THEORY OF COMPUTING, Volume 13 (6), 2017, pp. 1–33
www.theoryofcomputing.org

SPECIAL ISSUE: CCC 2016

Arithmetic Circuits with Locally Low Algebraic Rank

Mrinal Kumar* Shubhangi Saraf†

Received April 30, 2016; Revised June 7, 2017; Published September 1, 2017

Abstract: In recent years, there has been a flurry of activity towards proving lower bounds for homogeneous depth-4 arithmetic circuits (Gupta et al., Fournier et al., Kayal et al., Kumar-Saraf), which has brought us very close to statements that are known to imply $\mathsf{VP} \neq \mathsf{VNP}$. It is open if these techniques can go beyond homogeneity, and in this paper we make progress in this direction by considering depth-4 circuits of *low algebraic rank*, which are a natural extension of homogeneous depth-4 arithmetic circuits.

A depth-4 circuit is a representation of an N-variate, degree-n polynomial P as

$$P = \sum_{i=1}^{T} Q_{i1} \cdot Q_{i2} \cdot \dots \cdot Q_{it} \ ,$$

where the Q_{ij} are given by their monomial expansion. Homogeneity adds the constraint that for every $i \in [T]$, $\sum_j \deg(Q_{ij}) = n$. We study an extension, where, for every $i \in [T]$,

A conference version of this paper appeared in the Proceedings of the Conference on Computational Complexity, 2016 [27].

*Research supported in part by NSF grant CCF-1253886 and by a Simons Graduate Fellowship.

†Research supported by NSF grant CCF-1350572.

ACM Classification: F.1.3

AMS Classification: 68Q15, 68Q17

Key words and phrases: algebraic rank, arithmetic circuits, hitting sets, lower bounds, non-homogeneous depth-4 circuits, partial derivatives, polynomial identity testing, projected shifted partials

 DOI: 10.4086/toc.2017.v013a006

the *algebraic rank* of the set $\{Q_{i1}, Q_{i2}, \ldots, Q_{it}\}$ of polynomials is at most some parameter k. We call this the class of $\Sigma\Pi^{(k)}\Sigma\Pi$ circuits. Already for $k = n$, these circuits are a strong generalization of the class of homogeneous depth-4 circuits, where in particular $t \leq n$ (and hence $k \leq n$).

We study lower bounds and polynomial identity tests for such circuits and prove the following results.

1. **Lower bounds.** We give an explicit family of polynomials $\{P_n\}$ of degree n in $N = n^{O(1)}$ variables in VNP, such that any $\Sigma\Pi^{(n)}\Sigma\Pi$ circuit computing P_n has size at least $\exp\left(\Omega(\sqrt{n}\log N)\right)$. This strengthens and unifies two lines of work: it generalizes the recent exponential lower bounds for *homogeneous* depth-4 circuits (Kayal et al. and Kumar-Saraf) as well as the Jacobian based lower bounds of Agrawal et al. which worked for $\Sigma\Pi^{(k)}\Sigma\Pi$ circuits in the restricted setting where $T \cdot k \leq n$.
2. **Hitting sets.** Let $\Sigma\Pi^{(k)}\Sigma\Pi^{[d]}$ be the class of $\Sigma\Pi^{(k)}\Sigma\Pi$ circuits with bottom fan-in at most d. We show that if d and k are at most $\mathrm{Poly}(\log N)$, then there is an explicit hitting set for $\Sigma\Pi^{(k)}\Sigma\Pi^{[d]}$ circuits of size quasipolynomially bounded in N and the size of the circuit. This strengthens a result of Forbes who constructed such quasipolynomial-size hitting sets in the setting where d and t are at most $\mathrm{Poly}(\log N)$.

A key technical ingredient of the proofs is a result which states that over any field of characteristic zero (or sufficiently large characteristic), up to a translation, every polynomial in a set of polynomials can be written as a function of the polynomials in a transcendence basis of the set. We believe this may be of independent interest. We combine this with methods based on shifted partial derivatives to obtain our final results.

