Electronic Colloquium on Computational Complexity, Report No. 68 (2013)

Lower Bounds for Depth 4 Homogenous Circuits with Bounded Top Fanin

Mrinal Kumar* Shubhangi Saraf†

Abstract

We study the class of homogenous $\Sigma\Pi\Sigma\Pi(r)$ circuits, which are depth 4 homogenous circuits with top fanin bounded by r. We show that any homogenous $\Sigma\Pi\Sigma\Pi(r)$ circuit computing the permanent of an $n \times n$ matrix must have size at least $\exp\left(n^{\Omega(1/r)}\right)$.

In a recent result, Gupta, Kamath, Kayal and Saptharishi [6] showed that any homogenous depth 4 circuit with *bottom fanin* bounded by t which computes the permanent of an $n \times n$ matrix must have size at least $\exp(\Omega(n/t))$. Our work builds upon the results of [6], and explores the limits of computation of depth four homogenous circuits when the restriction for the bottom fanin is removed.

For any sequence $\mathcal{D} = D_1, D_2, \ldots, D_k$ of nonnegative integers such that $\sum D_i = n$, we also study the class of homogenous $\Sigma\Pi^{\mathcal{D}}\Sigma\Pi$ circuits, which are homogenous circuits where each Π gate at the second layer (from the the top) is restricted to having its inputs be polynomials whose sequence of degrees is precisely $\mathcal{D}$. We show that for *every* degree sequence $\mathcal{D}$, any $\Sigma\Pi^{\mathcal{D}}\Sigma\Pi$ circuit computing the permanent of an $n \times n$ matrix must have size at least $\exp(n^{\epsilon})$, for some fixed absolute constant ϵ independent of $\mathcal{D}$.

*Department of Computer Science, Rutgers University. Email: mrinal.kumar@rutgers.edu.

†Department of Computer Science and Department of Mathematics, Rutgers University. Email: shubhangi.saraf@gmail.com.

ISSN 1433-8092

1 Introduction

Arithmetic circuits are one of the most fundamental and basic models for the computation of polynomials. Constructing size efficient arithmetic circuits for a given polynomial and proving lower bounds for explicit polynomials are two of the central problems in the area of algebraic complexity. A related and equally fundamental problem in algebraic complexity is the polynomial identity testing (PIT) problem, which is the following: given an arithmetic circuit, decide if the polynomial it computes is identically zero. There is a very simple randomized algorithm for this problem. Schwartz [18] and Zippel [21] observed that evaluating the polynomial at a randomly chosen point from a sufficiently large domain suffices to determine with high probability if the polynomial is identically zero. PIT is one of the most natural problems for which there is a simple randomized solution, but no deterministic algorithm is known, and derandomizing PIT is one of the central questions in the areas of derandomization and pseudorandomness.

The two problems of finding deterministic algorithms for PIT and proving lower bounds for arithmetic circuits are in fact intimately connected. Impagliazzo and Kabanets [7] showed that a full derandomization of PIT would imply *superpolynomial* circuit lower bounds. Furthermore strong enough lower bounds for arithmetic circuits would imply a derandomization of PIT. In the blackbox model, where the PIT algorithm is only allowed blackbox access to the arithmetic circuit, the connection between the two problems is even tighter. A blackbox PIT algorithm for any class of arithmetic circuits gives immediately via interpolation an explicit polynomial that is hard to compute for that class [1].

Even though the problems of PIT and of proving lower bounds for explicit polynomials have received widespread attention and have been intensively studied, we basically have no nontrivial lower bounds or deterministic PIT algorithms for the general model of arithmetic circuits. Consequently, restricted models of circuits have received attention, and in the past two decades, circuits of small depth have been widely studied.

Nisan and Wigderson [14] proved exponential lower bounds for homogenous circuits of depth three which compute the permanent. Grigoriev and Karpinksi [4] showed that any depth 3 circuit over a fixed finite field (with no restriction of homogeneity) which computes the permanent must have exponential size. Even after these developments, proving strong lower bounds for general circuits of depth larger than three, remains a formidable barrier. In fact without the restriction of homogeneity, the best lower bound for even depth 3 circuits over the reals is just $\Omega(n^2)$ [19].

In case of PIT, even less is known. Recently and culminating a long sequence of works [12, 3, 9, 11, 16, 17], deterministic blackbox algorithms for PIT for depth 3 circuits with constant top fanin ($\Sigma\Pi\Sigma(r)$ circuits) were obtained. In the case of depth 4 circuits, we know polynomial time PIT algorithms for depth 4 circuits with constant top fanin ($\Sigma\Pi\Sigma\Pi(r)$ circuits) only when the circuits are restricted to be multilinear [8, 15]. In both cases removing the restriction on the top fanin seems difficult, and thus currently we have algorithms for only weak classes.

In recent years there have been several results "explaining" this lack of progress in proving lower bounds or PIT results for circuits of larger depth. Agrawal and Vinay [2] showed that proving exponential lower bounds for just *depth* 4 circuits (even when the circuits are restricted to be homogenous) would suffice for proving exponential lower bounds for circuits of *arbitrary depth*. Thus, depth 4 circuits seem to capture the inherent complexity of general circuits. Koiran [13] improved the parameters of this result and proved that showing $exp(\sqrt{n}\log^2 n)$ lower bounds for depth four homogenous circuits with bottom fanin bounded by $\sqrt{n}$ for the permanent of an $n \times n$ matrix would imply a superpolynomial lower bound for general arithmetic circuits computing the permanent. When the circuits are not restricted to be homogenous, very surprisingly Gupta, Kayal, Kamath and Saptharishi [5] showed that strong enough exponential lower bounds just for circuits of *depth 3* over the reals would imply superpolynomial circuit lower bounds.

