. Arithmetic circuits: A chasm at depth three. *Electronic Colloquium on Computational Complexity (ECCC)*, 20:26, 2013.

[9] Venkatesan Guruswami. Introduction to coding theory, Lecture 2: Gilbert-Varshamov bound. `http://www.cs.cmu.edu/ venkatg/teaching/codingtheory/`, 2010.

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

[11] 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)*, 21:5, 2014.

[12] 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.

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

[14] Mrinal Kumar and Shubhangi Saraf. The limits of depth reduction for arithmetic formulas: It's all about the top fan-in. *Electronic Colloquium on Computational Complexity (ECCC)*, 20:153, 2013.

[15] 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.

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

[17] Noam Nisan. Lower bounds for non-commutative computation (extended abstract). In *STOC*, pages 410–418, 1991.

[18] Noam Nisan and Avi Wigderson. Lower bounds on arithmetic circuits via partial derivatives. *Computational Complexity*, 6(3):217–234, 1997.

[19] Ran Raz. Separation of multilinear circuit and formula size. *Theory of Computing*, 2(1):121–135, 2006.

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

[21] Ran Raz and Amir Yehudayoff. Lower Bounds and Separations for Constant Depth Multilinear Circuits. *Computational Complexity*, 18(2):171–207, 2009.

[22] Amir Shpilka and Amir Yehudayoff. Arithmetic circuits: A survey of recent results and open questions. *Foundations and Trends in Theoretical Computer Science*, 5(3-4):207–388, 2010.

[23] Sven Skyum and Leslie G. Valiant. A Complexity Theory Based on Boolean Algebra. *J. ACM*, 32(2):484–502, 1985.

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

[25] L. G. Valiant. Completeness Classes in Algebra. In *STOC '79: Proceedings of the eleventh annual ACM symposium on Theory of computing*, pages 249–261, New York, NY, USA, 1979. ACM Press.

[26] Leslie G. Valiant, Sven Skyum, S. Berkowitz, and Charles Rackoff. Fast Parallel Computation of Polynomials Using Few Processors. *SIAM J. Comput.*, 12(4):641–644, 1983.

A Lower bounding $\mu_{k,\ell}(F)$

In this section, we prove Lemma 4.

By the definition of $\mu_{k,\ell}$, we have $\mu_{k,\ell}(F) = \dim(\mathcal{V}_{k,\ell}(f))$ where $\mathcal{V}_{k,\ell}(F)$ is given by

$$\begin{aligned}&\text{span}_{\mathbb{F}}\{\mathbf{x}^{\mathbf{i}} \cdot \pi_{S_1}\left(\frac{\partial^k F}{\partial x^{(p_1)}_{i_1,j_1} \dots \partial x^{(p_k)}_{i_k,j_k}}\right) \mid |\mathbf{i}| \leqslant \ell \text{ and } \prod_{q\in[k]} x^{(p_q)}_{i_q,j_q} \in S_2\}\\ &= \text{span}_{\mathbb{F}}\{\mathbf{x}^{\mathbf{i}} \cdot \pi_{S_1}\left(\partial_I F\right) \mid |\mathbf{i}| \leqslant \ell \text{ and } I \in [n]^{2k}\}\end{aligned}$$

First observe that any $\partial_I F$ is a monomial given by $\rho_1\rho_2\dots\rho_{k+1}$, where

$$\rho_1 = \underbrace{\left(x_1^{(1)} \cdot \prod_{1<p<p_1'} x_{1,1}^{(p)}\right)}_{g_1^I} \cdot x_{1,i_1}^{(p_1')} \cdot \underbrace{\left(\prod_{p_1'<p<p_1} x_{i_1,i_1}^{(p)}\right)}_{h_1^I}$$

$$\rho_q = \underbrace{\left(\prod_{p_{q-1}<p<p_q'} x_{j_{q-1},j_{q-1}}^{(p)}\right)}_{g_q^I} \cdot x_{j_{q-1},i_q}^{(p_q')} \cdot \underbrace{\left(\prod_{p_q'<p<p_q} x_{i_q,i_q}^{(p)}\right)}_{h_q^I}$$

$$\rho_{k+1} = \underbrace{\left(\prod_{p_k<p<p_{k+1}'} x_{j_k,j_k}^{(p)}\right)}_{g_{k+1}^I} \cdot x_{j_k,1}^{(p_{k+1}')} \cdot \underbrace{\left(\left(\prod_{p_{k+1}'<p<d} x_{1,1}^{(p)}\right) \cdot x_1^{(d)}\right)}_{h_{k+1}^I}$$

where the second equality holds for $1 < q < k+1$

Due to the above structure of $\partial_I F$ we have the following claim.

Claim 13. $\forall I \in [n]^{2k}$, $\partial_I F \in S_1$.

