Superpolynomial Lower Bounds for General Homogeneous Depth 4 Arithmetic Circuits*

Mrinal Kumar[1] and Shubhangi Saraf[2,**]

[1] Department of Computer Science, Rutgers University
[2] Department of Computer Science and Department of Mathematics, Rutgers University

Abstract. In this paper, we prove superpolynomial lower bounds for the class of homogeneous depth 4 arithmetic circuits. We give an explicit polynomial in VNP of degree n in n^2 variables such that any homogeneous depth 4 arithmetic circuit computing it must have size $n^{\Omega(\log \log n)}$.

Our results extend the works of Nisan-Wigderson [13] (which showed superpolynomial lower bounds for homogeneous depth 3 circuits), Gupta-Kamath-Kayal-Saptharishi and Kayal-Saha-Saptharishi [4, 7] (which showed superpolynomial lower bounds for homogeneous depth 4 circuits with bounded bottom fan-in), Kumar-Saraf [9] (which showed superpolynomial lower bounds for homogeneous depth 4 circuits with bounded top fan-in) and Raz-Yehudayoff and Fournier-Limaye-Malod-Srinivasan [3,14] (which showed superpolynomial lower bounds for multilinear depth 4 circuits). Several of these results in fact showed exponential lower bounds.

The main ingredient in our proof is a new complexity measure of *bounded support* shifted partial derivatives. This measure allows us to prove exponential lower bounds for homogeneous depth 4 circuits where all the monomials computed at the bottom layer have *bounded support* (but possibly unbounded degree/fan-in), strengthening the results of Gupta et al and Kayal et al [4, 7]. This new lower bound combined with a careful "random restriction" procedure (that transforms general depth 4 homogeneous circuits to depth 4 circuits with bounded support) gives us our final result.

1 Introduction

Proving lower bounds for explicit polynomials is one of the most important open problems in the area of algebraic complexity theory. Valiant [17] defined the classes VP and VNP as the algebraic analog of the classes P and NP, and showed that proving superpolynomial lower bounds for the Permanent would suffice in separating VP from VNP. Despite the amount of attention received by the problem, we still do not know any superpolynomial (or even *quadratic*) lower bounds for general arithmetic circuits. This absence of progress on the general

* The full version of the paper is available on ECCC at `http://eccc.hpi-web.de/report/2013/181/`

** Research supported by NSF grant CCF-1350572

J. Esparza et al. (Eds.): ICALP 2014, Part I, LNCS 8572, pp. 751–762, 2014.

problem has led to a lot of attention on the problem of proving lower bounds for restricted classes of arithmetic circuits. The hope is that an understanding of restricted classes might lead to a better understanding of the nature of the more general problem, and the techniques developed in this process could possibly be adapted to understand general circuits better. Among the many restricted classes of arithmetic circuits that have been studied with this motivation, *bounded depth* circuits have received a lot of attention.

In a striking result, Valiant et al [18] showed that any n variate polynomial of degree $\text{poly}(n)$ which can be computed by a polynomial sized arithmetic circuit of arbitrary depth can also be computed by an arithmetic circuit of depth $O(\log^2 n)$ and size $\text{poly}(n)$. Hence, proving superpolynomial lower bounds for circuits of depth $\log^2 n$ is as hard as proving lower bounds for general arithmetic circuits. In a series of recent works, Agrawal-Vinay [1], Koiran [8] and Tavenas [16] showed that the depth reduction techniques of Valiant et al [18] can in fact be extended much further. They essentially showed that in order to prove superpolynomial lower bounds for general arithmetic circuits, it suffices to prove strong enough lower bounds for just *homogeneous depth 4* circuits. In particular, to separate VNP from VP, it would suffice to focus our attention on proving strong enough lower bounds for homogeneous depth 4 circuits.

The first superpolynomial lower bounds for homogeneous circuits of depth 3 were proved by Nisan and Wigderson [13]. Their main technical tool was the use of the *dimension of partial derivatives* of the underlying polynomials as a complexity measure. For many years thereafter, progress on the question of improved lower bounds stalled. In a recent breakthrough result on this problem, Gupta, Kamath, Kayal and Saptharishi [4] proved the first superpolynomial $(2^{\Omega(\sqrt{n})})$ lower bounds for homogeneous depth 4 circuits when the fan-in of the product gates at the bottom level is bounded (by $\sqrt{n}$). This result was all the more remarkable in light of the results by Koiran [8] and Tavenas [16] which showed that $2^{\omega(\sqrt{n}\log n)}$ lower bounds for this model would suffice in separating VP from VNP. The results of Gupta et al were further improved upon by Kayal Saha and Sapthrashi [7] who showed $2^{\Omega(\sqrt{n}\log n)}$ lower bounds for the model of homogeneous depth 4 circuits when the fan-in of the product gates at the bottom level is bounded (by $\sqrt{n}$). Thus even a slight asymptotic improvement in the exponent of either of these bounds would imply lower bounds for general arithmetic circuits!

