2014 IEEE Annual Symposium on Foundations of Computer Science

On the power of homogeneous depth 4 arithmetic circuits

Mrinal Kumar
Department of Computer Science
Rutgers University
Piscataway, New Jersey, USA
mrinal.kumar@rutgers.edu

Shubhangi Saraf
Department of Computer Science and Department of Mathematics
Rutgers University
Piscataway, New Jersey, USA
shubhangi.saraf@rutgers.edu

***Abstract*—We prove exponential lower bounds on the size of homogeneous depth 4 arithmetic circuits computing an explicit polynomial in VP. Our results hold for the *Iterated Matrix Multiplication* polynomial - in particular we show that any homogeneous depth 4 circuit computing the $(1,1)$ entry in the product of n generic matrices of dimension $n^{O(1)}$ must have size $n^{\Omega(\sqrt{n})}$.**

Our results strengthen previous works in two significant ways.

1) **Our lower bounds hold for a polynomial in VP. Prior to our work, Kayal et al [KLSSa] proved an exponential lower bound for homogeneous depth 4 circuits (over fields of characteristic zero) computing a poly in VNP. The best known lower bounds for a depth 4 homogeneous circuit computing a poly in VP was the bound of $n^{\Omega(\log n)}$ by [KLSSb], [KLSSa].**
   Our exponential lower bounds also give the first exponential separation between general arithmetic circuits and homogeneous depth 4 arithmetic circuits. In particular they imply that the depth reduction results of Koiran [Koi12] and Tavenas [Tav13] are tight even for reductions to general homogeneous depth 4 circuits (without the restriction of bounded bottom fanin).
2) **Our lower bound holds over all fields. The lower bound of [KLSSa] worked only over fields of characteristic zero. Prior to our work, the best lower bound for homogeneous depth 4 circuits over fields of positive characteristic was $n^{\Omega(\log n)}$ [KLSSb], [KLSSa].**

***Keywords*-Lower bounds; arithmetic circuits; depth reduction**

I. Introduction

In a seminal work [Val79], Valiant defined the classes VP and VNP as the algebraic analogs of the classes P and NP. The problem of separating VNP from VP has since been one of the most important open problems in algebraic complexity theory. Although the problem has received a great deal of attention in the following years, the best lower bounds known for general arithmetic circuits are barely super linear [Str73], [BS83]. The absence of progress on the general problem has led to much attention being devoted to proving lower bounds for *restricted classes* of arithmetic circuits. Arithmetic circuits of small depth are one such class that has been intensively studied.

Depth Reduction:: Following a long line of structural results by Valiant et al [VSBR83], Agrawal-Vinay [AV08], Koiran [Koi12] and Tavenas [Tav13], it is known that in order to separate VNP form VP, it would suffice to prove strong enough ($n^{\omega(\sqrt{n})}$) lower bounds for just *homogeneous depth 4 circuits* computing an explicit polynomial of degree n in $n^{O(1)}$ variables.

Lower bounds for homogeneous bounded depth circuits:: In an extremely influential work, Nisan and Wigderson [NW95] proved the first super-polynomial (and in fact exponential) lower bound for the class of homogeneous depth 3 circuits using *dimension of the space of partial derivatives* as a measure of complexity of a polyomial. For several years thereafter, there were no improved lower bounds - even for the case of depth 4 homogeneous circuits, the best lower bounds were just mildly super-linear [Raz10]. This seemed surprising until the depth reduction results of Agrawal-Vinay [AV08] and later Koiran [Koi12] and Tavenas [Tav13], which demontrated that in some sense, homogeneous depth 4 circuits *capture* the inherent complexity of general arithmetic circuits.

In a breakthrough result in 2012, Gupta et al showed a lower bound of $2^{\Omega(\sqrt{n})}$ for homogeneous depth four circuit, with bottom fan-in at most $\sqrt{n}$ (we denote this class by $\Sigma\Pi\Sigma\Pi^{[\sqrt{n}]}$) computing a polynomial of degree n in $n^{O(1)}$ variables. This was later improved to $2^{\Omega(\sqrt{n}\log n)}$ in a follow up work of Kayal, Saha, Saptharishi [KSS]. These results were all the more remarkable in the light of the results of Koiran [Koi12] and Tavenas [Tav13] who had in fact showed that $2^{\omega(\sqrt{n}\log n)}$ lower bounds even for homogeneous $\Sigma\Pi\Sigma\Pi^{[\sqrt{n}]}$ circuits would suffice to separate VP from VNP. Thus, any asymptotic improvement in the exponent, in either the upper bound on depth reduction or the lower bound of [KSS] would separate VNP from VP. Both papers [GKKSa], [KSS] used 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.

The most tantalizing questions left open by these works was to improve either the depth reduction or the lower bounds. In [FLMS], the lower bounds of [KSS] were strengthened by showing that they also held for a polynomial

0272-5428/14 $31.00 © 2014 IEEE
DOI 10.1109/FOCS.2014.46

in VP. These were further extended in [KSa], where the same exponential ($n^{\Omega(\sqrt{n})}$) lower bounds were also shown to hold for very simple polynomial sized formulas of just depth 4 (if one requires them to be computed by homogeneous $\Sigma\Pi\Sigma\Pi^{[\sqrt{n}]}$ circuits). On one hand, these results give us extremely strong lower bounds for an interesting class of depth 4 homogeneous circuits. On the other hand, since these lower bounds also hold for polynomials in VP and for homogeneous formulas [FLMS], [KSa], it follows that the depth reduction results of Koiran [Koi12] and Tavenas [Tav13] to the class of homogeneous $\Sigma\Pi\Sigma\Pi^{[\sqrt{n}]}$ circuits are tight and cannot be improved even for homoegeneous formulas.

Although these results represent a lot of exciting progress on the problem of proving lower bounds for homogeneous $\Sigma\Pi\Sigma\Pi^{[\sqrt{n}]}$ circuits, and these results seemed possibly to be on the brink of proving lower bounds for general arithmetic circuits, they still seemed to give almost no nontrivial results for general homogeneous depth 4 circuits with no bound on bottom fanin (homogeneous $\Sigma\Pi\Sigma\Pi$ circuits). Moreover, it was shown in [KSa] that general homogeneous $\Sigma\Pi\Sigma\Pi$ circuits are exponentially more powerful than homogeneous $\Sigma\Pi\Sigma\Pi^{[\sqrt{n}]}$ circuits[1]. Till very recently, the only lower bounds we knew for general homogeneous depth 4 circuits were the slightly super-linear lower bounds by Raz using the notion of elusive functions [Raz10] (these worked even for non-homogeneous circuits).

Lower bounds for general homogeneous depth 4 circuits:: Recently, the first super-polynomial lower bounds for general homogeneous depth 4 ($\Sigma\Pi\Sigma\Pi$) circuits were proved independently by the authors of this paper [KSb] who showed a lower bound of $n^{\Omega(\log\log n)}$ for a polynomial in VNP and Limaye, Saha and Srinivasan [KLSSb], who showed a lower bound of $n^{\Omega(\log n)}$ for a polynomial in VP. Subsequently, Kayal, Limaye, Saha and Srinivasan greatly improved these lower bounds to obtain exponential ($2^{\Omega(\sqrt{n}\log n)}$) lower bounds for a polynomial in VNP (over fields of characteristic zero). Notice that this result also extends the results of [GKKSa] and [KSS] who proved similar exponential lower bounds for the more restricted class of homogeneous $\Sigma\Pi\Sigma\Pi^{[\sqrt{n}]}$ circuits. The result by [KLSSa] shows the same lower bound without the restriction of bottom fanin. Again, any asymptotic improvement of this lower bound in the exponent would separate VP from VNP.