We state some of these results more formally below. In order to be more precise, we first define some basic notions. A $\Sigma\Pi\Sigma\Pi$ circuit is a circuit of depth four where the layers have

alternating + and × gates with the top layer being that of + gates. An n variate homogenous polynomial of degree d computed by a homogenous ΣΠΣΠ circuit can be represented in the form

$$P(x_1, x_2, x_3, \ldots, x_n) = \sum_{i=0}^{m} \prod_{j=1}^{d_i} Q_{ij} \tag{1}$$

Here for every i and j, Q_{ij} is an n- variate homogenous polynomial being computed by a ΣΠ circuit. The homogeneity restriction on C implies that for every $i \in [m]$,

$$deg(P) = d = \sum_{j=1}^{d_i} deg(Q_{ij}) \tag{2}$$

A bound of t on the bottom fanin of ΣΠΣΠ circuits restricts the degrees of the Q_{ij} to be at most t.

We now state below the results of Agrawal, Vinay [2] and Koiran [13].

Theorem 1.1. *[2, 13] If there is a polynomial sized circuit for computing the permanent of an $n \times n$ matrix, then there is a $2^{O(\sqrt{n}\log^2 n)}$-homogenous ΣΠΣΠ circuit computing the permanent, such that the fanin of the bottom product gates is bounded by $\sqrt{n}$.*

In a remarkable recent result in this direction, Gupta, Kamath, Kayal and Saptharishi [6] proved a $exp(\sqrt{n})$ lower bound for the permanent against homogenous ΣΠΣΠ circuits with bottom fanin bounded by $\sqrt{n}$; thus coming really close to the bound which via the result of [13] would imply superpolynomial arithmetic circuit lower bounds. More precisely they showed the following result:

Theorem 1.2. *[6] Any homogenous ΣΠΣΠ circuit, with bottom fanin at most t computing the permanent of an $n \times n$ matrix must have size at least $exp(\Omega(n/t))$.*

Improving the exponent in the above lower bound even slightly would have extremely strong consequences, and it seems to be an extremely tempting line of approach towards proving lower bounds for general circuits. However, as of now it is not clear how simple the task might be, and seems quite possible that getting strong enough improved lower bounds might be out of the scope of current techniques.

1.1 Our results

In this paper, we explore the limits of computation of depth 4 homogenous circuits when the restriction for the bottom fanin is removed. There seem to be two main obstacles in extending the lower bounds of [6] for general depth 4 homogenous ΣΠΣΠ circuits. The lower bounds in [6] work only when the degrees of *all* polynomials feeding into the product gate at the second layer are small (in other words, the bottom fan in is small), say $\leq \sqrt{n}$. It is easy to see that if the degrees of all polynomials feeding into the product gate at the second layer is large (i.e. the bottom fanin of all the gates is large), say $\geq \sqrt{n}$, then for sparsity reasons and simple monomial counting, it is easy to obtain exponential lower bounds. The first obstacle is to handle the case when the degrees of some of the polynomials is small and for some of them it is large. For instance fix any arbitrary sequence $\mathcal{D}$ of degrees summing to n, and assume that the polynomials feeding into each product gate at the second from top layer have their degrees coming from this sequence. Is it still possible to obtain exponential lower bounds? The second obstacle to extending the results from [6] is to find a way to combine the lower bounds for all these various cases into a common lower bound for the case when the circuit is composed of product gates of different kinds. For instance we know lower bounds when all product gates at the second layer have small incoming degrees and when all product gates have large incoming

degrees. However we do not know how to combine these lower bounds into a single lower bound when the circuit is the sum of two circuits, one of the low degree kind, and one of the high degree kind. In this paper we show how to resolve the first obstacle. This result is formally stated as Theorem 1.4 below. As a consequence of our results we also obtain lower bounds for homogenous $\Sigma\Pi\Sigma\Pi(r)$ circuits, stated formally as Theorem 1.3 below.

For the general model of $\Sigma\Pi\Sigma\Pi$ circuits, only very weak lower bounds seem to be known. Even PIT for $\Sigma\Pi\Sigma\Pi$ circuits is known only when the top fanin is constant and the circuit is multilinear (in the multilinear case, the degree of the polynomials computed must anyway be bounded by the number of variables, and hence, multilinearity is a much bigger restriction than homogeneity[1]). The problem of showing lower bounds for depth 4 circuits with bounded top fanin is hence a problem that is simpler than derandomizing PIT for the same model (at least in the black box model), and it seems to be the first crucial step in that direction.

Lower bounds for homogenous $\Sigma\Pi\Sigma\Pi(r)$ circuits: We consider homogenous $\Sigma\Pi\Sigma\Pi(r)$ circuits, which are depth 4 homogenous circuits whose *top fanin* is bounded by r. When r is a constant we prove exponential lower bounds[2] for the class of $\Sigma\Pi\Sigma\Pi(r)$ circuits[3]. In particular, we prove the following theorem:

Theorem 1.3. *Let C be a homogenous $\Sigma\Pi\Sigma\Pi(r)$ circuit that computes the $n \times n$ permanent. Let s be the size of C. Then*

$$s \geq \exp\left(n^{\Omega(1/r)}\right).$$

Prior to this result, we are not aware of any such lower bounds for depth 4 circuits even when the top fanin r is bounded by 2.

Lower bounds for homogenous $\Sigma\Pi^{\mathcal{D}}\Sigma\Pi$ circuits: Another class of circuits we are able to prove a lower bound for is the class of depth 4 circuits where each product at the second layer (from the top) has the same degree sequence of incoming polynomials.