The main tool used in both the papers [4] and [7] was the notion of the dimension of *shifted partial derivatives* as a complexity measure, a refinement of the Nisan-Wigderson complexity measure of dimension of partial derivatives.

In spite of all this exciting progress on homogeneous depth 4 circuits with bounded bottom fanin (which suggests that possibly we might be within reach of lower bounds for much more general classes of circuits) these results give almost no non trivial (not even super linear) lower bounds for general homogeneous depth 4 circuits (with no bound on bottom fanin). Indeed the only lower bounds we know for general homogeneous depth 4 circuits are the slightly superlinear lower bounds by Raz using the notion of elusive functions [15].

Thus nontrivial lower bounds for the class of general depth 4 homogeneous circuits seems like a natural and basic question left open by these works, and strong enough lower bounds for this model seems to be an important barrier to overcome before proving lower bounds for more general classes of circuits.

In this direction, building upon the work in [4, 7], Kumar and Saraf [9, 10] proved superpolynomial lower bounds for depth 4 circuits with unbounded bottom fan-in but *bounded top fan-in*. For the case of *multilinear* depth 4 circuits, superpolynomial lower bounds were first proved by Raz and Yehudayoff [14]. These lower bounds were recently improved in a paper by Fournier, Limaye, Malod and Srinivasan [3]. The main technical tool in the work of Fournier et al was the use of the technique of *random restrictions* before using shifted partial derivatives as a complexity measure. By setting a large collection of variables at random to zero, all the product gates with high bottom fan-in got set to zero. Thus the resulting circuit had bounded bottom fanin and then known techniques of shifted partial derivatives could be applied. This idea of random restrictions crucially uses the multilinearity of the circuits, since in multilinear circuits high bottom fanin means *many* distinct variables feeding in to a gate, and thus if a large collection of variables is set at random to zero, then with high probability that gate is also set to zero.

Our Results: In this paper, we prove the first superpolynomial lower bounds for general homogeneous depth 4 circuits with no restriction on the fan-in, either top or bottom. The main ingredient in our proof is a new complexity measure of *bounded support* shifted partial derivatives. This measure allows us to prove exponential lower bounds for homogeneous depth 4 circuits where all the monomials computed at the bottom layer have only few variables (but possibly large degree/fan-in). This exponential lower bound combined with a careful "random restriction" procedure that allows us to transform general depth 4 homogeneous circuits to this form gives us our final result. We now formally state our results.

Our main theorem is stated below.

Theorem 1. *There is an explicit family of homogeneous polynomials of degree n in n^2 variables in* VNP *which requires homogeneous $\Sigma\Pi\Sigma\Pi$ circuits of size $n^{\Omega(\log\log n)}$ to compute it.*

We prove our lower bound for the family of Nisan-Wigderson polynomials NW_d which is based upon the idea of Nisan-Wigderson designs. We give the formal definition in Section 3.

As a first step in the proof of Theorem 1, we prove an exponential lower bound on the top fan-in of any homogeneous $\Sigma\Pi\Sigma\Pi$ circuit where every product gate at the bottom level has at most $O(\log n)$ distinct variables feeding into it. Let homogeneous $\Sigma\Pi\Sigma\Pi^{\{s\}}$ circuits denote the class of homogeneous $\Sigma\Pi\Sigma\Pi$ circuits where every product gate at the bottom level has at most s distinct variables feeding into it (i.e. has support at most s).

Theorem 2. *There exists a constant $\beta > 0$, and an explicit family of homogeneous polynomials of degree n in n^2 variables in* VNP *such that any homogeneous $\Sigma\Pi\Sigma\Pi^{\{\beta\log n\}}$ circuit computing it must have top fan-in at least $2^{\Omega(n)}$.*

Observe that since homogeneous $\Sigma\Pi\Sigma\Pi^{\{s\}}$ circuits are a more general class of circuits than homogeneous $\Sigma\Pi\Sigma\Pi$ circuits with bottom fan-in at most s, our result strengthens the results of of Gupta et al and Kayal et al [4, 7] when $s = O(\log n)$.

We prove Theorem 1 by applying carefully chosen random restrictions to both the polynomial family and to any arbitrary homogeneous $\Sigma\Pi\Sigma\Pi$ circuit and showing that with high probability the circuit simplifies into a homogeneous $\Sigma\Pi\Sigma\Pi$ circuit with bounded bottom support while the polynomial (even after the restriction) is still rich enough for Theorem 2 to hold. Our results hold over every field.