This class of results represents an important step forward, since homogeneous depth 4 circuits seem a much more natural class of circuits than homogeneous depth 4 circuits with bounded bottom fanin. The results of the current paper build upon and strengthen the results of Kayal et al [KLSSa]. Before we describe our results we first highlight some important questions left open by [KLSSa] and place them in the context of several of the other recent results in this area.

- **Dependence on the field:** Several of the major results on depth reduction and lower bounds have heavily depended on the underlying field one is working over. For instance, in a beautiful result [GKKSb], it was shown that if one is working over the field of real numbers, one can get surprising depth reduction of general circuits to just *depth 3 circuits*[2]! We know that such a depth reduction is not possible over small finite fields. Thus at least for depth 3 circuits, we know that there is a vast difference between the computational power of circuits for different fields.
  The lower bounds of [KLSSa] work only over fields of characteristic zero. This is because in order to bound the complexity of the polynomial being computed, the proof reduces the question to lower bounding the rank of a certain matrix. This computation ends up being highly nontrivial and is done by using bounds on eigenvalues. However a similar analysis does not go through for other fields. In particular it was an open question if working over characteristic zero was *necessary* in order to prove the lower bounds.
- **Explicitness of the hard polynomial:** The result of [KLSSa] only proved a lower bound for a polynomial in VNP. It is conceivable/likely that much more should be true, that even polynomials in VP should not be computable by depth 4 homogeneous circuits. The best lower bound known for homogeneous depth 4 circuits computing a poly in VP is the lower bound of $n^{\Omega(\log n)}$ by [KLSSb], [KLSSa]. Recall that when one introduces the restriction on bounded bottom fanin, then stronger exponential lower bounds are indeed known [FLMS], [KSa]. This fact is also related to the next bullet point below.
- **Tightness of depth reduction:** The result of [FLMS] (which showed an explicit polynomial of degree n in $n^{O(1)}$ variables in VP requiring an $n^{\Omega(\sqrt{n})}$ sized homogeneous $\Sigma\Pi\Sigma\Pi^{[\sqrt{n}]}$ to compute it), in particular showed the the depth reduction results of Koiran [Koi12] and Tavenas [Tav13] (showing that every polynomial of degree n in $n^{O(1)}$ variables in VP can be computed by an $n^{O(\sqrt{n})}$ sized homogeneous $\Sigma\Pi\Sigma\Pi^{[\sqrt{n}]}$ circuit) are tight. Given the new lower bounds for the more natural class of depth 4 homogeneous circuits (with no restriction on bottom fanin), and especially the exponential lower bounds of [KLSSa], the most obvious question that arises is the following: If one relaxes away the requirement of bounded bottom fanin, i.e. all one requires is to reduce to the class of general depth 4 homogeneous circuits, can one improve upon the upper bounds obtained by

[1] It was demonstrated that even very simple homogeneous $\Sigma\Pi\Sigma\Pi$ circuits of polynomial size might need $n^{\Omega(\sqrt{n})}$ sized homogeneous $\Sigma\Pi\Sigma\Pi^{[\sqrt{n}]}$ circuits to compute the same polynomial.

[2] albeit with loss of homogeneity.

Koiran and Tavenas? If we could do this over the reals/complex numbers, then given the [KLSSa] result, this would also suffice in separating VP from VNP!

- **Shifted partial derivatives and variants:** The results of [KSb], [KLSSb], [KLSSa] all use variants of the method of shifted partial derivates to obtain the lower bounds. All 3 works use different variants and they are all able to give nontrivial results. This suggests that we do not really fully understand the potential of these methods, and perhaps they can be used to give even much stronger lower bounds for richer classes of circuits.

A. Our results

In this paper, we show a lower bound of $2^{\Omega(\sqrt{n}\log n)}$ on the size of homogeneous depth 4 circuits computing a polynomial in VP. We first give a new, more combinatorial proof of the $2^{\Omega(\sqrt{n}\log n)}$ lower bound for a polynomial in VNP, which holds over all fields. This result is much simpler to prove than our result for a polynomial in VP and thus we prove it first. This will also enable us to develop methods and tools for the more intricate analysis of the lower bounds for VP.

Theorem I.1. *Let $\mathbb{F}$ be any field. There exists an explicit family of polynomials (over $\mathbb{F}$) of degree n and in $N = n^{O(1)}$ variables in* VNP*, such that any homogeneous $\Sigma\Pi\Sigma\Pi$ circuit computing it has size at least $n^{\Omega(\sqrt{n})}$.*

The lower bound in Theorem I.1 is shown for a family of polynomials (denoted by $NW_{n,D}$) whose construction is based on the idea of Nisan-Wigderson designs . These are the same polynomials for which [KLSSa] show their lower bounds. We give a formal definition in Section III. The combinatorial nature of our proof allows us to prove our results over all fields. The combinatorial nature of the proof also gives us much more flexibility and this is what enables the proof of our lower bounds for a polynomial in VP. Though our lower bound for the polynomial in VP is at a high level similar to the VNP lower bound, the analysis is much more delicate and the choice of parameters ends up being quite subtle. We will elaborate more on this in the proof outline given in Section II.

Theorem I.2 (Main Theorem)**.** *Let $\mathbb{F}$ be any field. There exists an explicit family of polynomials (over $\mathbb{F}$) of degree n and in $N = n^{O(1)}$ variables in* VP*, such that any homogeneous $\Sigma\Pi\Sigma\Pi$ circuit computing it has size at least $n^{\Omega(\sqrt{n})}$.*

As an immediate corollary of the result above, we conclude that the depth reduction results of Koiran [Koi12] and Tavenas [Tav13] are tight even when one wants to depth reduce to the class of general homogeneous depth 4 circuits.

Corollary I.3 (Depth reduction is tight)**.** *There exists a polynomial in* VP *of degree n in $N = n^{O(1)}$ variables such that any homogeneous $\Sigma\Pi\Sigma\Pi$ circuit computing it has size at least $n^{\Omega(\sqrt{n})}$. In other words, the upper bound in the depth reduction of Tavenas [Tav13] is tight, even when the bottom fan-in is unbounded.*

The polynomial in Theorem I.2 is the *Iterated Matrix Multiplication* ($IMM_{\tilde{n},n}$) polynomial. From the fact that the determinant polynomial is complete for the class VQP [Val79], we obtain the first exponential lower bounds for the polynomial Det_n (which is the determinant of an $n \times n$ generic matrix) computed by a homogeneous $\Sigma\Pi\Sigma\Pi$ circuit.

Corollary I.4. *There exists a constant $\epsilon > 0$ such that any homogeneous $\Sigma\Pi\Sigma\Pi$ circuit computing the polynomial Det_n has size at least $2^{\Omega(n^{\epsilon})}$.*

We have not optimized the value of ϵ in the statement above, but our proof gives a value of $\epsilon > 1/22$.

B. Organisation of the paper

In Section II, we provide a broad overview of the proofs of Theorem I.1 and Theorem I.2. In Section III, we define some preliminary notions and set up some notations used in the rest of the paper. We state an upper bound on the dimension of the projected shifted partial derivatives of a homogeneous depth 4 circuit of bounded bottom support in Section IV. We lay down our strategy for obtaining a lower bound on the complexity of the polynomials of interest in Section V. Finally in Sections VI, we give an outline of the proof of Theorem I.1. For the lack of space, we have omitted many of the details from the proofs and the proof of Theorem I.2, which can be found in the full version of the paper [KS14].