For any degree sequence $\mathcal{D} = D_1, D_2, \ldots, D_k$ of nonnegative integers such that $\sum D_i = n$, we study the class of homogenous $\Sigma\Pi^{\mathcal{D}}\Sigma\Pi$ circuits, which are homogenous circuits where each Π gate at the second layer is restricted to having its inputs be polynomials whose sequence of degrees is precisely $\mathcal{D}$. (We give a more formal definition in Section 2.) We show that for *every* degree sequence $\mathcal{D}$, any $\Sigma\Pi^{\mathcal{D}}\Sigma\Pi$ circuit computing the permanent of an $n \times n$ matrix must have size at least $\exp(n^{\epsilon})$, for some fixed absolute constant ϵ independent of $\mathcal{D}$.

Theorem 1.4. *Let C be a homogenous $\Sigma\Pi^{\mathcal{D}}\Sigma\Pi$ circuit that computes the $n \times n$ permanent. Let s be the size of C. Then*

$$s \geq \exp(n^{\epsilon}),$$

for some fixed absolute constant $\epsilon > 0$.

One consequence of the above result is that we show that one can partition the set of product gates of every depth 4 circuit into constantly many parts (roughly 10 parts would suffice), and for each part we are able to prove exponential lower bounds. However as of now we do not know how to combine this bound across the parts in order to get a lower bound for all depth 4 circuits.

[1] In all the results of this paper, the restriction of homogeneity can be replaced by the restriction that all gates in the circuit compute polynomials of degree at most n.

[2] In the rest of the paper, by exponential lower bound we will mean a lower bound of the form $2^{n^{\epsilon}}$ for some constant ϵ.

[3] It is important to observe that the reduction of an polynomial sized homogenous $\Sigma\Pi\Sigma\Pi$ circuit with arbitary bottom fanin to a homogenous $\Sigma\Pi\Sigma\Pi$ circuit with bounded bottom fanin as given by the results of [2, 13] can lead to circuits of size $O(2^{O(\sqrt{n}\log^2 n)})$ and so Theorem 1.2 does not imply any nontrivial lower bounds for it.

1.2 Completeness of the model of $\Sigma\Pi\Sigma\Pi(r)$ circuits

Depth 3 and depth 4 circuits with bounded top fanin ($\Sigma\Pi\Sigma(r)$ and $\Sigma\Pi\Sigma\Pi(r)$ respectively) have been extensively studied in the past especially in the context of polynomial identity testing (PIT). The question of lower bound for $\Sigma\Pi\Sigma(r)$ circuits is almost uninteresting since it can be shown quite easily that for $r < n$, $\Sigma\Pi\Sigma(r)$ circuits cannot compute the $n \times n$ permanent or determinant, *no matter what the size* of the circuit. Thus the class of $\Sigma\Pi\Sigma(r)$ circuits is not complete, in the sense that the class of circuits cannot even compute all polynomials. In contrast, the class of depth 2 $\Sigma\Pi$ circuits (with no restriction on top fanin) is complete, but lower bounds are trivial for this model since any polynomial with m monomials needs a $\Sigma\Pi$ circuit of size at least m to compute it.

It was observed by Kayal [10] that if one considers the class of depth 4 circuits and one imposes the additional requirement that each product gate has at least 2 nontrivial factors, then the class of $\Sigma\Pi\Sigma\Pi(r)$ circuits with $r < n/2$ circuits is not complete. This is because if α is a common root of at least two of the factors of each of the product gates, then it would be a zero of multiplicity 2 of the polynomial computed by the circuit. Also if $r < n/2$ then such an α always exists. Hence if one starts with a polynomial that does not vanish at any point with multiplicity 2, then it cannot be computed by such a circuit. Thus in this case we can prove lower bounds easily.

The general class of depth 4 $\Sigma\Pi\Sigma\Pi(r)$ circuits even when $r = 1$ is a complete class, since it contains the class of depth 2 $\Sigma\Pi$ circuits. However lower bounds for $\Sigma\Pi\Sigma\Pi(r)$ circuits for $r \geq 2$ did not seem to be known prior to this work.

Organization of the paper: In Section 2, we discuss some preliminary notions used in the paper. In Section 3, we give an overview of the proof. In Section 4, we present the proof of Theorem 1.3. We conclude with some future directions of work and open problems in Section 5.

2 Preliminaries

An arithmetic circuit over a field $\mathbb{F}$ and variables $\{x_1, x_2, \ldots, x_n\}$ is a directed acyclic graph with every node, called a gate, being labelled by one of the symbols from the set $\{+, \times, x_1, x_2, \ldots, x_n\}$ or constants from the field $\mathbb{F}$. The gates labelled by the set of variables or field elements are called input gates. The circuit has one or more gates of fanout 0 called the output gate. The size of the circuit is the number of nodes in the circuit and the depth of the circuit is the length of the longest path from an output gate to an input gate. A circuit is said to be homogenous if the polynomial computed at every gate is homogenous. A $\Sigma\Pi\Sigma\Pi$ circuit is a circuit of depth four where the layers have alternating $+$ and $\times$ gates with the top layer being that of $+$ gates. In this work, we will mainly be working with $\Sigma\Pi\Sigma\Pi(r)$ circuits, which are depth four homogenous circuits whose top fanin is bounded by r. An n variate homogenous polynomial of degree d computed by such a circuit C can be represented in the form

$$P(x_1, x_2, x_3, \ldots, x_n) = \sum_{i=1}^{r} \prod_{j=1}^{d_i} Q_{ij} \tag{3}$$

For each $i \in [r]$, the product $P_i = \prod_{j=1}^{d_i} Q_{ij}$ is said to be computed by the product gate i. Therefore, $P = \sum_{i=1}^{r} P_i$. Here for every i and j, Q_{ij} is an n variate homogenous polynomial being computed by a $\Sigma\Pi$ circuit. The homogeneity restriction on C implies that for every product gate i,

$$deg(P) = d = \sum_{j=1}^{d_i} deg(Q_{ij}) \tag{4}$$

With every product gate $i \in [r]$, we can associate a multiset $\mathcal{D} = (D_i, m_i)$, where

$$D_i = \{deg(Q_{ij}) : j \in [d_i]\} \tag{5}$$

and m_i is a map from D_i to $\mathbb{N}$, which assigns to every element l in D_i, the number of $j \in [d_i]$ such that Q_{ij} has degree equal to l. For a homogenous depth 4 circuit, computing a degree d polynomial, equation 4 can be rewritten as

$$deg(P) = d = \sum_{j \in D_i} j \times m_i(j) \tag{6}$$

for each i in $[r]$. We define $\Sigma\Pi^{\mathcal{D}}\Sigma\Pi$ circuits to be $\Sigma\Pi\Sigma\Pi$ circuits in which every product gate i has the same multiset $(D_i, m_i) = \mathcal{D}$ associated with it.