Claim 13 implies that for all $I \in [n]^{2k}$, $\pi_{S_1}(\partial_I F) = \partial_I F$. Therefore, we get

$$\mathcal{V}_{k,\ell}(F) = \text{span}_{\mathbb{F}}\{\mathbf{x}^{\mathbf{i}} \cdot \partial_I F : |\mathbf{i}| \leqslant \ell \text{ and } I \in [n]^{2k}\}$$

The analysis of the dimension of $\mathcal{V}_{k,\ell}(F)$ is now very similar to the analysis of the dimension of the shifted partial derivative space of F as done in [4].

Let $\mathcal{M} = \{\mathbf{x}^{\mathbf{i}} \cdot \partial_I F : |\mathbf{i}| \leqslant \ell \text{ and } I \in [n]^{2k}\}$. Since $\mathcal{M}$ is a set of *monomials*, the dimension of the span of $\mathcal{M}$ is exactly $|\mathcal{M}|$.

Another way of looking at $\mathcal{M}$ is $\mathcal{M} = \bigcup_{I\in[n]^{2k}} \mathcal{M}_I$, where $\mathcal{M}_I := \{\mathbf{x}^{\mathbf{i}} \mid |\mathbf{i}| \leqslant \ell + d - k \text{ and } \partial_I F \text{ divides } \mathbf{x}^{\mathbf{i}}\}$. Therefore, we have the following claim.

Claim 14. *For F and $\mathcal{M}_I$ ($I \in [n]^{2k}$) as defined above, we have $\dim(\mathcal{V}_{k,\ell}(F)) = |\mathcal{M}|$, where $\mathcal{M} = \bigcup_{I\in[n]^{2k}} \mathcal{M}_I$.*

In what follows, we do not distinguish between multilinear monomials over the variable set X and subsets of X.

Claim 15. *For any $I, I' \in [n]^{2k}$, we have*

$$|\partial_{I'} F \backslash \partial_I F| \geqslant \Delta(I, I') \cdot \left\lfloor \frac{r-1}{2} \right\rfloor$$

where $\Delta(I, I')$ denotes the Hamming distance between I and I'.

Proof. Consider any $I, I' \in [n]^{2k}$. Say $I = (i_1, j_1, \ldots, i_k, j_k)$ and $I' = (i_1', j_1', \ldots, i_k', j_k')$. Then, using the notation from the definition of $\partial_I F$, we have

$$\begin{aligned}
\partial_{I'} F \backslash \partial_I F &\supseteq \dot{\bigcup_{q\in[k]}} (g_{q+1}^{I'} \backslash g_{q+1}^I) \dot{\cup} \dot{\bigcup_{q\in[k]}} (h_q^{I'} \backslash h_q^I) \\
&\supseteq \dot{\bigcup_{q\in[k]: j_q \neq j_q'}} (g_{q+1}^{I'} \backslash g_{q+1}^I) \dot{\cup} \dot{\bigcup_{q\in[k]: i_q \neq i_q'}} (h_q^{I'} \backslash h_q^I).
\end{aligned}$$

where $A \dot\cup B$ denotes the union of disjoint sets A and B.

Now, when $j_q \neq j'_q$, then the monomials g^I_{q+1} and $g^{I'}_{q+1}$ are disjoint and hence $|g^{I'}_{q+1} \backslash g^I_{q+1}| = |g^{I'}_{q+1}| \geqslant \left\lfloor \frac{r-1}{2} \right\rfloor$. Similarly, when $i_q \neq i'_q$, we have $|h^{I'}_q \backslash h^I_q| \geqslant \left\lfloor \frac{r-1}{2} \right\rfloor$.

$$\begin{aligned} |\partial_{I'} F \backslash \partial_I F| &\geqslant \sum_{q \in [k] : j_q \neq j'_q} |g^{I'}_{q+1} \backslash g^I_{q+1}| + \sum_{q \in [k] : i_q \neq i'_q} |h^{I'}_q \backslash h^I_q| \\ &\geqslant \Delta(I, I') \cdot \left\lfloor \frac{r-1}{2} \right\rfloor, \end{aligned}$$

which completes the proof of the claim. □

Claim 16. *For any $I \in [n]^{2k}$, we have $|\mathcal{M}_I| = \binom{N+\ell}{\ell}$.*

Proof. A monomial $\mathbf{x^i} \in \mathcal{M}_I$ iff there is a monomial $\mathbf{x^j}$ such that $\mathbf{j} \leqslant \ell$ and $\mathbf{x^i} = \mathbf{x^j} \cdot \partial_I F$. Thus, $|\mathcal{M}_I|$ is equal to the number of monomials of degree at most ℓ, which is $\binom{N+\ell}{\ell}$. □