II. Proof Overview

Let C be a homogeneous $\Sigma\Pi\Sigma\Pi$ circuit computing the polynomial P (either $NW_{n,D}$ or $IMM_{\tilde{n},n}$). The broad outline of the proof of lower bound on the size of C is as follows.

1) If C is *large* ($\geq n^{\epsilon\sqrt{n}}$) to start with, we have nothing to prove. Else, the size of C is small ($< n^{\epsilon\sqrt{n}}$).
2) We choose a random subset V of the variables from some carefully defined distribution $\mathcal{D}$, and then restrict P and C to be the resulting polynomial and circuit after setting the variables not in V to zero. We will let $C|_V$ and $P|_V$ be the resulting circuit and polynomial. Since C computed P, thus $C|_V$ still computes $P|_V$. This choice of distribution $\mathcal{D}$ has to be very carefully designed in order to enable the rest of the proof to go through. When $P = NW_{n,D}$, V will be a random subset of variables which is chosen by picking each variable independently with a certain probability. In the case that $P = IMM_{\tilde{n},n}$, our distribution is much more carefully designed.

3) We show that with a very high probability over the choice of $V \leftarrow \mathcal{D}$, no product gate in the bottom level of $C|_V$ has large support. Thus $C|_V$ is a homogeneous $\Sigma\Pi\Sigma\Pi^{\{\sqrt{n}\}}$ circuit (this is the class of $\Sigma\Pi\Sigma\Pi$ circuits where every product gate at the bottom layer has only $\sqrt{n}$ distinct variables feeding into it, and we formally define this class in Section III).
4) For any homogeneous $\Sigma\Pi\Sigma\Pi^{\{\sqrt{n}\}}$ circuit, we obtain a good estimate on the upper bound on its complexity $\Phi_{\mathcal{M},m}(C|_V)$ (this is the complexity measure of projected shifted partial derivatives that we use, and we define it formally in Section III) in terms of its size. This step is very similar to that in [KLSSa], and is fairly straightforward.
5) We show that with a reasonably high probability over $V \leftarrow \mathcal{D}$, the complexity of $P|_V$ remains large. This step is the most technical and novel part of the proof. Unlike the proof of the earlier exponential bound by [KLSSa], our proof is completely combinatorial. We lower bound the complexity measure $\Phi_{\mathcal{M},m}(P|_V)$ by counting the number of distinct *leading monomials* that can arise after differentiating, shifting and projecting. This calculation turns out to be quite challenging. We first define three related quantities T_1, T_2 and T_3 and show that $T_1 - T_2 - T_3$ is a lower bound on $\Phi_{\mathcal{M},m}(P|_V)$. We elaborate on what these quantities are in Section V. These quantities are easier to compute when $P = NW_{n,D}$, and we are able to show that $\mathbb{E}_{V \leftarrow \mathcal{D}}[T_1 - T_2 - T_3]$ is large. Using variance bounds then lets us conclude that $\Phi_{\mathcal{M},m}(P|_V)$ is large with high probability. When $P = IMM_{\tilde{n},n}$ however, all we are able to show is that $T_2 + T_3$ is not too much larger than T_1 in expected value (it will still be exponentially larger). We then use some sampling arguments to handle this and deduce anyway that $\Phi_{\mathcal{M},m}(P|_V)$ is large. We refer the interested reader to the full version of this paper [KS14] for details.
6) Then, we argue that both the events in the above two items happen simultaneously with non-zero probability. Now, comparing the complexities $P|_V$ and $C|_V$, we deduce that the size of $C|_V$ and hence C must be large.

At a high level, the proof uses several ingredients from [KSb] and [KLSSa]. We remark that in [KSb], the complexity measure and the notion of random restrictions used is very different from this work. Compared to [KLSSa], our strategy for proving a lower bound on the complexity of the polynomial is much more combinatorial and based on elementary ideas. This essentially ensures that our proof works over all fields, as opposed to fields of characterstic zero, as needed in [KLSSa].

III. Preliminaries

Arithmetic Circuits: An arithmetic circuit over a field $\mathbb{F}$ and a set of variables $x_1, x_2, \ldots, x_N$ is a directed acyclic graph with internal nodes labelled by the field operations and the leaf nodes labelled by input variables or field elements. By the *size* of the circuit, we mean the total number of nodes in the underlying graph and by the *depth* of the circuit, we mean the length of the longest path from the output node to a leaf node. A circuit is said to be *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. 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

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

Here, T is the top fan-in of the circuit. Since the circuit is homogeneous, therefore, for every $i \in \{1, 2, 3, \ldots, T\}$,

$$\sum_{j=i}^{d_i} \deg(Q_{i,j}) = n$$

Support of a polynomial: By the support of a polynomial P, denoted by $\mathrm{Supp}(P)$, we mean the set of monomials which have a non zero coefficient in P. When we consider this set, we will ignore the information in the coefficients of the monomials and just treat them to be 1. We will also use the notion of the support of a monomial α defined as the subset of variables which have degree at least 1 in α. We will follow the notation that when we invoke the function Supp for a monomial, we mean the support in the latter sense. When we invoke it for a polynomial, we mean it in the former sense.

For any monomial α and a set of polynomials $\mathcal{S}$, we define the set $\alpha \cdot \mathcal{S} = \{\alpha\beta : \beta \in \{\mathcal{S}\}\}$. For two monomials α and β, we say that α is disjoint from β if the supports of α and β are disjoint.

Multilinear projections of a polynomial: For any monomial α, we define $\sigma(\alpha)$ to be α if α is multilinear and define it to be 0 otherwise. The map can be then extended by linearity to all polynomials and sets of polynomials.

Homogeneous $\Sigma\Pi\Sigma\Pi^{\{s\}}$ Circuits: A homogeneous $\Sigma\Pi\Sigma\Pi$ circuit as 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 (i.e. each monomial in each Q_{ij} has at most s distinct variables feeding into it). Observe that there is no restriction on the bottom fan-in except that implied by the restriction of homogeneity.

Restriction of homogeneous $\Sigma\Pi\Sigma\Pi$ circuit $C|_V$: For a homoegeneous $\Sigma\Pi\Sigma\Pi^{\{s\}}$ circuit C in variables $v_1, v_2, \ldots, v_N$, and a subset of variables $V \subset \{v_1, v_2, \ldots, v_N\}$, we define $C|_V$ to be the new homogeneous $\Sigma\Pi\Sigma\Pi$ circuit obtained after setting the variables outside V to zero. Equivalently we can think of this as the circuit obtained after removing all multiplication gates at the bottom layer which have a variable not in V that feeds into it.

The complexity measure:

The notion of *shifted partial derivatives* was introduced in [Kay12] and was subsequently used as a complexity measure in proving several recent lower bound results [FLMS], [GKKSa], [KSS], [KSb], [KSa]. In this paper, we use a variant of the method which first introduced in [KLSSa].

For a polynomial P and a monomial γ, we denote by $\partial_\gamma(P)$ the partial derivative of P with respect to γ. For every polynomial P and a set of monomials $\mathcal{M}$, we define $\partial_{\mathcal{M}}(P)$ to be the set of partial derivatives of P with respect to monomials in $\mathcal{M}$. We now define the space of $(\mathcal{M}, m)$-projected shifted partial derivatives of a polynomial P below.