For more on arithmetic circuits and related results, we refer the interested reader to the survey [20].
For any positive integer n, the permanent of an $n \times n$ matrix M is defined as

$$Perm(M) = \sum_{\sigma \in S_n} \prod_{i \in [n]} M[i, \sigma(i)] \tag{7}$$

where $M[i, j]$ is the element in the i^{th} row and j^{th} column of M, and S_n is the set of all $n!$ permutations of $\{1, 2, \ldots, n\}$. When M is a matrix such that $M[i, j] = x_{ij}$, the permanent is a homogenous polynomial of degree n in n^2 variables. We will use $Perm_n$ for the permanent of an $n \times n$ matrix.

We will now define the notion of shifted partial derivatives which is the basic complexity measure used for the proof. This is the same measure that was used in the results on [6], and we use the same definitions. For an n variate polynomial $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ and a positive integer k, we denote by $\partial^{=k} f$, the set of all partial derivatives of order equal to k of f. Our proof uses the notion of shifted partial derivatives of a polynomial defined below.

Definition 2.1 ([6]). *For an n variate polynomial $P \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ and integers $k, \ell \geq 0$, the space of ℓ shifted k^{th} order partial derivatives of P is defined as*

$$\langle \partial^{=k} P \rangle_{\leq \ell} \stackrel{def}{=} \mathbb{F}\text{-}span\{ \prod_{i \in [n]} {x_i}^{j_i} \cdot g : \sum_{i \in [n]} j_i \leq \ell, g \in \partial^{=k} P\} \tag{8}$$

Here, $\partial^{=k} P$ is the set of all partial derivatives of P of order k.

3 Proof Overview

Most lower bounds for arithmetic circuits proceed by identifying some kind of "progress measure", and show that for any given circuit in a circuit class, the measure is small if the size of the circuit is small, whereas for the polynomial one is trying to compute (for instance the permanent), the measure is large. In the result by Gupta et al. [6], the progress measure used is the dimension of the ℓ shifted k^{th} order partial derivative $\dim(\langle \partial^{=k} P \rangle_{\leq \ell})$, for a suitable choice of ℓ and k. It is shown that every small depth 4 circuit with bounded bottom fanin has small $\dim(\langle \partial^{=k} P \rangle_{\leq \ell})$ compared to that of the permanent. Thus if a depth 4 circuit with bounded bottom fanin must compute the permanent, then it must be large. More precisely it is shown that every product gate $Q_i = \prod_{j=1}^{d} Q_{ij}$ has $\dim(\langle \partial^{=k} P \rangle_{\leq \ell})$ much smaller than that of the permanent, provided the degrees of the Q_{ij} are small. This is the core of the argument. Combined with the sub-additivity of $\dim(\langle \partial^{=k} P \rangle_{\leq \ell})$, the result easily follows.

Our proof builds upon the results of [6], and combines the use of the progress measure $\dim(\langle \partial^{=k} P \rangle_{\leq \ell})$ with the notion of "sparsity". Suppose $C = \sum_{i=0}^{r} \prod_{j=1}^{d_i} Q_{ij}$ is a homogenous

$\Sigma\Pi\Sigma\Pi$ circuit computing the $n \times n$ permanent. If all the Q_{ij} had low degree, then the results of [6] give exponential lower bounds for the size of C computing the permanent. Also in the extreme case where all the Q_{ij} have high degree, then since C is homogenous, the number of Q_{ij} per product gate $Q_i = \prod_{j=1}^{d} Q_{ij}$ must be small, and hence their product cannot have too many monomials[4]. If the number of monomials is too few, we would not even be able to get all the monomials in the permanent. In general of course there might be some high degree and some low degree polynomials, and we attempt to interpolate between the two settings to obtain our results.

For each product gate $Q_i = \prod_{j=1}^{d} Q_{ij}$, recall that each Q_{ij} is a homogenous polynomial of degree d_{ij} (say), and $\sum_{j=1}^{d} d_{ij} = n$. If the size of the circuit is at most s, then each Q_{ij} has at most s monomials. We decompose each product gate into its inputs Q_{ij} of *high degree* (those of degree $\geq t$) and its inputs Q_{ij} of *low degree* (those of degree <t). Observe that there cannot be too many (greater than n/t) high degree polynomials Q_{ij} as otherwise their product would have degree exceeding n. Thus the product of all the high degree Q_{ij} cannot have more than $s^{n/t}$ monomials. Let H be the product of the high degree Q_{ij}, and L be the product of the low degree Q_{ij}. Then, by writing out H as a sum of monomials ($H = \sum_k h_k$) and multiplying each monomial h_k with L, we can expand out Q as $\sum_k h_k \cdot L$. Note that L is a product of low degree polynomials. Also, each h_k is a monomial and hence a product of degree 1 polynomials. Thus we have expressed Q as a $\Sigma\Pi\Sigma\Pi$ circuit, where now all the product gates multiply polynomials of degree at most t.