Claim 17. *For any $I, I' \in [n]^{2k}$, we have*

$$|\mathcal{M}_I \cap \mathcal{M}_{I'}| = \binom{N + \ell - |(\partial_{I'} F \backslash \partial_I F)|}{\ell - |(\partial_{I'} F \backslash \partial_I F)|}.$$

Proof. Fix any I, I' as above. Any monomial $\mathbf{x^i} \in \mathcal{M}_I \cap \mathcal{M}_{I'}$ may be factored as $\mathbf{x^i} = \mathbf{x^j} \cdot \partial_I F \cdot (\partial_{I'} F \backslash \partial_I F)$. where $j \leqslant \ell + d - k - (d-k) - |(\partial_{I'} F \backslash \partial_I F)| = \ell - |(\partial_{I'} F \backslash \partial_I F)|$.

Thus, $|\mathcal{M}_I \cap \mathcal{M}_{I'}|$ is equal to the number of monomials of degree at most $\ell - |(\partial_{I'} F \backslash \partial_I F)|$, from which the claim follows. □

Claim 18. *For any $k \in \mathbb{N}$ and large enough $n \in \mathbb{N}$, there exists an $\mathcal{S} \subseteq [n]^{2k}$ such that*

- $|\mathcal{S}| = \left\lfloor n^{1.5k} \right\rfloor$,
- *For all distinct $I, I' \in \mathcal{S}$, we have $\Delta(I, I') \geqslant k/4$.*

Proof. We construct the set $\mathcal{S}$ by first greedily choosing vectors which have pairwise Hamming distance at least $k/4$ and then prove that the set thus formed has size $\left\lfloor n^{1.5k} \right\rfloor$. A standard volume argument [9] gives that the set picked greedily as above has size at least $\frac{n^{2k}}{\mathrm{Vol}_n(2k, k/4)}$, where $\mathrm{Vol}_n(2k, k/4)$ stands for the volume of the Hamming ball of radius k for strings of length $2k$ over an alphabet of size n. It is easy to see that $\mathrm{Vol}_n(2k, k/4) = \sum_{i=0}^{k/4} \binom{2k}{i} (n-1)^i$, which is upper bounded by $2\binom{2k}{k/4}(n-1)^{k/4}$. This in turn is at most $n^{k/3}$ for large enough n. Therefore, $|\mathcal{S}|$ is at least $\frac{n^{2k}}{n^{k/3}}$, i.e. $|\mathcal{S}| \geqslant n^{5k/3}$. By choosing a subcollection of the vectors thus chosen, we can ensure that $|\mathcal{S}|$ is exactly $\left\lfloor n^{1.5k} \right\rfloor$. □

Recall that a very similar claim (Claim 10) proved in [4] gave $\mathcal{S} = \left\lfloor \left(\frac{n}{4}\right)^k \right\rfloor$. This size of $\mathcal{S}$ was sufficient for the proof of Lemma 11 in [4]. We will now see that a slightly larger sized $\mathcal{S}$ will be useful for us to prove Lemma 4.

of Lemma 4. Fix $\mathcal{S}$ as guaranteed by Claim 18. By Claim 14, it suffices to lower bound $|\mathcal{M}|$. For this, we use inclusion-exclusion. Since $\mathcal{M} = \bigcup_I \mathcal{M}_I$, we have

$$\begin{aligned} |\mathcal{M}| &\geqslant |\bigcup_{I \in \mathcal{S}} \mathcal{M}_I| \\ &\geqslant \sum_{I \in \mathcal{S}} |\mathcal{M}_I| - \sum_{I \neq I' \in \mathcal{S}} |\mathcal{M}_I \cap \mathcal{M}_{I'}|. \end{aligned} \tag{7}$$

By Claim 16, we know that $|\mathcal{M}_I| = \binom{N+\ell}{\ell}$. By Claims 17 and 15 and our choice of $\mathcal{S}$, we see that for any distinct $I, I' \in \mathcal{S}$, we have

$$|\mathcal{M}_I \cap \mathcal{M}_{I'}| \leqslant \binom{N+\ell-k/4\cdot\lfloor(r-1)/2\rfloor}{\ell-k/4\cdot\lfloor(r-1)/2\rfloor} \leqslant \binom{N+\ell-d/40}{\ell-d/40}$$

where the last inequality follows since $\lfloor(r-1)/2\rfloor \geqslant d/10k$ for $k \leqslant d/20$ (recall that r denotes $\left\lfloor\frac{d}{k+1}\right\rfloor - 1$).

Plugging the above into (7), we obtain

$$|\mathcal{M}| \geqslant |\mathcal{S}| \cdot \binom{N+\ell}{\ell} - |\mathcal{S}|^2 \cdot \binom{N+\ell-d/40}{\ell-d/40}.$$

Since $|\mathcal{S}| = \lfloor n^{1.5k}\rfloor$, the lemma follows.

□