Definition III.1 ($(\mathcal{M}, m)$-projected shifted partial derivatives)**.** *For an N variate polynomial $P \in \mathbb{F}[x_1, x_2, \ldots, x_N]$, set of monomials $\mathcal{M}$ and a positive integer $m \geq 0$, the space of $(\mathcal{M}, m)$-projected shifted partial derivatives of P is defined as*

$$\begin{aligned}\langle \partial_{\mathcal{M}}(P) \rangle_m \stackrel{def}{=} \mathbb{F}\text{-}span\{\sigma(\prod_{i \in S} x_i \cdot g) \\ : g \in \partial_{\mathcal{M}}(P), S \subseteq [N], |S| = m\}\end{aligned} \tag{2}$$

In this paper, we carefully choose a set of monomials $\mathcal{M}$ and a parameter m and use the quantity $\Phi_{\mathcal{M},m}(P)$ defined as

$$\Phi_{\mathcal{M},m}(P) = \mathsf{Dim}(\langle \partial_{\mathcal{M}}(P) \rangle_m)$$

as a measure of complexity of the polynomial P.

We will now elaborate on this definition of the measure in words - we look at the space of $(\mathcal{M}, m)$-projected shifted partial derivatives as the space of polynomials obtained at the end of the following steps, starting with the polynomial P.

1) We fix a set of monomials $\mathcal{M}$ and a parameter m.
2) We take partial derivatives of P with every monomial in $\mathcal{M}$, to obtain the set $\partial_{\mathcal{M}}(P)$.
3) We obtain the set of shifted partial derivatives of P by taking the product of every polynomial in $\partial_{\mathcal{M}}(P)$ with every monomial of degree m. In this paper, we will often be working with restrictions of polynomial P obtained by setting some of the input variables to zero. Even for such restrictions, we consider product of the derivatives by all multilinear monomials of degree m over the complete set of input variables $\{x_1, x_2, \ldots, x_N\}$.
4) Then, we consider each polynomial in the set defined in the item above and project it to the polynomial composed of only the multilinear monomials in its support. The span of this set over $\mathbb{F}$ is defined to be $\langle \partial_{\mathcal{M}}(P) \rangle_m$.
5) We define the complexity of the polynomial $\Phi_{\mathcal{M},m}(P)$ to be the dimension of $\langle \partial_{\mathcal{M}}(P) \rangle_m$ over $\mathbb{F}$.

It follows easily from the definitions that the complexity measure is subadditive. We formalize this in the lemma below.

Lemma III.2 (Sub-additivity)**.** *Let P and Q be any two multivariate polynomials in $\mathbb{F}[x_1, x_2, \ldots, x_N]$ any set of monomials. Let $\mathcal{M}$ be any set of monomials and m be any positive integer. Then, for all scalars α and β*

$$\Phi_{\mathcal{M},m}(\alpha \cdot P + \beta \cdot Q) \leq \Phi_{\mathcal{M},m}(P) + \Phi_{\mathcal{M},m}(Q)$$

$P|_V$ and $\Phi_{\mathcal{M},m}(P|_V)$: For a polynomial P and a subset of its variables V, we define $P|_V$ to be the polynomial obtained after setting variables not in V to zero (i.e. removing all monomials containing a variable not in V in its support). When we consider $\Phi_{\mathcal{M},m}(P|_V)$, we will be computing the complexity of the new polynomial with respect to the original set of variables, not just the variables in V. I.e. we set the variables outside V to zero only in order to compute $P|_V$. Once we get this new polynomial, we do not think of the variables outside V to be set to zero when computing $\Phi_{\mathcal{M},m}(P|_V)$.

Nisan-Wigderson Polynomials: We will now define the family of polynomials $NW_{n,D}$ in VNP which were used for the first time in the context of lower bounds in [KSS]. The key motivation for this definition is that over any finite field, any two distinct low degree polynomials do not agree at too many points, and hence we use this property to construct a polynomial with monomials that have large distance. Let $\mathbb{F}_n$ be a finite field of size n^3 and let F_{n^2} be its quadratic extension. For the set of $N = n^3$ variables $\{x_{i,j} : i \in [n], j \in [n^2]\}$ and $D < n$, we define the degree n homogeneous polynomial $NW_{n,D}$ as

$$NW_{n,D} = \sum_{\substack{f(z) \in \mathbb{F}_{n^2}[z] \\ deg(f) \leq D-1}} \prod_{i \in [n]} x_{i,f(i)}$$

From the definition, we can observe the following properties of $NW_{n,D}$.

1) The number of monomials in $NW_{n,D}$ is exactly n^{2D}.
2) Each of the monomials in $NW_{n,D}$ 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.

[3]We are assuming for simplicity that n is a prime power, but the definitions can be easily adapted for when n is not.

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

Definition III.3. *A monomial θ is said to be an extension of a monomial $\tilde{\theta}$, if θ divides $\tilde{\theta}$.*

We will 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 will use the following notion of distance between two monomials which was also used in [CM13].

Definition III.4 (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 III.5. *Let α and β be two multilinear monomials of the same degree which are at a distance Δ from each other. If Supp(α) and Supp(β) are the supports of α and β respectively, then*

$$\begin{aligned} |\textit{Supp}(\alpha)| - |\textit{Supp}(\alpha) \cap \textit{Supp}(\beta)| = \\ |\textit{Supp}(\beta)| - |\textit{Supp}(\alpha) \cap \textit{Supp}(\beta)| = \Delta \end{aligned} \tag{3}$$

For any two multilinear monomials α and β of equal degree, we say that α and β have agreement t if $|\text{Supp}(\alpha) \cap \text{Supp}(\beta)| = t$. When $t = 0$, we say that α and β are disjoint.

Approximations: We will repeatedly refer to the following lemma to approximate expressions during our calculations.

Lemma III.6 ([GKKSa])**.** *Let $a(n), f(n), g(n) : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ be integer valued functions such that $(f + g) = o(a)$. Then,*

$$\log \frac{(a+f)!}{(a-g)!} = (f+g)\log a \pm O\left(\frac{(f+g)^2}{a}\right)$$

In this paper, we invoke Lemma III.6 only in situations where $(f + g)^2$ will be $O(a)$. In this case, the error term will be bounded by an absolute constant. Hence, up to multiplication by constants, $\frac{(a+f)!}{(a-g)!} = a^{(f+g)}$. We will use the symbol $\approx$ to indicate equality up to multiplication by constants.

Probability lemma: We will now state a simple lemma which we crucially use in our proof.

Lemma III.7. *Let X be a random variable sampled from a distribution $\mathcal{R}$ supported on the set R. Let f and g be functions from R to the set of positive real numbers, such that the following are true:*

- *For each $x \in R$, $f(x) \leq g(x)$*
- $\mathbb{E}_{X \leftarrow \mathcal{R}}[f(X)] \geq 0.5 \cdot \mathbb{E}_{X \leftarrow \mathcal{R}}[g(X)]$
- $Pr_{X \leftarrow \mathcal{R}}[|g(X) - \mathbb{E}_{X \leftarrow \mathcal{R}}[g(X)]| \geq 0.1 \cdot (\mathbb{E}_{X \leftarrow \mathcal{R}}[g(X)])] \leq 0.01$

Then,

$$Pr_{X \leftarrow \mathcal{R}}[f(X) \geq 0.01 \cdot (\mathbb{E}_{X \leftarrow \mathcal{R}}[f(X)])] \geq 0.1$$

IV. Upper bound on the complexity of homogeneous $\Sigma\Pi\Sigma\Pi^{\{s\}}$ circuits

In this section, we state and prove the upper bound on the complexity of a $\Sigma\Pi\Sigma\Pi^{\{s\}}$ circuit. A very similar bound was proved by Kayal et al in [KLSSa]. We defer the proof to the full version of the paper [KS14].