1 Introduction

Arithmetic circuits are natural algebraic analogues of Boolean circuits, with the logical operations being replaced by sum and product operations over the underlying field. Valiant [44] developed the complexity theory for algebraic computation via arithmetic circuits and defined the complexity classes VP and VNP as the algebraic analogs of complexity classes P and NP respectively. We refer the interested reader to the survey by Shpilka and Yehudayoff [42] for more on arithmetic circuits.

Two of the most fundamental questions in the study of algebraic computation are the questions of *polynomial identity testing*(PIT)[1] and the question of proving *lower bounds* for explicit polynomials. It was shown by structural results known as *depth reductions* [2, 24, 43] that strong enough lower bounds or PIT results for just (homogeneous) depth-4 circuits, would lead to superpolynomial lower bounds and derandomized PIT for general circuits too. Consequently, depth-4 arithmetic circuits have been the focus of much investigation in the last few years.

Just in the last few years, we have seen rapid progress in proving lower bounds for homogeneous depth-4 arithmetic circuits, starting with the work of Gupta et al. [13] who proved exponential lower

[1]Given an arithmetic circuit, the problem is to decide if it computes the identically zero polynomial. In the whitebox setting we are allowed to look inside the wirings of the circuit, while in the blackbox setting, we can only query the circuit at some points.

bounds for homogeneous depth-4 circuits with bounded bottom fan-in and terminating with the results of Kayal et al. [18] and of the authors of this paper [29], which showed exponential lower bounds for general homogeneous depth-4 circuits. Any asymptotic improvement in the exponent of these lower bounds would lead to superpolynomial lower bounds for general arithmetic circuits.[2] Most of this progress was based on an understanding of the complexity measure of the family of *shifted partial derivatives* of a polynomial (this measure was introduced by Kayal [17]), and other closely related measures.

Although we now know how to use these measure to prove such strong lower bounds for homogeneous depth 4 circuits, the best known lower bounds for non-homogeneous depth three circuits over fields of characteristic zero are just cubic [41, 39, 21], and those for non-homogeneous depth-4 circuits over any field except $\mathbb{F}_2$ are just about superlinear [33]. It remains an extremely interesting question to get improved lower bounds for these circuit classes.

In sharp contrast to this state of knowledge on lower bounds, the problem of polynomial identity testing is very poorly understood even for depth three circuits. Till a few years ago, almost all the PIT algorithms known were for extremely restricted classes of circuits and were based on diverse proof techniques (for instance, [7, 23, 15, 22, 14, 37, 38, 36, 1, 10, 30]). The paper by Agrawal et al. [1] gave a unified proof of several of them.

It is a big question to go *beyond homogeneity* (especially for proving lower bounds) and in this paper we make progress towards this question by considering depth-4 circuits of *low algebraic rank*,[3] which are a natural extension of homogeneous depth-4 arithmetic circuits.

A depth-4 circuit is a representation of an N-variate, degree-n polynomial P as

$$P = \sum_{i=1}^{T} Q_{i1} \cdot Q_{i2} \cdots Q_{it}$$

where the Q_{ij} are given by their monomial expansion. Homogeneity adds the constraint that for every $i \in [T]$, $\sum_j \deg(Q_{ij}) = n$. We study an extension where, for every $i \in [T]$, the *algebraic rank* of the set $\{Q_{i1}, Q_{i2}, \ldots, Q_{it}\}$ of polynomials is at most some parameter k. We call this the class of $\Sigma\Pi^{(k)}\Sigma\Pi$ circuits. Already for $k = n$, these circuits are a strong generalization of the class of homogeneous depth-4 circuits, where in particular $t \leq n$ (and hence $k \leq n$).