Recent Related Work: Recently, in an independent work, superpolynomial lower bounds for depth 4 homogeneous circuits were also shown by Limaye, Saha and Srinivasan [12]. They proved an $n^{\Omega(\log n)}$ lower bound on the size of homogeneous depth 4 circuits computing the Determinant of an $n \times n$ matrix. They also achieved a similar bound for the Iterated Matrix Multiplication polynomial. Their proof uses a different variation of shifted partial derivatives as their complexity measure- instead of bounding the support of the monomials used in the shift, they use projections to a particular set of randomly chosen monomials after shifting. Their proof doesn't proceed via first proving lower bounds for homogeneous depth 4 circuits with bounded bottom support, and thus the proof of Theorem 2 that we give here is the only proof we know of this result (which also works over all fields - see next paragraph).

In a subsequent independent work, Kayal, Limaye, Saha and Srinivasan [6] showed exponential lower bounds for homogeneous depth 4 circuits over the field of real numbers. This result combines the use of "bounded support shifts" along with the use of *random projections*. This proof does proceed via first proving lower bounds for depth 4 circuits for bounded bottom support, and over the field of real numbers they are able to prove exponential lower bounds for this model as well.

Organization of the Paper: The rest of the paper is organized as follows. In Section 2, we provide a high level overview of the proof. In Section 3, we introduce some notations and preliminary notions used in the paper. In Section 4, we sketch a proof of Theorem 2. In Section 5, we describe the effects of the random restriction procedure on the circuit and the polynomial. In Section 6, we provide a sketch of the proof of Theorem 1. In the absence of sufficient space, we skip some of the details. We refer the interested reader to the full version of the paper on ECCC [10].

2 Proof Overview

Our proof is divided into two parts. In the first part we show a $2^{\Omega(n)}$ lower bound for homogeneous $\Sigma\Pi\Sigma\Pi$ circuits whose *bottom support* is at most $O(\log n)$. To the best of our knowledge, even when the bottom support is 1, none of the earlier lower bound techniques sufficed for showing nontrivial lower bounds for this

model. Thus a new complexity measure was needed. We consider the measure of *bounded support* shifted partial derivatives, a refinement of the measure of shifted partial derivatives used in several recent works [3, 4, 7, 9, 10]. For this measure, we show that the complexity of the NW_d polynomial (an explicit polynomial in VNP) is *high* whereas any subexponential sized homogeneous depth 4 circuit with bounded bottom support has a much smaller complexity measure. Thus for any depth 4 circuit to compute the NW_d polynomial, it must be large – we show that it must have exponential top fan-in. Thus we get an exponential lower bound for bounded bottom support homogeneous $\Sigma\Pi\Sigma\Pi$ circuits. We believe this result might be of independent interest.

In the second part we show how to "reduce" any $\Sigma\Pi\Sigma\Pi$ circuit that is not too large to a $\Sigma\Pi\Sigma\Pi$ circuit with bounded bottom support. This reduction basically follows from a random restriction procedure that sets some of the variables feeding into the circuit to zero. At the same time we ensure that when this random restriction procedure is applied to NW_d, the polynomial does not get affected very much, and still has large complexity.

We could have set variables to zero by picking the variables to set to zero independently at random. The problem with this approach is that we do not know how to analyze the effect of this simple randomized procedure on NW_d[1]. Thus we define a slightly more refined random restriction procedure which keeps the NW_d polynomial hard and at the same time makes the $\Sigma\Pi\Sigma\Pi$ circuit one of bounded bottom support. We remark that it is the choice of these random restrictions that lead to a lower bound of $n^{\Omega(\log\log n)}$ as opposed to $n^{\Omega(\log n)}$.

3 Preliminaries and Notations

Arithmetic Circuits: An arithmetic circuit over a field $\mathbb{F}$ and a set of variables $x_1, x_2, \ldots, x_N$ is an directed acyclic graph whose internal nodes are labelled by the field operations and the leaf nodes are labelled by the variables or field elements. The nodes with fan-out zero are called the output gates and the nodes with fan-in zero are called the leaves. In this paper, we always assume that there is a unique output gate in the circuit. The *size* of the circuit is the number of nodes in the underlying graph and the *depth* of the circuit is the length of the longest path from the root to a leaf. We call a circuit *homogeneous* if the polynomial computed at every node is a homogeneous polynomial. By a $\Sigma\Pi\Sigma\Pi$ circuit or a depth 4 circuit, we mean a circuit of depth 4 with the top layer and the third layer only have sum gates and the second and the bottom layer have only product gates. In this paper, we confine ourselves to working with homogeneous depth 4 circuits. A homogeneous polynomial P of degree n in N variables, which is computed by a homogeneous $\Sigma\Pi\Sigma\Pi$ circuit can be written as

$$P(x_1, x_2, \ldots, x_N) = \sum_{i=1}^{T} \prod_{j=1}^{d_i} Q_{i,j}(x_1, x_2, \ldots, x_N) \tag{1}$$

[1] This strategy was shown to work with some change in parameters and a more careful analysis in [6] and [11].