The hope at this point would be to apply this transformation to all the product gates and then possibly apply the result by [6] to obtain a lower bound. The trouble with this argument is that under the transformation described, the top fanin of the original circuit might blow up by a factor equalling the number of monomials in H, which could be nearly as large as $s^{n/t}$. With this loss in parameters, the bound given by the [6] result gives nothing nontrivial. Thus in general one cannot choose an absolute threshold t and for all product gates choose degrees greater than t to be the high degree polynomials and the ones below t to the the low degree polynomials.

What we show is that by examining the degrees of the polynomials feeding into the product gates, one can carefully choose a threshold t that works for each product gate individually, though it might not be the same threshold for all gates. It turns out that this threshold that we find is purely a function of the degree sequence $\mathcal{D}$ of the product gate. Thus if all product gates have the *same* degree sequence, i.e. we have a $\Sigma\Pi^{\mathcal{D}}\Sigma\Pi$ circuit, then we obtain exponential lower bounds. However for general $\Sigma\Pi\Sigma\Pi$ circuits it can be a problem, since if the threshold is different for different gates, we do not have any one single progress measure that works for all gates and thus for the entire circuit. However we are still able to show that for each gate, only very few thresholds are "bad", and when the top fanin is a *constant*, then we show there is a single threshold that will work for all gates to give exponential lower bounds.

4 Proof of Theorem 1.3

In this section, we will present the proof of Theorem 1.3. Let us consider a homogenous $\Sigma\Pi\Sigma\Pi(r)$ circuit C of size s computing the permanent of an $n \times n$ matrix M. From Equation 3, this implies that

$$Perm(M) = \sum_{i=1}^{r} \prod_{j=1}^{d_i} Q_{ij} \tag{9}$$

[4]The number of monomials in each Q_{ij} is a most the size of the circuit.

where for every value of i and j, Q_{ij} is a homogenous polynomial being computed by a sub-circuit of depth 2 of C. Observe that Q_{ij} is being computed by a $\Sigma\Pi$ circuit and hence, the number of monomials with nonzero coefficients in a sum of products expansion of Q_{ij} will be at most the size of C. In other words, Q_{ij} is s sparse for each $i \in [r]$ and $j \in [d_i]$. Without loss of generality, we will assume that for every $i \in [r]$, $d_i = n$, since if $d_i < n$ for any i, we can always make it equal to n by multiplying it with the identically 1 polynomial.

Let us now consider the polynomial computed at a product gate near the top of C. It is of the form $Q = \prod_{i\in[n]} Q_i$. Let us also assume without loss of generality that the Q_i are arranged in non-increasing order of their degrees. The idea of the proof as described in Section 3 would be to decompose the Q_i into *high degree* and *low degree* parts and then multiply out all the *high degree* parts and count on their sparsity to show that the product does not blow up the dimension of the space of shifted partial derivatives by too much. We will then use the following lemma implicit in the work of [6], to obtain our bounds.

Lemma 4.1. *[Implicit in [6]] Let $P = \prod_{i=1}^{d} \tilde{P}_i$ be a polynomial in N variables such that the sum of the degrees of any k of these d polynomials $\tilde{P}_1, \tilde{P}_2, \ldots, \tilde{P}_d$ is at most D. Then, for any integer $\ell \geq 0$,*

$$\dim(\langle \partial^{=k} f \rangle_{\leq \ell}) \leq \binom{d+k-1}{k}\binom{N+D-k+\ell}{N}.$$

Proof. The proof of the lemma is very similar to that in [6]. The version of the Lemma in [6] is when *all* degrees are small and hence the sum of few degrees is also small. In particular, the only change to the result of [6] is to replace their bound of tk (which for them was the sum of degrees of k polynomials of degree at most t), by our bound of D. □

The following lemma is the core of our argument.

Lemma 4.2. *Let $Q = \prod_{j\in[n]} Q_i$ be a depth 3 $\Pi\Sigma\Pi$ homogenous circuit of degree n in N variables, where each Q_i has at most s monomials. Let $0 < \epsilon < 1$ be any small constant. Consider $k = n^{i/m}$, for $1 \leq i \leq m$ and any integer $\ell \geq 0$. Then for all but $1/\epsilon$ choices of i ,*

$$\dim(\langle \partial^{=k} Q \rangle_{\leq \ell}) \leq s^{k\cdot n^{-1/m}} \cdot \binom{k/\epsilon+k-1}{k}\binom{N+4\epsilon n-k+\ell}{N}.$$

Proof. Since the Q_i's are arranged in order of decreasing degree, Q_1 has highest degree and Q_n has the smallest degree.

For $1 \leq i \leq m$, let $S_i = \{Q_j | j \leq n^{i/m}\}$ be the set of the first $n^{i/m}$ of the Q_j's. For each i, we will sum the degrees of the Q_j's in $S_i \setminus S_{i-1}$. Let

$$D_i = \sum_{j \text{ s.t.} Q_j \in S_i \setminus S_{i-1}} \deg(Q_j).$$

Then $\sum_{i=1}^{m} D_i = n$. Thus there are at most $1/\epsilon$ choices of i for which $D_i \geq \epsilon n$. We will show that for all other choices of i, for $k = n^{i/m}$ and any integer $\ell \geq 0$, $\dim(\langle \partial^{=k} Q \rangle_{\leq \ell}) \leq s^{k\cdot n^{-1/m}} \cdot \binom{k/\epsilon+k-1}{k}\binom{N+4\epsilon n-k+\ell}{N}$.

Let us fix i such that $D_i \leq \epsilon n$. We will split up the various Q_j's into those that are in S_{i-1} and those that are not. For those Q_j in S_{i-1}, we will exploit the fact that there aren't too many of them and they each have at most s monomials, to show that they do not affect the dimension of shifted partial derivatives by too much. For the rest of the Q_j we will take advantage of the fact that their degrees are not too large, and hence the sum of degrees of any k of them is small, and thus we will be able to bound the span of shifted partial derivatives of their product using the argument presented in [6].