We prove exponential lower bounds for $\Sigma\Pi^{(k)}\Sigma\Pi$ circuits for $k \leq n$ and give quasipolynomial time deterministic polynomial identity tests for $\Sigma\Pi^{(k)}\Sigma\Pi$ circuits when k and the bottom fan-in are bounded by $\mathrm{Poly}(\log N)$. All our results actually hold for a more general class of circuits, where the product gates at the second level can be replaced by an arbitrary circuits whose inputs are polynomials of algebraic rank at most k. In particular, our results hold for representations of a polynomial P as

$$P = \sum_{i=1}^{T} C_i \left(Q_{i1}, Q_{i2}, \ldots, Q_{it}\right)$$

where, for every $i \in [T]$, C_i is an arbitrary polynomial function of t inputs, and the algebraic rank of the set $\{Q_{i1}, Q_{i2}, \ldots, Q_{it}\}$ of polynomials is at most some parameter k.

[2] We refer the interested reader to the surveys of recent lower bounds results by Saptharishi [35, 34].

[3] The algebraic rank of a set of polynomials is the size of the maximal subset of this set which are algebraically independent. See Section 2 for formal definitions.

1.1 Some background and motivation

Before we more formally define the model and state our results, we give some background and motivation for studying this class of circuits.

Strengthening of the model of homogeneous depth-4 circuits. As already mentioned, we know very strong exponential lower bounds for homogeneous depth-4 arithmetic circuits. In contrast, for general (non-homogeneous) depth-4 circuits, we know only barely superlinear lower bounds, and it is a challenge to obtain improved bounds. $\Sigma\Pi^{(k)}\Sigma\Pi$ circuits with k as large as n (the degree of the polynomial being computed), which is the class we study in this paper, is already a significant strengthening of the model of homogeneous depth-4 circuits (since the intermediate degrees could be exponentially large). We provide exponential lower bounds for this model. Note that when $k = N$, $\Sigma\Pi^{(k)}\Sigma\Pi$ circuits would capture general depth-4 arithmetic circuits.

Low algebraic rank and lower bounds. In a recent paper, Agrawal et al. [1] studied the notion of circuits of low algebraic rank and by using the Jacobian to capture the notion of algebraic independence, they were able to prove exponential lower bounds for a certain class of arithmetic circuits.[4] They showed that over fields of characteristic zero, for any set $\{Q_1, Q_2, \ldots, Q_t\}$ of polynomials of sparsity at most s and algebraic rank k, any arithmetic circuit of the form $C(Q_1, Q_2, \ldots, Q_t)$ which computes the determinant polynomial for an $n \times n$ symbolic matrix must have $s \geq \exp(n/k)$. Note that if $k = \Omega(n)$, then the lower bound becomes trivial. The lower bounds in this paper strengthen these results in two ways.

1. Our lower bounds hold for a (potentially) richer class of circuits. In the model considered by [1], one imposes a global upper bound k on the rank of all the Q_i feeding into some polynomial C. In our model, we can take exponentially many different sets of polynomials Q_i, each with bounded rank, and apply some polynomial function to each of them and then take a sum.

2. Our lower bounds are stronger—we obtain exponential lower bounds even when k is as large as the degree of the polynomial being computed.

Algebraic rank and going beyond homogeneity. Even though we know exponential lower bounds for homogeneous[5] depth-4 circuits, the best known lower bounds for non-homogeneous depth-4 circuits are barely superlinear [33].

Grigoriev-Karpinski [11], Grigoriev-Razborov [12] and Shpilka-Wigderson [41] outlined a program based on "rank" to prove lower bounds for arithmetic circuits. They used the notion of "linear rank" and used it to prove lower bounds for depth-3 arithmetic circuits in the following way. Let $C = \sum_{i=1}^{T} \prod_{j=1}^{t} L_{ij}$ be a depth three (possibly nonhomogeneous) circuit computing a polynomial P of degree-n. Now, partition the inputs to the top sum gate to two halves, C_1 and C_2 based on the rank of the inputs feeding into it in the following way. For each $i \in [T]$, if the linear rank of the set $\{L_{ij} : j \in [t]\}$ of polynomials is at most k (for some threshold k), then include the gate i into the sum C_1, else include it into C_2. Therefore,

$$C = C_1 + C_2 .$$

[4] Even more significantly they also give efficient PIT algorithms for the same class of circuits.

[5] These results, in fact, hold for depth-4 circuits with not-too-large formal degree.

Their program had two steps.