Here, T is the top fan-in of the circuit. Since the circuit is homogeneous, we know that for every $i \in \{1, 2, 3, \ldots, T\}$, $\sum_{j=1}^{d_i} \deg(Q_{i,j}) = n$. By the support of a monomial α, we refer to the set of variables which have a positive degree in α. In this paper, we also study the class of homogeneous $\Sigma\Pi\Sigma\Pi$ circuits such that for every i, j, every monomial in $Q_{i,j}$ has bounded support. We now formally define this class.

Homogeneous $\Sigma\Pi\Sigma\Pi^{\{s\}}$ Circuits: A homogeneous $\Sigma\Pi\Sigma\Pi$ circuit in Equation 1, is said to be a $\Sigma\Pi\Sigma\Pi^{\{s\}}$ circuit if every product gate at the bottom level has support at most s. Observe that there is no restriction on the bottom fan-in except that implied by the restriction of homogeneity.

Shifted Partial Derivatives: In this paper we use a variant of the notion of *shifted partial derivatives* which was introduced in [5] and has subsequently been the complexity measure used to to prove lower bounds for various restricted classes of depth four circuits and formulas(for example in [3, 4, 7, 9, 10]). For a field $\mathbb{F}$, an N variate polynomial $P \in \mathbb{F}[x_1, \ldots, x_N]$ and a positive integer r, we denote by $\partial^r P$, the set of all partial derivatives of order equal to r of P. For a polynomial P and a monomial γ, we denote by $\partial_\gamma(P)$ the partial derivative of P with respect to γ. We now reproduce the formal definition from [4].

Definition 3 (Order-r ℓ-Shifted Partial Derivatives). *For an N variate polynomial $P \in \mathbb{F}[x_1, x_2, \ldots, x_N]$ and positive integers $r, \ell \geq 0$, the space of order-r ℓ-shifted partial derivatives of P is defined as*

$$\langle \partial^r P \rangle_\ell \stackrel{def}{=} \mathbb{F}\text{-}span\{ \prod_{i \in [N]} {x_i}^{j_i} \cdot g : \sum_{i \in [N]} j_i = \ell, g \in \partial^r P\} \tag{2}$$

In this paper, we introduce the variation of *bounded support* shifted partial derivatives as a complexity measure. The basic difference is that instead of shifting the partial derivatives by all monomials of degree ℓ, we shift the partial derivatives only by only those monomials of degree ℓ which have support(the number of distinct variables which have non-zero degree in the monomial) exactly equal to m. We now formally define the notion of support-m degree-ℓ shifted partial derivatives of order-r of a polynomial, which for the rest of the paper, we refer by (m, ℓ, r)-shifted partial derivatives.

Definition 4 ((m, ℓ, r)-Shifted Partial Derivatives). *For an N variate polynomial $P \in \mathbb{F}[x_1, x_2, \ldots, x_N]$ and positive integers $r, \ell, m \geq 0$, the space of support-m degree-ℓ shifted partial derivatives of order-r of P is defined as*

$$\langle \partial^r P \rangle_{(\ell,m)} \stackrel{def}{=} \mathbb{F}\text{-}span\{\prod_{i \in S} {x_i}^{j_i} \cdot g : S \subseteq [N], |S| = m, \sum_{i \in S} j_i = \ell, j_i \geq 1, g \in \partial^r P\}$$

The following property follows from the definition above.

Lemma 5. *For any two multivariate polynomials P and Q in $\mathbb{F}[x_1, x_2, \ldots, x_N]$ and any positive integers r, ℓ, m, and scalars α and β*

$$\mathsf{Dim}(\langle \partial^r(\alpha P + \beta Q) \rangle_{(\ell,m)}) \leq \mathsf{Dim}(\langle \partial^r P \rangle_{(\ell,m)}) + \mathsf{Dim}(\langle \partial^r Q \rangle_{(\ell,m)})$$

For any linear or affine space V over a field $\mathbb{F}$, we use $\mathsf{Dim}(V)$ to represent the dimension of V over $\mathbb{F}$. We use the dimension of the space $\langle \partial^r P \rangle_{(\ell,m)}$ which we denote by $\mathsf{Dim}(\langle \partial^r P \rangle_{(\ell,m)})$ as the measure of complexity of a polynomial.