Let $H = \prod_{Q_j \in S_{i-1}} Q_j$, and let $Q_{\bar{H}} = Q/H$. Since each Q_i has at most s monomials, thus H has at most $s^{n^{(i-1)/m}}$ monomials. Hence we can express the polynomial Q as the sum of at most $s^{n^{(i-1)/m}}$ polynomials $P_1, P_2, \ldots P_u$, where each of the polynomials is the product of some monomial (from H), and the product of all the Q_j that are not in S_{i-1} (i.e. those in $Q_{\bar{H}}$) .

We will show that for each P_j, $1 \leq j \leq u$, for $k = n^{i/m}$,

$$\dim(\langle \partial^{=k} P_j \rangle_{\leq \ell}) \leq \binom{k/\epsilon + k - 1}{k} \binom{N + 4\epsilon n - k + \ell}{N}.$$

Since u is at most the number of monomials in H, thus $u \leq s^{n^{(i-1)/m}} = s^{k \cdot n^{-1/m}}$. Since $Q = \sum_{j \in [u]} P_j$, the sub-additivity of $\dim(\langle \partial^{=k} \rangle_{\leq \ell})$ will imply that

$$\dim(\langle \partial^{=k} Q \rangle_{\leq \ell}) \leq s^{k \cdot n^{-1/m}} \cdot \binom{k/\epsilon + k - 1}{k} \binom{N + 4\epsilon n - k + \ell}{N}.$$

Let us focus our attention on any one of these polynomials P_j, and call it P.

Then $P = h \cdot Q_{\bar{H}} = h \cdot \prod_{j \geq n^{(i-1)/m}+1} Q_j$, where h is a monomial of H and can be thus written as a product of degree one homogenous polynomials. Let us rename the degree 1 polynomials in h and the different Q_j dividing $Q_{\bar{H}}$, so that $P = \hat{P}_1 \hat{P}_2 \cdots \hat{P}_\ell$.

Consider all the polynomials $\hat{P}_i$ dividing P which have degree at most $\epsilon n/k$, and group them together and multiply them so that each of the grouped polynomials now has degree at least $\epsilon n/k$ and at most $2\epsilon n/k$. Clearly this can be done. Call the new set of polynomials (the grouped ones and the ones that had degree at least $\epsilon n/k$ to start out with) $\tilde{P}_1, \tilde{P}_2, \ldots, \tilde{P}_d$. Since the sum of their degrees is at most n, thus the total number d of these polynomials is at most k/ϵ.

Proposition 4.3. *The sum of the degrees of any k of these d polynomials $\tilde{P}_1, \tilde{P}_2, \ldots, \tilde{P}_d$ is at most $4\epsilon n$.*

Proof. Out of the k polynomials, we see what fraction lie among the "grouped" polynomials, and what lie among the original ungrouped polynomials. Recall that by the choice of i, and setting $k = n^{\frac{i}{m}}$, the sum of degrees of any $k - kn^{\frac{-1}{m}}$ of the $\hat{P}_i$ dividing P was at most ϵn. Therefore, the sum of the degrees of any k of them will be at most $2\epsilon n$. Thus, the contribution from the original ungrouped polynomials is at most $2\epsilon n$. Also, the contribution from the grouped polynomials can be at most $2\epsilon n$ since there are at most k of them, and each has degree at most $2\epsilon n/k$. Thus the total sum of degrees is at most $4\epsilon n$. □

Thus, $P = \prod_{i=1}^{d} \tilde{P}_i$ is a polynomial in N variables such that the sum of the degrees of any k of the d polynomials $\tilde{P}_1, \tilde{P}_2, \ldots, \tilde{P}_d$ is at most $D = 4\epsilon n$. Recall also that $d \leq k/\epsilon$. Hence, by Lemma 4.1, for any integer $\ell \geq 0$,

$$\dim(\langle \partial^{=k} P \rangle_{\leq \ell}) \leq \binom{k/\epsilon + k - 1}{k} \binom{N + 4\epsilon n - k + \ell}{N}.$$

□

Theorem 4.4. *Let C be a homogenous $\Sigma\Pi\Sigma\Pi(r)$ circuit in N variables, of size s and of degree at most n. Then for all constants ϵ, with $0 < \epsilon < 1$, there exists a choice of i, with $1 \leq i \leq 2r/\epsilon$, such that for $k = n^{\epsilon i/2r}$, and for all integers $\ell \geq 0$,*

$$\dim(\langle \partial^{=k} C \rangle_{\leq \ell}) \leq r \cdot s^{k \cdot n^{-\epsilon/2r}} \cdot \binom{k/\epsilon + k - 1}{k} \binom{N + 4\epsilon n - k + \ell}{N}.$$

Proof. Let $m = 2r/\epsilon$. Let $C = \sum_{j=1}^{r} Q_j$. Let $i \in [m]$.

Then for each Q_j, by Lemma 4.2, for all but $1/\epsilon$ choices of i, for $k = n^{i/m}$,

$$\dim(\langle \partial^{=k} Q_j \rangle_{\leq \ell}) \leq s^{k \cdot n^{-1/m}} \cdot \binom{k/\epsilon + k - 1}{k} \binom{N + 4\epsilon n - k + \ell}{N}.$$

Hence for each Q_j we get at most $1/\epsilon$ choices of i that may not work to get the bound above, and we call those choices "bad" for Q_j. We call the rest of the choices "good" for Q_j. Thus by the union bound there are at most r/ϵ choices of i that are bad for some Q_j. Since $m > r/\epsilon$, thus there is a choice of $i \in [m]$ that is good for every Q_j.