Lemma IV.1. *Let C be a depth 4 homogeneous circuit computing a polynomial of degree u in N variables such that the support of the bottom product gates in C is at most s. Let $\mathcal{M}$ be a set of monomials of degree equal to r and let m be a positive integer. Then,*

$$\Phi_{\mathcal{M},m}(C) \leq \textit{Size}(C)\binom{\lceil \frac{2u}{s} \rceil + r}{r}\binom{N}{m+rs}$$

for any choice of m, r, s, N satisfying $m + rs \leq N/2$.

V. Strategy for proving a lower bound on the complexity of $NW_{n,D}$ and $IMM_{\tilde{n},n}$

To show a lower bound on the complexity of the polynomial P(which will be $IMM_{\tilde{n},n}$ or $NW_{n,D}$ in this paper), we choose an appropriate set of monomials $\mathcal{M}$ and a parameter m and then obtain a lower bound on the value of $\Phi_{\mathcal{M},m}(P)$. When $\mathcal{M}$ and m are clear from the context, we use $\Phi_{\mathcal{M},m}(P)$ and $\Phi(P)$ interchangeably. We will now try to gain a more concrete understanding of the space of polynomials, whose dimension we want to lower bound. We will need some notations first.

We denote by $M(\alpha)$ the set of monomials $\text{Supp}(\partial_\alpha(P))$. We will use the two interchangeably. For any monomial $\alpha \in \mathcal{M}$ and any monomial $\beta \in \text{Supp}(\partial_\alpha(P))$, define the set

$$\begin{aligned} S^P_m(\alpha, \beta) = \{\gamma : \deg(\gamma) = \text{Supp}(\gamma) = m \text{ and} \\ \text{Supp}(\gamma) \cap \text{Supp}(\beta) = \phi\} \end{aligned} \tag{4}$$

to be the set of all multilinear monomials of degree m which are disjoint from β. We define the set $\tilde{S}^P_m(\alpha, \beta)$ to be the subset of multilinear monomials γ in $S^P_m(\alpha, \beta)$ such that $\beta \cdot \gamma$ is the leading monomial of $\sigma(\gamma \cdot \partial_\alpha(P))$. Define

$$A^P_m(\alpha, \beta) = \{\gamma \cdot \beta : \gamma \in \tilde{S}^P_m(\alpha, \beta)\}$$

When the polynomial P is clear from the context, we drop the P from $A^P_m(\alpha, \beta)$, $S^P_m(\alpha, \beta)$ and $\tilde{S}^P_m(\alpha, \beta)$ and instead denote them by $A_m(\alpha, \beta)$, $S_m(\alpha, \beta)$ and $\tilde{S}_m(\alpha, \beta)$ respectively.

The following simple lemma relates the size of the union of the sets $A_m(\alpha,\beta)$ to $\Phi_{\mathcal{M},m}(P)$ We refer the interested reader to the full version of this paper [KS14] for the proof.

Lemma V.1. *Let P be a polynomial in N variables and let $\mathcal{M}$ be any set of monomials on these variables. Let $m \leq N$ be a positive integer and let $\Phi_{\mathcal{M},m}(P)$ and $A_m(\alpha,\beta)$ be as defined. Then,*

$$\Phi_{\mathcal{M},m}(P) \geq \left| \bigcup_{\substack{\alpha\in\mathcal{M} \\ \beta\in Supp(\partial_\alpha(P))}} A_m(\alpha,\beta) \right|$$

By the principle of inclusion-exclusion, we get the following corollary.

Corollary V.2. *Let P be a polynomial in N variables and let $\mathcal{M}$ be any set of monomials on these variables. Let $m \leq N$ be a positive integer and let $\Phi_{\mathcal{M},m}(P)$ and $A_m(\alpha,\beta)$ be as defined. Then,*

$$\Phi_{\mathcal{M},m}(P) \geq \sum_{\substack{\alpha\in\mathcal{M} \\ \beta\in Supp(\partial_\alpha(P))}} |A_m(\alpha,\beta)| - \sum_{\substack{\alpha_1,\alpha_2\in\mathcal{M} \\ \beta_1\in Supp(\partial_{\alpha_1}(P)) \\ \beta_2\in Supp(\partial_{\alpha_2}(P)) \\ (\alpha_1,\beta_1)\neq(\alpha_2,\beta_2)}} |A_m(\alpha_1,\beta_1)\cap A_m(\alpha_2,\beta_2)| \quad (5)$$

Therefore, to get a lower bound on $\Phi_{\mathcal{M},m}(P)$, we show that $\sum_{\alpha\in\mathcal{M},\beta\in\partial_\alpha(P)} |A_m(\alpha,\beta)|$ is large and the second term in the expression above is small. The following lemma relates $\sum_{\beta\in\partial_\alpha(P)} |A_m(\alpha,\beta)|$ to the size of the sets $S_m(\alpha,\beta)$, which, in principle are somewhat simpler objects to describe.

Lemma V.3. *Let P be a polynomial in N variables and let $\alpha \in \mathcal{M}$ be a monomial on these variables such that $\partial_\alpha(P)$ is not identically zero. Let $S_m(\alpha,\beta)$ and $A_m(\alpha,\beta)$ be sets as defined. Then,*

$$\sum_{\beta\in Supp(\partial_\alpha(P))} |A_m(\alpha,\beta)| \geq \left| \bigcup_{\beta\in Supp(\partial_\alpha(P))} S_m(\alpha,\beta) \right|$$

Proof: Consider the sets $Z = \{(\beta,\gamma) : \beta \in \text{Supp}(\partial_\alpha(P)), \gamma \in A_m(\alpha,\beta)\}$ and $W = \bigcup_{\beta\in\text{Supp}(\partial_\alpha(P))} S_m(\alpha,\beta)$. The proof follows by showing a one one map from W to Z. ∎

A. Obtaining the lower bound on $\Phi_{\mathcal{M},m}(P)$

For a polynomial P, a set of monomials $\mathcal{M}$ and a positive integer m, we now outline the general sequence of arguments which we use to lower bound $\Phi_{\mathcal{M},m}(P)$. The exact sequence of arguments used in the proofs vary slightly for $NW_{n,D}$ and $IMM_{\bar{n},n}$. To express this outline more concretely, we will need some notations. For a polynomial P and a monomials $\alpha,\alpha' \in \mathcal{M}$, we define

$$T_1(\alpha,P) = \sum_{\beta\in\text{Supp}(\partial_\alpha(P))} |S_m(\alpha,\beta)|$$

$$T_2(\alpha,P) = \sum_{\substack{\beta_1,\beta_2\in\text{Supp}(\partial_\alpha(P)) \\ \beta_1\neq\beta_2}} |S_m(\alpha,\beta_1)\cap S_m(\alpha,\beta_2)|$$

and

$$T_3(\alpha,\alpha',P) = \sum_{\substack{\beta_1\in\text{Supp}(\partial_\alpha(P)) \\ \beta_2\in\text{Supp}(\partial_{\alpha'}(P)) \\ (\alpha,\beta_1)\neq(\alpha',\beta_2)}} |A_m(\alpha,\beta_1)\cap A_m(\alpha',\beta_2)|$$

We also define

$$T_1(P) = \sum_{\alpha\in\mathcal{M}} T_1(\alpha,P)$$

$$T_2(P) = \sum_{\alpha\in\mathcal{M}} T_2(\alpha,P)$$

and

$$T_3(P) = \sum_{\alpha,\alpha'\in\mathcal{M}} T_3(\alpha,\alpha',P)$$

At places where P is clear from the context, we drop the P in $T_1(\alpha,P), T_2(\alpha,P)$ and $T_3(\alpha,\alpha',P)$ and denote them by $T_1(\alpha), T_2(\alpha)$ and $T_3(\alpha,\alpha')$ respectively.