1. Show that the subcircuit C_1 is *weak* with respect to some complexity measure, and thus prove a lower bound for C_1 (and hence C) when C_2 is trivial.

2. Also since C_2 is "high rank," show that there are many inputs for which C_2 is identically zero. Then try to look at restrictions over which C_2 is identically zero, and show that the lower bounds for C_1 continue to hold.

The following is the natural generalization of this approach to proving lower bounds for depth-4 circuits. Let $C = \sum_{i=1}^{T} \prod_{j=1}^{t} Q_{ij}$ be a depth-4 circuit computing a polynomial P of degree-n. Note that in general, the formal degree of C could be much larger than n. Now, we partition the inputs to the top sum gate to two halves, C_1 and C_2 based on the *algebraic rank* of the inputs feeding into it in the following way. For each $i \in [T]$, if the algebraic rank of the set $\{Q_{ij} : j \in [t]\}$ of polynomials is at most k (for some threshold k), then we include the gate i into the sum C_1 else we include it into C_2. Therefore,

$$C = C_1 + C_2 .$$

To implement the G-K, G-R and S-W program, as a first step one would show that the subcircuit C_1 is *weak* with respect to some complexity measure, and thus prove a lower bound for C_1 (and hence C) when C_2 is trivial. The second step would be to try to look at restrictions over which C_2 is identically zero, and show that the lower bounds for C_1 continue to hold.

For the case of depth-4 circuits, even the first step of proving lower bounds when C_2 is trivial was not known prior to this work (even for $k = 2$). Our results in this paper are an implementation of this first step, as we prove exponential lower bounds when the algebraic rank of inputs into each of the product gates is at most n (the degree of the polynomial being computed).

Connections to divisibility testing. Recently, Forbes [9] showed that given two sparse multivariate polynomials P and Q, the question of deciding if P divides Q can be reduced to the question of polynomial identity testing for $\Sigma\Pi^{(2)}\Sigma\Pi$ circuits. This question was one of the original motivations for this paper. Although we are unable to answer this question in general, we make some progress towards it by giving a quasipolynomial identity tests for $\Sigma\Pi^{(k)}\Sigma\Pi$ circuits when the various Q_{ij} feeding into the circuit have degree bounded by $\mathrm{Poly}(\log N)$ (and we are also able to handle k as large as $\mathrm{Poly}(\log N)$).

Low algebraic rank and PIT. Two very interesting PIT results which are also very relevant to the results in this paper are those of Beecken et al. [3] and those of Agrawal et al. [1]. The key idea explored in both these papers is that of algebraic independence. Together, they imply efficient deterministic PIT for polynomials which can be expressed in the form $C(Q_1, Q_2, \ldots, Q_t)$, where C is a circuit of polynomial degree and $Q_i's$ are either sparse polynomials or product of linear forms, such that the algebraic rank of $\{Q_1, Q_2, \ldots, Q_t\}$ is bounded.[6] This approach was extremely powerful as Agrawal et al. [1] demonstrate that they can use this approach to recover many of the known PIT results, which otherwise had very different proofs techniques. The PIT results of this paper hold for a variation of the model just described and we describe it in more detail in Section 1.3.3.

[6] See Section 2 for definitions.

Polynomials with low algebraic rank. In addition to potential applications to arithmetic circuit complexity, it seems an interesting mathematical question to understand the structure of a set of algebraically dependent polynomials. In general, our understanding of algebraic dependence is not as clear as our understanding of linear dependence. For instance, we know that if a set of polynomials is linearly dependent, then every polynomial in the set can be written as a linear combination of the polynomials in the basis. However, for higher degree dependencies (linear dependence is dependency of degree-1), we do not know any such clean statement. As a significant core of our proofs, we prove a statement of this flavor in Lemma 1.10.

We now formally define the model of computation studied in this paper, and then state and discuss our results.

1.2 Model of computation

We start with the definition of algebraic dependence. See Section 2 for more details.