Nisan-Wigderson Polynomials: We show our lower bounds for a family of polynomials in VNP which were used for the first time in the context of lower bounds in [7]. The construction is based upon the intuition that over any field, any two distinct low degree polynomials do not agree at too many points. For the rest of this paper, we assume n to be of the form 2^k for some positive integer k. Let $\mathbb{F}_n$ be a field of size n. For the set of $N = n^2$ variables $\{x_{i,j} : i, j \in [n]\}$ and $d < n$, we define the degree n homogeneous polynomial NW_d as

$$NW_d = \sum_{\substack{f(z)\in\mathbb{F}_n[z] \\ deg(f)\leq d-1}} \prod_{i\in[n]} x_{i,f(i)}$$

From the definition, we can observe the following properties of NW_d.

1. The number of monomials in NW_d is exactly n^d.
2. Each of the monomials in NW_d is multilinear.
3. Each monomial corresponds to evaluations of a univariate polynomial of degree at most $d-1$ at all points of $\mathbb{F}_n$. Thus, any two distinct monomials agree in at most $d-1$ variables in their support.

For any $S \subseteq [n]$ and each $f \in \mathbb{F}_n[z]$, we define the monomial $m_f^S = \prod_{i\in S} x_{i,f(i)}$ and $m_f = \prod_{i\in[n]} x_{i,f(i)}$ We also define the set $\mathcal{M}^S$ to represent the set of monomials $\{x_{i_1,j_1} \cdot x_{i_2,j_2} \cdot x_{i_3,j_3} \cdots x_{i_{|S|},j_{|S|}} : i_1 < i_2 \ldots < i_{|S|} \in S \text{ and } \forall t \in [|S|], j_t \in [n]\}$. Clearly, $NW_d = \sum_{\substack{f(z)\in\mathbb{F}_n[z] \\ deg(f)\leq d-1}} m_f$.

Monomial Ordering and Distance: We also use the notion of a monomial being an extension of another as defined below.

Definition 6. *A monomial θ is said to be an extension of a monomial $\tilde{\theta}$, if θ divides $\tilde{\theta}$.*

In this paper, we imagine our variables to be coming from a $n \times n$ matrix $\{x_{i,j}\}_{i,j\in[n]}$. We also consider the following total order on the variables. $x_{i_1,j_1} > x_{i_2,j_2}$ if either $i_1 < i_2$ or $i_1 = i_2$ and $j_1 < j_2$. This total order induces a lexicographic order on the monomials. For a polynomial P, we use the notation $\mathsf{Lead\text{-}Mon}(P)$ to indicate the leading monomial of P under this monomial ordering.

We use the following notion of distance between two monomials which was also used in [2].

Definition 7 (Monomial Distance). *Let m_1 and m_2 be two monomials over a set of variables. Let S_1 and S_2 be the multiset of variables in m_1 and m_2 respectively, then the distance $\Delta(m_1, m_2)$ between m_1 and m_2 is the min$\{|S_1| - |S_1 \cap S_2|, |S_2| - |S_1 \cap S_2|\}$ where the cardinalities are the order of the multisets.*

In this paper, we invoke this definition only for multilinear monomials of the same degree. In this special case, we have the following crucial observation.

Observation 8. *Let α and β be two multilinear monomials of the same degree which are at a distance Δ from each other. If $Supp(\alpha)$ and $Supp(\beta)$ are the supports of α and β respectively, then $|Supp(\alpha)| - |Supp(\alpha) \cap Supp(\beta)| = |Supp(\beta)| - |Supp(\alpha) \cap Supp(\beta)| = \Delta$.*

4 Lower Bounds for $\Sigma\Pi\Sigma\Pi^{\{O(\log n)\}}$ Circuits

In this section, we sketch the outline of the proof of Theorem 2. We refer the interested reader to the full version of the paper [10] for the complete proof. We show an exponential lower bound on the top fan-in for homogeneous $\Sigma\Pi\Sigma\Pi$ circuits such that every product gate at the bottom has a bounded number of variables feeding into it. We use the dimension of the span of (m, ℓ, r)-shifted partial derivatives as the complexity measure. Our lower bound holds for the NW_d polynomial. The proof has two major components. In the first part, we obtain an upper bounded on the complexity of the circuit. Then, we obtain a lower bound on the complexity of the NW_d polynomial. Comparing the two then implies our lower bound. The bound holds for NW_d for any $d = \delta n$, where δ is a constant such that $0 < \delta < 1$.