From the Corollary V.2 and Lemma V.3, it follows that for any polynomial P, set of monomials $\mathcal{M}$ and a parameter m,

$$\Phi_{\mathcal{M},m}(P) \geq T_1(P) - T_2(P) - T_3(P)$$

Outline for Nisan-Wigderson polynomials In the proof of the lower bound for the $NW_{n,D}$ polynomial, we observe that over the random restrictions of $NW_{n,D}$, the expected value of $T_1 - T_2 - T_3$ is almost as large as the expected value of T_1. We will then use Lemma III.7 to argue that with a sufficiently high probability, the complexity of a random restriction of $NW_{n,D}$ is high.

VI. Lower bound for $NW_{n,D}$

In this section, we prove lower bound on the size of homogeneous $\Sigma\Pi\Sigma\Pi$ circuits which compute the $NW_{n,D}$ polynomial.

A. Random restrictions

From the definition, it follows that the total number of variables N in $NW_{n,D}$ is $N = n^3$. Let the set of all these variables be $\mathcal{V}$. We will now define our random restriction procedure by defining a distribution $\mathcal{D}$ over subsets $V \subset \mathcal{V}$. The random restriction procedure will sample $V \leftarrow \mathcal{D}$ and then keep only those variables "alive" that come from V and set the rest to zero. The restriction of the set of variables induces a restriction on any polynomial of these variables. We will use the notation $NW_{n,D}|_V$ for the restriction of

$NW_{n,D}$ obtained by setting every variable outside V to 0. Therefore, any distribution $\mathcal{D}$ also induces a distribution on the set of restrictions of $NW_{n,D}$. Similarly, the distribution $\mathcal{D}$ also induces a distribution over the restrictions of any circuit computing a polynomial over $\mathcal{V}$. We will use the notation $C|_V$ for the restriction of a circuit C obtained by setting every input gate in C which is labelled by a variable outside V to 0.

The distribution: Each variable in $\mathcal{V}$ is independently kept alive with a probability $p = n^{-\epsilon}$, where ϵ is an absolute constant such that $0 \leq \epsilon \leq 0.01$. This gives a distribution over the subsets of $\mathcal{V}$. We call it $\mathcal{D}$.

B. Choice of parameters

We enumerate the values of the parameters used in this proof below.

1) n. (This is the degree of the polynomial $NW_{n,D}$)
2) $N = n^3$. (This is the total number of variables)
3) $r = \frac{1.1\sqrt{n}}{5}$. (This is the order of the derivatives involved)
4) $s = \sqrt{n}$. (This indicates the support of a product gate in the circuit after random restrictions)
5) $m = \frac{N}{2}(1 - \frac{\ln n}{5\sqrt{n}})$. (This is the degree of the multilinear shifts)
6) ϵ is any absolute constant such that $0 < \epsilon < 0.01$.
7) $p = n^{-\epsilon}$. (This is the probability with which each variable is kept alive independently)
8) $k = n - r$. (This is the size of the support of the monomials in any r^{th} order derivative of $NW_{n,D}$)
9) $d = \theta\left(\frac{n}{\log n}\right)$ is a parameter chosen such that$n^{2d} = 1/4 \cdot n^{-2}\frac{\binom{N-k}{m}}{\binom{N-2k}{m-k}}$.
10) $D = \frac{\epsilon n}{2} + d$. (This is the parameter D in $NW_{n,D}$)
11) $\mathcal{D}$. (This is the distribution on the subsets of $\mathcal{V}$ obtained by keeping each variable in $\mathcal{V}$ alive independently with a probability $p = n^{-\epsilon}$)

In the rest of this paper, we always invoke the definition of the Nisan-Wigderson polynomials for $D = \frac{\epsilon n}{2} + d$. So, for the rest of the proof, we use the notation NW for $NW_{n,D}$.

C. Effect of random restrictions on the circuit

The following lemma gives us an upper bound on the complexity of *small* circuits under the random restrictions. We skip the proof to the full version of this paper [KS14].

Lemma VI.1. *Let $s = \sqrt{n}, r = \frac{1.1\sqrt{n}}{5}$ and let m be a parameter such that $m + rs \leq N/2$ and let $\epsilon > 0$ be a constant. Let $\mathcal{M}$ be any set of monomials of degree equal to r. Let C be a homogeneous depth 4 circuit of size at most $2^{\frac{\epsilon}{2}\sqrt{n}\log n}$ computing the polynomial NW. Then, with probability at least $1 - o(1)$ over $V \leftarrow \mathcal{D}$*

$$\Phi_{\mathcal{M},m}(C|_V) \leq \mathit{Size}(C)\binom{\lceil \frac{2n}{s} \rceil + r}{r}\binom{N}{m + rs}$$

Observe that the above lemma implies that if the circuit was of size at most $2^{\frac{\epsilon}{2}\sqrt{n}\log n}$, then with probability at least $1 - o(1)$, at the end of the random restriction process, none of the product gates with support larger than $s = \sqrt{n}$ at the bottom level is alive. Otherwise, the size of the circuit was larger than $2^{\frac{\epsilon}{2}\sqrt{n}\log n}$ to start with, in which case, we have nothing to prove.

D. Effect of random restrictions on $NW_{n,D}$

In this section, we show that with a reasonably high probability, a random restriction of NW has a large complexity. We outline the plan and set some notations below.

Plan of the proof: We will show that for $V \leftarrow \mathcal{D}$ expected value of the expression $T_1|_V - T_2|_V - T_3|_V$ is large and then use this to obtain a lower bound on the complexity of a random restriction of NW. We will do this by proving a lower bound on the expected value of $T_1|_V$ and upper bounds on the expected values of $T_2|_V$ and $T_3|_V$. At this point, we would like to argue that the complexity remains close to the expectation with a reasonably high probability. This observation is proved using Lemma III.7 and the bound on the variance of the number of monomials alive at the end of random restrictions obtained in [KLSSa].

Recall that $D = \frac{n.\epsilon}{2} + d$ for some constant ϵ and a parameter $d = \theta(\frac{n}{\log n})$.

Let $\mathcal{M}^{[r]} = \{\prod_{i\in[r]} x_{i,j} : j \in [n^2]\}$ be a set of monomials. Observe that for $r < D$, every monomial in $\mathcal{M}^{[r]}$ has an extension in Supp(NW). This implies that for every $\alpha \in \mathcal{M}^{[r]}$, $\partial_\alpha(NW)$ is non zero. In fact, it consists of exactly $n^{2(D-r)}$ monomials. For our partial derivatives, we consider the set of partial derivatives of NW with respect to monomials from $\mathcal{M}^{[r]}$. For brevity, we call this set $\mathcal{M}$ for the rest of the proof.