Definition 1.1 (Algebraic independence and algebraic rank)**.** Let $\mathbb{F}$ be any field. A set

$$\mathcal{Q} = \{Q_1, Q_2, \ldots, Q_t\} \subseteq \mathbb{F}[X_1, X_2, \ldots, X_N]$$

of polynomials is said to be algebraically independent over $\mathbb{F}$ if there is no nonzero polynomial $R \in \mathbb{F}[Y_1, Y_2, \ldots, Y_t]$ such that $R(Q_1, Q_2, \ldots, Q_t)$ is identically zero.

A maximal subset of $\mathcal{Q}$ which is algebraically independent is said to be a transcendence basis of $\mathcal{Q}$ and the size of such a set is said to be the algebraic rank of $\mathcal{Q}$.

It is known that algebraic independence satisfies the Matroid property [31], and therefore the algebraic rank is well defined. We are now ready to define the model of computation.

Definition 1.2. Let $\mathbb{F}$ be any field. A $\Sigma\Pi^{(k)}\Sigma\Pi$ circuit C in N variables over $\mathbb{F}$ is a representation of an N-variate polynomial as

$$C = \sum_{i=1}^{T} Q_{i1} \cdot Q_{i2} \cdots Q_{it}$$

for some t, T such that for each $i \in [T]$, the algebraic rank of the set $\{Q_{ij} : j \in [t]\}$ of polynomials is at most k. Additionally, if for every $i \in [T]$ and $j \in [t]$, the degree of Q_{ij} is at most d, we say that C is a $\Sigma\Pi^{(k)}\Sigma\Pi^{[d]}$ circuit.

We will state all our results for $\Sigma\Pi^{(k)}\Sigma\Pi$ and $\Sigma\Pi^{(k)}\Sigma\Pi^{[d]}$ circuits. However, the results in this paper hold for a more general class of circuits where the product gates at the second level can be replaced by arbitrary polynomials. This larger class of circuits will be crucially used in our proofs and we define it formally below.

Definition 1.3. Let $\mathbb{F}$ be any field. A $\Sigma\Gamma^{(k)}\Sigma\Pi$ circuit C in N variables over $\mathbb{F}$ is a representation of an N-variate polynomial as

$$C = \sum_{i=1}^{T} \Gamma_i(Q_{i1}, Q_{i2}, \ldots, Q_{it})$$

for some t,T such that Γ_i is an arbitrary polynomial in t variables, and for each $i \in [T]$, the algebraic rank of the set $\{Q_{ij} : j \in [t]\}$ of polynomials is at most k. Additionally, if for every $i \in [T]$ and $j \in [t]$, the degree of Q_{ij} is at most d, we say that C is a $\Sigma\Gamma^{(k)}\Sigma\Pi^{[d]}$ circuit.

Definition 1.4 (Size of a circuit)**.** The *size* of a $\Sigma\Pi^{(k)}\Sigma\Pi$ or a $\Sigma\Gamma^{(k)}\Sigma\Pi$ circuit C is defined as the maximum of T and the number of monomials in the set

$$\left(\bigcup_{i\in[T],j\in[t]} \mathrm{Support}(Q_{ij}) \right).$$

Here for a polynomial Q, $\mathrm{Support}(Q)$ is the set of all monomials which appear with a non-zero coefficient in Q.

A $\Sigma\Pi^{(k)}\Sigma\Pi$ circuit C for which the polynomials $\{Q_{ij} : i \in [T], j \in [t]\}$ are homogeneous polynomials such that for every $i \in [T]$,

$$\sum_{j\in[t]} \deg(Q_{ij}) = \deg(P)$$

(where P is the polynomial being computed)[7] is the class of homogeneous depth-4 circuits. If we drop the condition of homogeneity, then in general the value of t could be much larger than $\deg(P)$ and the degrees of the Q_{ij} could be much larger than $\deg(P)$. Thus, the class of $\Sigma\Pi^{(k)}\Sigma\Pi$ circuits with k equaling the degree of the polynomial being computed could potentially be a larger class of circuits compared to that of homogeneous depth-4 circuits.