4.1 Complexity of Homogeneous Depth 4 $\Sigma\Pi\Sigma\Pi^{\{s\}}$ Circuits

Let C be a homogeneous $\Sigma\Pi\Sigma\Pi^{\{s\}}$ circuit computing the NW_d polynomial. We now state an upper bound on the complexity of a product gate in such a circuit. The proof is fairly straightforward, and we refer the reader to [10] for details. The bound on the complexity of the circuit follows from the subadditivity of the complexity measure.

Lemma 9. *Let $Q = \prod_{i=1}^{n} Q_i$ be a product gate at the second layer from the top in a homogeneous $\Sigma\Pi\Sigma\Pi^{\{s\}}$ circuit computing a homogeneous degree n polynomial in N variables. For any positive integers m, r, s, ℓ satisfying $m + rs \leq \frac{N}{2}$ and $m + rs \leq \frac{\ell}{2}$,*

$$\mathsf{Dim}(\langle \partial^r Q \rangle_{(\ell,m)}) \leq poly(nrs) \binom{n+r}{r} \binom{N}{m+rs} \binom{\ell+n-r}{m+rs}$$

For a homogeneous $\Sigma\Pi\Sigma\Pi$ circuit where each of the bottom level product gates is of support at most s, Lemma 9 immediately implies the following upper bound on the complexity of the circuit due to subadditivity from Lemma 5.

Corollary 10. *Let $C = \sum_{j=1}^{T} \prod_{i=1}^{n} Q_{i,j}$ be a a homogeneous $\Sigma\Pi\Sigma\Pi^{\{s\}}$ circuit computing a homogeneous degree n polynomial in N variables. For any m, r, s, ℓ satisfying $m + rs \leq \frac{N}{2}$ and $m + rs \leq \frac{\ell}{2}$,*

$$\mathsf{Dim}(\langle \partial^r C \rangle_{(\ell,m)}) \leq T \times poly(nrs) \binom{n+r}{r} \binom{N}{m+rs} \binom{\ell+n-r-1}{m+rs-1}$$

4.2 Lower Bound on the Complexity of the NW_d Polynomial

We now outline the approach to obtain a lower bound on the complexity of the NW_d polynomial. For this, we first observe that distinct partial derivatives of the NW_d polynomial are *far* from each other in some sense and then show that shifting such partial derivatives gives us a lot of distinct shifted partial derivatives. Recall that we defined the set $\mathcal{M}^S$ to represent the set $\{x_{i_1,j_1} \cdot x_{i_2,j_2} \cdot x_{i_3,j_3} \cdots x_{i_{|S|},j_{|S|}} : i_1 < i_2 \ldots < i_{|S|} \in S \text{ and } \forall t \in [|S|], j_t \in [n]\}$. We start with the following observation.

Lemma 11. *For any positive integer r such that $n - r > d$ and $r < d - 1$, the set $\{\partial_\alpha(NW_d) : \alpha \in \mathcal{M}^{[r]}\}$ consists of $|\mathcal{M}^{[r]}| = n^r$ nonzero distinct polynomials.*

It can be observed that for any $\alpha \neq \beta \in \mathcal{M}^{[r]}$, the leading monomials of $\partial_\alpha(NW_d)$ and $\partial_\beta(NW_d)$ are multilinear monomials of at a distance at least $n-r-d$ from each other. We exploit this structure in order to show that shifting the polynomials in the set $\{\partial_\alpha(NW_d) : \alpha \in \mathcal{M}^{[r]}\}$ by monomials of support m and degree ℓ results in many linearly independent shifted partial derivatives. We crucially use the following simple lemma.

Lemma 12. *Let α and β be two distinct multilinear monomials of equal degree such that the distance between them is Δ. Let S_α and S_β be the set of all monomials obtained by shifting α and β respectively with monomials of degree ℓ and support exactly m over N variables. Then $|S_\alpha \cap S_\beta| \leq \binom{N-\Delta}{m-\Delta}\binom{\ell-1}{m-1}$.*

For any monomial α and positive integers ℓ, m, we denote by $S_{\ell,m}(\alpha)$ the set of all shifts of $\partial_\alpha NW_d$ by monomials of degree ℓ and support m. More formally,

$$S_{\ell,m}(\alpha) = \{\gamma \cdot \partial_\alpha(NW_d) : \gamma = \prod_{i \in U} {x_i}^{j_i}, U \subseteq [N], |U| = m, \sum_{i \in U} j_i = \ell, j_i \geq 1\}$$

also, let

$$LM_{\ell,m}(\alpha) = \{\mathsf{Lead\text{-}Mon}(f) : f \in S_{\ell,m}(\alpha)\}$$

An application of Lemma 12 to the NW_d polynomial gives us the following lemma.