We will now prove that with a high probability over $V \leftarrow \mathcal{D}$, $\Phi_{\mathcal{M},m}(NW|_V)$ is large. Recall that from the discussion in Section V, it will suffice to show that $\Phi_{\mathcal{M},m}(NW|_V) = T_1(NW|_V) - T_2(NW|_V) - T_3(NW|_V)$ is large with a good probability. To this end, we first show that $\Phi_{\mathcal{M},m}(NW)$ is large in expectation and then argue that with a good probability the complexity measure is not too much less the mean.

Observe that according to our definitions here, the set of monomials $\mathcal{M}$ is fixed and does not depend upon the random restrictions. Also, the contribution of any monomial $\alpha \in \mathcal{M}$ is a random variable. For example, for any $\alpha \in \mathcal{M}$ and $\beta \in M(\alpha)$, if α and β both survive the random restriction procedure, then the contribution of β to $A_m(\alpha, \beta)$ is $|S_m(\alpha, \beta)| = \binom{N-k}{m}$ whereas if either of them is set to zero during the random restrictions, then the contribution is 0. Similarly for T_2 and T_3. Taking this into account, we state the definitions of T_1, T_2, T_3 which we use in our expectations calculations below. We need a piece of notation first. For monomials $\alpha_1, \alpha_2, \ldots, \alpha_j$, we define $1_{\alpha_1,\alpha_2,\ldots,\alpha_j}$ to be the

event that every monomial in $\{\alpha_1, \alpha_2, \ldots, \alpha_j\}$ survives the random restriction procedure.

- $T_1(NW|_V) = \sum_{\substack{\alpha \in \mathcal{M}^{[r]} \\ \beta \in M(\alpha)}} 1_{\alpha,\beta} \cdot |S_m(\alpha, \beta)|$
- $T_2(NW|_V) = \sum_{\substack{\alpha \in \mathcal{M}^{[r]} \\ \beta,\gamma \in M(\alpha) \\ \beta \neq \gamma}} 1_{\alpha,\beta,\gamma} \cdot |S_m(\alpha, \gamma) \cap S_m(\alpha, \beta)|$
- $T_3(NW|_V) = \sum_{\substack{\alpha_1,\alpha_2 \in \mathcal{M}^{[r]} \\ \beta_1 \in M(\alpha_1) \\ \beta_2 \in M(\alpha_2) \\ (\alpha_1,\beta_1) \neq (\alpha_2,\beta_2)}} 1_{\alpha_1,\alpha_2,\beta_1,\beta_2} \cdot |A_m(\alpha_1, \beta_1) \cap A_m(\alpha_2, \beta_2)|$

For the ease of notations, for the rest of the proof of lower bound for NW, we denote $T_1(NW|_V)$ by $T_1|_V$. Similarly, we use $T_2|_V$ for $T_2(NW|_V)$ and $T_3|_V$ for $T_3(NW|_V)$. We know that for any restriction $NW|_V$,

$$\Phi_{\mathcal{M},m}(NW|_V) \geq T_1|_V - T_2|_V - T_3|_V \tag{6}$$

Therefore, by the linearity of expectation is, the expected complexity of a random restriction of NW,

$$\begin{aligned} \mathbb{E}_{V \leftarrow \mathcal{D}}[\Phi_{\mathcal{M},m}(NW|_V)] \geq \mathbb{E}_{V \leftarrow \mathcal{D}}[T_1|_V] \\ -\mathbb{E}_{V \leftarrow \mathcal{D}}[T_2|_V] - \mathbb{E}_{V \leftarrow \mathcal{D}}[T_3|_V] \end{aligned} \tag{7}$$

We will now bound the expected values of $T_1|_V$, $T_2|_V$, $T_3|_V$ under random restrictions. More precisely, we use the following bounds, whose proofs can be found in the full version at [KS14].

Lemma VI.2.

$$\mathbb{E}_{V \leftarrow \mathcal{D}}[T_1|_V] = \binom{N-k}{m} \cdot n^{2d}$$

Lemma VI.3.

$$\mathbb{E}_{V \leftarrow \mathcal{D}}[T_2|_V] \leq n^{4d-2r+\epsilon r+1} \cdot \binom{N-2k}{m}$$

Lemma VI.4.

$$\mathbb{E}_{V \leftarrow \mathcal{D}}[T_3|_V] \leq n^{4d+2} \cdot \binom{N-2k}{m-k}$$

We will now use the bounds given by the lemmas above to complete the proof of the lower bound.

E. Lower bound on the complexity of $NW_{n,D}$

Lemma VI.5. *For any choice of parameters $m, r, d, \epsilon, n, N, k$ such that*

- $n^{2d-2r+\epsilon r+1} \leq 1/4 \cdot \frac{\binom{N-k}{m}}{\binom{N-2k}{m}}$
- $n^{2d+2} \leq 1/4 \cdot \frac{\binom{N-k}{m}}{\binom{N-2k}{m-k}}$

the following is true

$$\mathbb{E}_{V \leftarrow \mathcal{D}}[\Phi_{\mathcal{M},m}(NW|_V)] \geq 0.5 \cdot \mathbb{E}_{V \leftarrow \mathcal{D}}[T_1|_V]$$

Proof: From the choice of parameters and Lemma VI.2, Lemma VI.3 and Lemma VI.4, it easily follows that $\mathbb{E}_{V \leftarrow \mathcal{D}}[T_1|_V] \geq 4 \cdot \mathbb{E}_{V \leftarrow \mathcal{D}}[T_2|_V]$ and $\mathbb{E}_{V \leftarrow \mathcal{D}}[T_1|_V] \geq 4 \cdot \mathbb{E}_{V \leftarrow \mathcal{D}}[T_3|_V]$. Thus

$$\mathbb{E}_{V \leftarrow \mathcal{D}}[\Phi_{\mathcal{M},m}(NW|_V)] \geq 0.5 \cdot \mathbb{E}_{V \leftarrow \mathcal{D}}[T_1].$$

■

Thus for the above choice of parameters, we get a lower bound on the expected value of $\Phi_{\mathcal{M},m}(NW|_V)$. We would like to conclude that with a decent (≥ 0.1) probability, the complexity is large. Observe that we cannot directly use Markov's inequality. However we are still able to prove such a statement (see Lemma VI.9). We make the following crucial observation. We defer the proof to the full version of the paper [KS14].

Lemma VI.6. *For any $V \subseteq \mathcal{V}$,*

$$\Phi_{\mathcal{M},m}(NW|_V) \leq |\mathit{Supp}(NW|_V)| \binom{N-k}{m}$$

.

We will now use Lemma III.7 to argue that with a decent probablity, a random restriction of NW has a complexity very close to its expected value. For a restriction $P = NW|_V$ of NW, define $g(P) = |\text{Supp}(P)| \cdot \binom{N-k}{m}$ and define $f(P) = \Phi_{\mathcal{M}^{[r]},m}(P)$. Lemma VI.6 implies that for every restriction $P = NW|_V$ of NW, $f(P) \leq g(P)$. Lemma VI.5 implies that $\mathbb{E}_{V \leftarrow \mathcal{D}}[f] \geq 1/2 \cdot \mathbb{E}_{V \leftarrow \mathcal{D}}[g]$. The following lemma of Kayal et al [KLSSa] tells us that g takes values very close to its expected value with a high probability.