Also note that in the definition of $\Sigma\Pi^{(k)}\Sigma\Pi$ circuits, the bound on the algebraic rank is local for each $i \in [T]$, and in general, the algebraic rank of the entire set $\{Q_{ij} : i \in [T], j \in [t]\}$ can be as large as N.

1.3 Our results

We now state our results and discuss how they relate to other known results.

1.3.1 Lower bounds

As our first result, we give exponential lower bounds on the size of $\Sigma\Pi^{(k)}\Sigma\Pi$ circuits computing an explicit polynomial when the algebraic rank (k) is at most the degree (n) of the polynomial being computed.

Theorem 1.5. *Let $\mathbb{F}$ be any field of characteristic zero.*[8] *There exists a family $\{P_n\}$ of polynomials in* VNP*, such that P_n is a polynomial of degree-n in $N = n^{O(1)}$ variables with $0,1$ coefficients, and for any $\Sigma\Pi^{(k)}\Sigma\Pi$ circuit C, if $k \le n$ and if C computes P_n over $\mathbb{F}$, then*

$$\mathrm{Size}(C) \ge N^{\Omega(\sqrt{n})}.$$

[7] Observe that in this case, $k \le t \le \deg(P)$.

[8] Sufficiently large characteristic suffices.

Remark 1.6. From our proofs it follows that our lower bounds hold for the more general class of $\Sigma\Gamma^{(k)}\Sigma\Pi$ circuits, but for the sake of simplicity, we state our results in terms of $\Sigma\Pi^{(k)}\Sigma\Pi$ circuits. We believe it is likely that the lower bounds also hold for a polynomial in VP and it would be interesting to know if this is indeed true.[9]

Remark 1.7. Even though we state Theorem 1.5 for $k \leq n$, the proof goes through as long as k is any polynomial in n and N is chosen to be an appropriately large polynomial in n.

1.3.2 Comparison to known results

As we alluded to in the introduction, $\Sigma\Pi^{(k)}\Sigma\Pi$ circuits for $k \geq n$ subsume the class of homogeneous depth-4 circuits. Therefore, Theorem 1.5 subsumes the lower bounds for homogeneous depth-4 circuits [18, 29] for sufficiently large characteristic. Moreover, it also subsumes and generalizes the lower bounds of Agrawal et al. [1] since their lower bounds hold only if the algebraic rank of the entire set $\{Q_{ij} : i \in [T], j \in [t]\}$ of polynomials is bounded, while for Theorem 1.5, we only need upper bounds on the algebraic rank separately for every $i \in [T]$.

1.3.3 Polynomial identity tests

We show that there is a quasipolynomial size hitting set for all polynomials $P \in \Sigma\Pi^{(k)}\Sigma\Pi^{[d]}$ for *bounded* d and k. More formally, we prove the following theorem.

Theorem 1.8. *Let $\mathbb{F}$ be any field of characteristic zero.*[10] *Then, for every N, there exists a set $\mathcal{H} \subseteq \mathbb{F}^N$ such that*

$$|\mathcal{H}| \leq \exp(O(\log^{O(1)} N))$$

and for every nonzero N-variate polynomial P over $\mathbb{F}$ which is computable by a $\Sigma\Pi^{(k)}\Sigma\Pi^{[d]}$ circuit with $d,k \leq \log N$ and size $\mathrm{Poly}(N)$, there exists an $h \in \mathcal{H}$ such that $P(h) \neq 0$. Moreover, the set $\mathcal{H}$ can be explicitly constructed in time

$$\exp(O(\log^{O(1)} N)).$$

We now mention some remarks about Theorem 1.8.

Remark 1.9. It follows from our proof that the hitting set works for the more general class of $\Sigma\Gamma^{(k)}\Sigma\Pi^{[d]}$ circuits with $d,k \leq \log N$, size $\mathrm{Poly}(N)$ and formal degree at most $\mathrm{Poly}(N)$.