Lemma 13. *For any positive integers r, m and ℓ such that $n - r > d$ and $r < d - 1$, let α and β be two distinct monomials in $\mathcal{M}^{[r]}$. Then $|S_{\ell,m}(\alpha) \cap S_{\ell,m}(\beta)| \leq \binom{N-(n-d-r)}{m-(n-d-r)}\binom{\ell-1}{m-1}$.*

We now obtain a lower bound on the dimension of the span of (m, ℓ, r)-shifted partial derivatives of the NW_d polynomial. For this, we use the following proposition from [4], the proof of which is a simple application of Gaussian elimination.

Proposition 14 ([4]). *For any field $\mathbb{F}$, let $\mathcal{P} \subseteq \mathbb{F}[z]$ be any finite set of polynomials. Then,*

$$\mathsf{Dim}(\mathbb{F}\text{-}span(\mathcal{P})) = |\{\mathsf{Lead\text{-}Mon}(f) : f \in \mathbb{F}\text{-}span(\mathcal{P})\}|$$

Therefore, in order to lower bound $\mathsf{Dim}(\langle \partial^r NW_d \rangle_{(\ell,m)})$, it would suffice to get a lower bound on the size of the set $\bigcup_\alpha LM_{\ell,m}(\alpha)$, where the union is over all monomials α of degree equal to r. To achieve this, we first obtain a lower bound on the size of the set $\bigcup_{\alpha \in \mathcal{M}^{[r]}} LM_{\ell,m}(\alpha)$. The bound is formally given by the lemma below. The proof follows via an application of the principle of inclusion-exclusion. We refer the reader to the full version of this paper [10] for more details.

Lemma 15. *Let $d = \delta n$ for any constant $0 < \delta < 1$. Let ℓ, m, r be positive integers such that $n - r > d$, $r < d - 1$, $m \leq N$, $m = \theta(N)$ and for $\phi = \frac{N}{m}$, r satisfies $r \leq \frac{(n-d)\log\phi \pm O(\phi\frac{(n-d-r)^2}{N})}{\log n + \log\phi}$. Then,*

$$\mathsf{Dim}(\langle \partial^r NW_d \rangle_{(\ell,m)}) \geq 0.5n^r \binom{N}{m}\binom{\ell-1}{m-1}$$

4.3 Top Fan-in Lower Bound

Comparing the bounds in complexity given by Lemma 15 and Corollary 10 gives us a lower bound on the top fan-in of any homogeneous $\Sigma\Pi\Sigma\Pi^{\{\beta \log n\}}$ (for some constant β) that computes the NW_d polynomial, where $d = \delta n$ for some constant δ between 0 and 1. We formally state the result below and refer the reader to [10] for more details.

Theorem 16. *Let $d = \delta n$ for any constant $0 < \delta < 1$. There exists a constant β such that all homogeneous $\Sigma\Pi\Sigma\Pi^{\{\beta \log n\}}$ circuits which compute the NW_d polynomial have top fan-in at least $2^{\Omega(n)}$.*

5 Random Restrictions

The strategy now, is to define an appropriate random restriction procedure and show that with a non-zero probability, all the large support product gates in the bottom level of the circuit get set to zero while the complexity of the polynomial remains large enough. For the lack of space we refer the reader to the full version of the paper [10] for details. The two main statements we need in order to complete the proof are enumerated below. The lemma below summarizes that any restriction $R_\epsilon(NW_d)$ of NW_d obtained as the outcome of our random restriction procedure still remains hard with respect to $\Sigma\Pi\Sigma\Pi^{\{O(\log n)\}}$ circuits.

Lemma 17. *Let $d = \delta n$ for any constant δ such that $0 < \delta < 1$. Then, there exist constants ϵ, β such that any homogeneous $\Sigma\Pi\Sigma\Pi^{\{\beta \log n\}}$ circuit computing the $R_\epsilon(NW_d)$ polynomial for any random restriction R_ϵ has top fan-in is at least $2^{\Omega(n)}$.*

The proof of the lemma is essentially the same as the proof of Theorem 16 and we skip the details to the full version of this paper.

The following lemma summarizes that under our random restriction procedure, all the product gates with large support vanish with a high probability.

Lemma 18 (Random restriction on $\Sigma\Pi\Sigma\Pi$ circuit). *Let $\epsilon > 0$ and $\beta > 0$ be constants. Then there exists $\rho > 0$ such that if C is a $\Sigma\Pi\Sigma\Pi$ circuit of size at most $n^{\rho \log\log n}$, then with probability $> 9/10$, all the monomials computed at the bottom layer which have support at least $\beta \log n$ have some variable set to 0 by R_ϵ.*

6 Lower Bounds for NW_d

In this section, we state our main theorem and give a sketch of the proof. The proof is very similar to proof of Theorem 16 and follows via comparing the complexities of the polynomial and the circuit after random restrictions.