Lemma VI.7 ([KLSSa])**.** $Pr_{V \leftarrow \mathcal{D}}[|g(NW|_V) - \mathbb{E}_{V' \leftarrow \mathcal{D}}[g]| \geq 0.1 \cdot \mathbb{E}_{V' \leftarrow \mathcal{D}}[g]] \leq 0.01$.

The functions f and g now satisfy the hypothesis of Lemma III.7. Therefore, we get the following lemma.

Lemma VI.8. $Pr_{V \leftarrow \mathcal{D}}[f(NW|_V) \geq 0.01 \cdot \mathbb{E}_{V' \leftarrow \mathcal{D}}[g]] \geq 0.1$.

Therefore, the following lemma is true.

Lemma VI.9. *For any choice of parameters $m, r, d, \epsilon, n, N, k$ such that*

- $n^{2d-2r+\epsilon r+1} \leq 1/4 \cdot \frac{\binom{N-k}{m}}{\binom{N-2k}{m}}$
- $n^{2d+2} \leq 1/4 \cdot \frac{\binom{N-k}{m}}{\binom{N-2k}{m-k}}$

the following is true

$$Pr_{V \leftarrow \mathcal{D}}[\Phi_{\mathcal{M},m}(NW|_V) \geq 0.005 \cdot n^{2d} \binom{N-k}{m}] \geq 0.1$$

F. Wrapping up the proof

We now complete the proof of the lower bound for the case of NW polynomial which implies Theorem I.1.

Theorem VI.10. *Let C be any homogeneous $\Sigma\Pi\Sigma\Pi$ circuit computing $NW_{n,D}$. Then, the size of C is at least $n^{\Omega(\sqrt{n})}$.*

Proof: Recall that, from our choice of parameters, we have $s = \sqrt{n}$, $r = \frac{1.1\sqrt{n}}{5}$, $N = n^3$, $m = \frac{N}{2}(1 - \frac{\ln n}{5\sqrt{n}}) = \frac{N}{2}(1 - \frac{\ln n}{5s})$, d such that $n^{2d} = 1/4 \cdot n^{-2}\frac{\binom{N-k}{m}}{\binom{N-2k}{m-k}}$, $k = n - r$, and $\epsilon < 0.01$. Observe that $m + rs < \frac{N}{2}$. Let C be a circuit computing the polynomial NW.

If the size of the circuit is at least $n^{\frac{\epsilon}{2}\sqrt{n}}$, then we are done. Else, the size of C is at most $n^{\frac{\epsilon}{2}\sqrt{n}}$. Lemma VI.1 implies that with probability at least $1 - o(1)$ the complexity of the circuit is at most $\text{Size}(C)\binom{\lceil \frac{2n}{s} \rceil + r}{r}\binom{N}{m+rs}$.

It can be verified that for the choice of paramters made above, the hypotheses of Lemma VI.5 hold. More concretely, the following claim is true.

Claim VI.11. *For $m, r, d, \epsilon, n, N, k$ as chosen above,*

- $n^{2d-2r+\epsilon r+1} \leq 1/4 \cdot \frac{\binom{N-k}{m}}{\binom{N-2k}{m}}$
- $n^{2d+2} \leq 1/4 \cdot \frac{\binom{N-k}{m}}{\binom{N-2k}{m-k}}$

Thus by the claim above and Lemma VI.9, we conclude that with

$$\text{Pr}_{V \leftarrow \mathcal{D}}\left[\Phi_{\mathcal{M},m}(NW|_V) \geq \Omega\left(n^{2d}\binom{N-k}{m}\right)\right] \geq 0.1.$$

So, with probability at least $0.1 - o(1)$, the complexity of $C|_V$ is low while at the same time the complexity of the $NW|_V$ remains high. Comparing the bounds, we have

$$\text{Size(C)} \geq \Omega\left(\frac{n^{2d}\binom{N-k}{m}}{\binom{\lceil \frac{2n}{s} \rceil + r}{r}\binom{N}{m+rs}}\right)$$

Substituting the value of the parameters, and applying Lemma III.6, we get our desired bound. ■

ACKNOWLEDGMENT

This research was supported by NSF grant CCF-1350572.

REFERENCES

[AV08] M. Agrawal and V. Vinay. Arithmetic circuits: A chasm at depth four. In *Proceedings of FOCS*, 2008.

[BS83] Walter Baur and Volker Strassen. The complexity of partial derivatives. *Theoretical Computer Science*, 22:317–330, 1983.

[CM13] Suryajith Chillara and Partha Mukhopadhyay. Depth-4 lower bounds, determinantal complexity: A unified approach. *CoRR*, abs/1308.1640v3, 2013.

[FLMS] Hervé Fournier, Nutan Limaye, Guillaume Malod, and Srikanth Srinivasan. Lower bounds for depth 4 formulas computing iterated matrix multiplication. *In Proceedings of STOC 2014*.

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

[GKKSb] Ankit Gupta, Pritish Kamath, Neeraj Kayal, and Ramprasad Saptharishi. Arithmetic circuits: A chasm at depth three. *In Proceedings of FOCS 2013*.

[Kay12] Neeraj Kayal. An exponential lower bound for the sum of powers of bounded degree polynomials. *ECCC*, 19:81, 2012.

[KLSSa] Neeraj Kayal, Nutan Limaye, Chandan Saha, and Srikanth Srinivasan. An exponential lower bound for homogeneous depth four arithmetic formulas. *To appear in FOCS 2014*.

[KLSSb] Neeraj Kayal, Nutan Limaye, Chandan Saha, and Srikanth Srinivasan. Super-polynomial lower bounds for depth-4 homogeneous arithmetic formulas. *In Proceedings of STOC 2014*.

[Koi12] P. Koiran. Arithmetic circuits: The chasm at depth four gets wider. *Theoretical Computer Science*, 448:56–65, 2012.

[KSa] Mrinal Kumar and Shubhangi Saraf. The limits of depth reduction for arithmetic formulas: It's all about the top fan-in. *In Proceedings of STOC 2014*.

[KSb] Mrinal Kumar and Shubhangi Saraf. Superpolynomial lower bounds for general homogeneous depth 4 arithmetic circuits. *In Proceedings of ICALP 2014*.

[KS14] Mrinal Kumar and Shubhangi Saraf. On the power of homogeneous depth 4 arithmetic circuits. *CoRR*, abs/1404.1950, 2014.

[KSS] Neeraj Kayal, Chandan Saha, and Ramprasad Saptharishi. A super-polynomial lower bound for regular arithmetic formulas. *In Proceedings of STOC 2014*.

[NW95] N. Nisan and A. Wigderson. Lower bounds on arithmetic circuits via partial derivatives. In *Proceedings of FOCS*, pages 16–25, 1995.

[Raz10] Ran Raz. Elusive functions and lower bounds for arithmetic circuits. *Theory of Computing*, 6(1):135–177, 2010.

[Str73] V. Strassen. Die berechnungskomplexiät von elementarsymmetrischen funktionen und von interpolationskoeffizienten. *Numer. Math*, 20:238–251, 1973.

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

[Val79] L. G. Valiant. Completeness classes in algebra. In *Proceedings of STOC*, 1979.

[VSBR83] Leslie G. Valiant, Sven Skyum, S. Berkowitz, and Charles Rackoff. Fast parallel computation of polynomials using few processors. *SIAM Journal of Computation*, 12(4):641–644, 1983.