Thus for any integer $\ell \geq 0$ and $k = n^{i/m}$, for all $j \in [r]$,

$$\dim(\langle \partial^{=k} Q_j \rangle_{\leq \ell}) \leq s^{k \cdot n^{-1/m}} \cdot \binom{k/\epsilon + k - 1}{k} \binom{N + 4\epsilon n - k + \ell}{N}.$$

Hence

$$\dim(\langle \partial^{=k} C \rangle_{\leq \ell}) \leq r \cdot s^{k \cdot n^{-1/m}} \cdot \binom{k/\epsilon + k - 1}{k} \binom{N + 4\epsilon n - k + \ell}{N}.$$

□

We can observe that the choice of the threshold and k for every product gate just depends upon the multiset of the degrees associated with the input feeding into it. In particular, if we start with a $\Sigma\Pi^{\mathcal{D}}\Sigma\Pi$ circuit, then the value of the threshold and k that works for one product gate also works for the circuit in general. Hence, we have the following theorem which gives us an upper bound on the dimension of the shifted partial derivative space of a $\Sigma\Pi^{\mathcal{D}}\Sigma\Pi$ circuit.

Theorem 4.5. *Let C be a homogenous $\Sigma\Pi^{\mathcal{D}}\Sigma\Pi$ circuit in N variables, of size s, top fanin r and of degree at most n. Then for all constants ϵ, with $0 < \epsilon < 1$, there exists a choice of i, with $1 \leq i \leq m$, where $m = 1/\epsilon + 1$ such that for $k = n^{i/m}$, and for all integers $\ell \geq 0$,*

$$\dim(\langle \partial^{=k} C \rangle_{\leq \ell}) \leq r \cdot s^{k \cdot n^{-1/m}} \cdot \binom{k/\epsilon + k - 1}{k} \binom{N + 4\epsilon n - k + \ell}{N}.$$

It is important to note the difference between the bounds in Theorem 4.4 and Theorem 4.5. In Theorem 4.5, the exponent of s is independent of the top fanin r as m is a constant.

Now, by the results of [6], we will bound the dimension of the space of shifted partial derivatives for the permanent and then use this bound to complete the proof of Theorem 1.3. Below we state the results we use from [6].

Theorem 4.6 ([6])**.** *For any integers $n, m, k, l \geq 0$*

$$\dim(\langle \partial^{=k} Perm_n \rangle_{\leq \ell}) \geq \binom{n+k}{2k} \binom{n-k-1}{m-n+k} \binom{n^2 - n + \ell - k + 1}{n^2 - 2n + m + 1}.$$

Theorem 4.7 ([6])**.** *$\exists \epsilon_0 > 0$ such that the following holds: Let ϵ be a constant, with $0 < \epsilon < \epsilon_0$. Let $\ell, m, n, k, t, d > 0$ be integers such that $\ell = n^2 t$, $m = 2n - (n/t)$, $k = \epsilon(n/t)$, $d = cn/t$ for some constant $c \leq 3$. Let*

$$E = \frac{\binom{n+k}{2k}\binom{n-k-1}{m-n+k}\binom{n^2-n+\ell-k+1}{n^2-2n+m+1}}{\binom{d+k-1}{k}\binom{n^2+\ell+(t-1)k}{n^2}}.$$

Then, $E \geq \exp(\Omega(\frac{n}{t}))$.

We now prove our main result, Theorem 1.3.

Proof of Theorem 1.3. Clearly the degree of the polynomial computed by C is n and the number of variables in C is $n^2 = N$. Let ϵ be a constant such that $0 < \epsilon < \epsilon_0$, where ϵ_0 is the same constant as in Theorem 4.7. Let $\epsilon' = \epsilon/4$.

By Theorem 4.4, there exists a choice of i, with $1 \leq i \leq 2r/\epsilon'$, such that for $k = n^{\epsilon' i/2r}$, and for all integers $\ell \geq 0$,

$$\dim(\langle \partial^{=k} C \rangle_{\leq \ell}) \leq r \cdot s^{k \cdot n^{-\epsilon'/2r}} \cdot \binom{k/\epsilon' + k - 1}{k} \binom{N + 4\epsilon' n - k + \ell}{N}.$$

Fix that choice of i and set $k = n^{\epsilon' i/2r}$. Let $t = \epsilon n/k$. Thus $tk = \epsilon n$. Let $\ell = n^2 t$, $m = 2n - (n/t)$, and $d = k/\epsilon' = 4n/t$.

Also by Theorem 4.6,

$$\dim(\langle \partial^{=k} Perm_n \rangle_{\leq \ell}) \geq \binom{n+k}{2k} \binom{n-k-1}{m-n+k} \binom{n^2 - n + \ell - k + 1}{n^2 - 2n + m + 1}.$$

Since C computes $Perm_n$, thus $\dim(\langle \partial^{=k} C \rangle_{\leq \ell}) \geq \dim(\langle \partial^{=k} Perm_n \rangle_{\leq \ell})$. Thus

$$r \cdot s^{k \cdot n^{-\epsilon'/2r}} \cdot \binom{k/\epsilon' + k - 1}{k} \binom{N + 4\epsilon' n - k + \ell}{N} \geq \binom{n+k}{2k} \binom{n-k-1}{m-n+k} \binom{n^2 - n + \ell - k + 1}{n^2 - 2n + m + 1}.$$

Hence,

$$\begin{aligned} r \cdot s^{k \cdot n^{-\epsilon'/2r}} &\geq \frac{\binom{n+k}{2k}\binom{n-k-1}{m-n+k}\binom{n^2-n+\ell-k+1}{n^2-2n+m+1}}{\binom{k/\epsilon'+k-1}{k}\binom{N+4\epsilon' n-k+\ell}{N}} \\ &\geq \frac{\binom{n+k}{2k}\binom{n-k-1}{m-n+k}\binom{n^2-n+\ell-k+1}{n^2-2n+m+1}}{\binom{d+k-1}{k}\binom{N+tk-k+\ell}{N}} \\ &\geq \exp(\Omega(\frac{n}{t})) = \exp(\Omega(k)) \qquad \text{(by Theorem 4.7).} \end{aligned}$$

Using the fact that r is at most s (in fact it is much much smaller), we conclude that

$$k \cdot n^{-\epsilon'/2r} \cdot \log s \geq \Omega(k).$$

Thus

$$\log s \geq \Omega(n^{\epsilon'/2r})$$

and hence

$$s \geq \exp\left(n^{\Omega(1/r)}\right).$$

□

A very similar calculation lets us prove Theorem 1.4.