Theorem 19. *Let $d = \delta n$ for any constant δ such that $0 < \delta < 1$. Any homogeneous $\Sigma\Pi\Sigma\Pi$ circuit computing the NW_d must have size at least $n^{\Omega(\log\log n)}$.*

Proof. For every value of δ, such that $0 < \delta < 1$, choose the parameters $\epsilon = \tilde{\epsilon}, \beta = \tilde{\beta}$ such that Lemma 17 is true for $\tilde{d} = \delta n$. Now, let us choose a constant $\rho = \tilde{\rho}$ such that Lemma 18 holds. Now, let C be a homogeneous $\Sigma\Pi\Sigma\Pi$ circuit computing the $NW_{\tilde{d}}$ polynomial. If the number of bottom product gates of C was at least $n^{\tilde{\rho}\log\log n}$, then C has large size and we are done. Else, let us now apply a random restriction R_ϵ to the circuit. By the choice of parameters, Lemma 18 holds and so with probability 0.9 every bottom product gate in C with support larger than $\tilde{\beta}\log n$ is set to zero. After a restriction, the circuit computes $R_{\tilde{\epsilon}}(NW_{\tilde{d}})$. So, now we are in the case when we have a small support homogeneous circuit of depth four computing some random restriction of the $NW_{\tilde{d}}$ polynomial and then, by Lemma 17 above, the top fan-in of $R_{\tilde{\epsilon}}(C)$ must be at least $2^{\Omega(n)}$. Hence, any homogeneous $\Sigma\Pi\Sigma\Pi$ circuit computing $NW_{\tilde{d}}$ must have size at least $n^{\Omega(\log\log n)}$.

References

1. Agrawal, M., Vinay, V.: Arithmetic circuits: A chasm at depth four. In: Proceedings of the 49th Annual FOCS, pp. 67–75 (2008)
2. Chillara, S., Mukhopadhyay, P.: Depth-4 lower bounds, determinantal complexity: A unified approach. CoRR, abs/1308.1640v3 (2013)
3. Fournier, H., Limaye, N., Malod, G., Srinivasan, S.: Lower bounds for depth 4 formulas computing iterated matrix multiplication. In: STOC 2014 (to appear, 2014)
4. Gupta, A., Kamath, P., Kayal, N., Saptharishi, R.: Approaching the chasm at depth four. In: Proceedings of CCC (2013)
5. Kayal, N.: An exponential lower bound for the sum of powers of bounded degree polynomials. ECCC 19, 81 (2012)
6. Kayal, N., Limaye, N., Saha, C., Srinivasan, S.: An exponential lower bound for homogeneous depth four arithmetic formulas. ECCC (2014)
7. Kayal, N., Saha, C., Saptharishi, R.: A super-polynomial lower bound for regular arithmetic formulas. ECCC 20, 91 (2013)

8. Koiran, P.: Arithmetic circuits: The chasm at depth four gets wider. Theoretical Computer Science 448, 56–65 (2012)
9. Kumar, M., Saraf, S.: The limits of depth reduction for arithmetic formulas: It's all about the top fan-in. In: STOC 2014 (to appear, 2014)
10. Kumar, M., Saraf, S.: Superpolynomial lower bounds for general homogeneous depth 4 arithmetic circuits. ECCC (2013)
11. Kumar, M., Saraf, S.: On the power of homogeneous depth 4 arithmetic circuits. ECCC (2014)
12. Limaye, N., Saha, C., Srinivasan, S.: Super-polynomial lower bounds for depth-4 homogeneous arithmetic formulas. In: STOC 2014 (to appear, 2014)
13. Nisan, N., Wigderson, A.: Lower bounds on arithmetic circuits via partial derivatives. In: Proceedings of the 36th Annual FOCS, pp. 16–25 (1995)
14. Raz, R., Yehudayoff, A.: Lower bounds and separations for constant depth multilinear circuits. In: Conference on Computational Complexity, pp. 128–139 (June 2008)
15. Raz, R.: Elusive functions and lower bounds for arithmetic circuits. Theory of Computing 6(1), 135–177 (2010)
16. Tavenas, S.: Improved bounds for reduction to depth 4 and depth 3. In: Chatterjee, K., Sgall, J. (eds.) MFCS 2013. LNCS, vol. 8087, pp. 813–824. Springer, Heidelberg (2013)
17. Valiant, L.: Completeness classes in algebra. In: Proceedings of the 11th Annual STOC, STOC 1979, pp. 249–261. ACM, New York (1979)
18. Valiant, L., Skyum, S., Berkowitz, S., Rackoff, C.: Fast parallel computation of polynomials using few processors. SIAM Journal of Computation 12(4), 641–644 (1983)