Proof of Theorem 1.4. For a $\Sigma\Pi^{\mathcal{D}}\Sigma\Pi$ circuit, the calculation will proceed exactly the same as above, and in the end, we will get

$$s \geq \exp\left(n^{\Omega(1/m)}\right),$$

which on substituting $m = 1/\epsilon + 1$, completes the proof. Thus, for all $\mathcal{D}$ we obtain exponential lower bounds for $\Sigma\Pi^{\mathcal{D}}\Sigma\Pi$ circuits computing the permanent regardless of their top fanin. □

5 Future directions

One of the most interesting questions left open by this work is to remove the restriction on top fanin, and to prove super polynomial lower bounds for all homogenous $\Sigma\Pi\Sigma\Pi$ circuits. While this would not still suffice in proving lower bounds for general arithmetic circuits, this seems to be an important step in that direction. Our results show that given any homogenous $\Sigma\Pi\Sigma\Pi$ circuit we can partition the circuit as a sum of constantly many circuits, such that for each of those circuits, for some choice of ℓ and k, the dimension of the span of ℓ shifted k^{th} order partial derivative is a strong enough progress measure for proving lower bounds for that circuit. The trouble is that the value of k and ℓ could be different for the different parts, and we do not know how to combine these different values of k and ℓ into one single progress measure which would work for the original circuit. Another very interesting direction would be to give nontrivial PIT results for $\Sigma\Pi\Sigma\Pi(r)$ circuits when r is a constant. So far, we only know how to derandomize PIT when the $\Sigma\Pi\Sigma\Pi(r)$ circuits are multilinear, and our lower bound for $\Sigma\Pi\Sigma\Pi(r)$ circuits could be viewed an a first step in this direction.

References

[1] M. Agrawal. Proving lower bounds via pseudo-random generators. In *Proceedings of the 25th FSTTCS*, pages 92–105, 2005.

[2] M. Agrawal and V. Vinay. Arithmetic circuits: A chasm at depth four. In *Proceedings of the 49th Annual FOCS*, pages 67–75, 2008.

[3] Z. Dvir and A. Shpilka. Locally decodable codes with 2 queries and polynomial identity testing for depth 3 circuits. *SIAM Journal on Computing*, 36(5):1404–1434, 2006.

[4] D. Grigoriev and M. Karpinski. An exponential lower bound for depth 3 arithmetic circuits. In *Proceedings of the 30th Annual STOC*, pages 577–582, 1998.

[5] A. Gupta, P. Kamath, N. Kayal, and R. Saptharishi. Arithmetic circuits: A chasm at depth three. *Electronic Colloquium on Computational Complexity (ECCC)*, 20:26, 2013.

[6] A. Gupta, P. Kamath, N. Kayal, and R. Saptharishi. An exponential lower bound for homogeneous depth four arithmetic circuits with bounded bottom fanin. *To appear in the Proceedings of CCC*, 2013.

[7] V. Kabanets and R. Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *Computational Complexity*, 13(1-2):1–46, 2004.

[8] Z. Karnin, P. Mukhopadhyay, A. Shpilka, and I. Volkovich. Deterministic identity testing of depth 4 multilinear circuits with bounded top fan-in. In *Proceedings of the 42nd Annual STOC*, pages 649–658, 2010.

[9] Z. Karnin and A. Shpilka. Black box polynomial identity testing of generalized depth-3 arithmetic circuits with bounded top fan-in. In *In proceedings of 23rd Annual CCC*, pages 280–291, 2008.

[10] N. Kayal. Personal communication.

[11] N. Kayal and S. Saraf. Blackbox polynomial identity testing for depth 3 circuits. In *Proceedings of the 50th Annual FOCS*, pages 198–207, 2009.

[12] N. Kayal and N. Saxena. Polynomial identity testing for depth 3 circuits. *Computational Complexity*, 16(2):115–138, 2007.

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

[14] N. Nisan and A. Wigderson. Lower bounds on arithmetic circuits via partial derivatives. In *Proceedings of the 36th Annual FOCS*, pages 16–25, 1995.

[15] S. Saraf and I. Volkovich. Black-box identity testing of depth-4 multilinear circuits. In *Proceedings of the 43rd Annual STOC*, pages 421–430, 2011.

[16] N. Saxena and C. Seshadhri. From sylvester-gallai configurations to rank bounds: Improved black-box identity test for deph-3 circuits. In *Proceedings of the 51st Annual FOCS*, pages 21–30, 2010.

[17] N. Saxena and C. Seshadhri. Blackbox identity testing for bounded top-fanin depth-3 circuits: The field doesn't matter. *SIAM Journal on Computing*, 41(5):1285–1298, 2012.

[18] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of ACM*, 27(4):701–717, 1980.

[19] A. Shpilka and A. Wigderson. Depth-3 arithmetic circuits over fields of characteristic zero. *Computational Complexity*, 10(1):1–27, 2001.

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

[21] R. Zippel. Probabilistic algorithms for sparse polynomials. In *Symbolic and algebraic computation*, pages 216–226. 1979.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de