1.3.4 Comparison to known results

The two known results closest to our PIT result are the results of Forbes [9] and the results of Agrawal et al. [1]. Forbes [9] studies PIT for the case where the number of *distinct inputs* to the second level product gates in a depth-4 circuit with bounded bottom fan-in also bounded (which naturally also bounds the algebraic rank of the inputs), and constructs quasipolynomial-size hitting sets for this case. On the other hand, we handle the case where there is no restriction on the number of distinct inputs feeding into the

[9] More on this in Section 6.

[10] Sufficiently large characteristic suffices.

second level product gates, but we need to bound the bottom fan-in as well as the algebraic rank. In this sense, the results in this paper are a generalization of the results of Forbes [9].

Agrawal et al. [1] give a construction of polynomial-size hitting sets in the case when the total algebraic rank of the set $\{Q_{ij} : i \in [T], j \in [t]\}$ is bounded, but they can work with unbounded d. On the other hand, the size of our hitting set depends exponentially on d, but requires only local algebraic dependencies for every $i \in [T]$. So, these two results are not comparable, although there are similarities in the sense that both of them aim to use the algebraic dependencies in the circuit. In general, summation is a tricky operation with respect to designing PIT algorithms (as opposed to multiplication), so it is not clear if the ideas in the work of Agrawal et al. [1] can be somehow adapted to prove Theorem 1.8.

1.3.5 From algebraic dependence to functional dependence

Our lower bounds and PIT results crucially use the following lemma, which (informally) shows that over fields of characteristic zero, up to a translation, every polynomial in a set of polynomials can be written as a *function* of the polynomials in *transcendence basis*.[11] We now state the lemma precisely.

Lemma 1.10 (Algebraic dependence to functional dependence)**.** *Let $\mathbb{F}$ be any field of characteristic zero or sufficiently large positive characteristic. Let $\mathcal{Q} = \{Q_1, Q_2, \ldots, Q_t\}$ be a set of polynomials in N variables such that the algebraic rank of $\mathcal{Q}$ equals k. Let $d_i = \deg(Q_i)$ $(i \in [t])$ and let $\mathcal{B} = \{Q_1, Q_2, \ldots, Q_k\}$ be a maximal algebraically independent subset of $\mathcal{Q}$. Then, there exists an $\overline{a} = (a_1, a_2, \ldots, a_N)$ in $\mathbb{F}^N$ and polynomials $F_{k+1}, F_{k+2}, \ldots, F_t$ in k variables such that $\forall i \in \{k+1, k+2, \ldots, t\}$*

$$Q_i(\overline{X} + \overline{a}) = \mathsf{Hom}^{\le d_i}\left[F_i(Q_1(\overline{X} + \overline{a}), Q_2(\overline{X} + \overline{a}), \ldots, Q_k(\overline{X} + \overline{a}))\right] .$$

Here, for any polynomial P, we use $\mathsf{Hom}^{\le i}[P]$ to refer to the sum of homogeneous components of P of degree at most i.[12]

Even though the lemma seems a very basic statement about the structure of algebraically dependent polynomials, to the best of our knowledge this was not known before. The proof builds upon a result on the structure of roots of multivariate polynomials by Dvir et al. [8]. Observe that for *linear* dependence, the statement analogous to that of Lemma 1.10 is trivially true. We believe that this lemma might be of independent interest (in addition to its applications in this paper).

In fact, the lemma holds for a random choice of the vector $\overline{a}$ chosen uniformly from a large enough grid in $\mathbb{F}^N$.

Remark 1.11. In a recent result, Pandey et al. [32] show that this connection between algebraic dependence and functional dependence continues to hold over fields of small characteristic. Consequently, they show that the results of this paper also hold over fields of small characteristic.

[11] A transcendence basis of a set of polynomials is a maximal subset of the polynomials with the property that its elements are algebraically independent. For more on this see Section 2.

[12] For a more precise definition see Definition 2.2.

1.4 Proof overview

Even though the results in this paper seem related to the results in [1] (both exploiting some notion of low algebraic rank), the proof strategy and the way algebraic rank is used are quite different. We now briefly outline our proof strategy.

We first discuss the overview of proof for our lower bound.

Let P_n be the degree-n polynomial we want to compute, and let C be a $\Sigma\Pi^{(k)}\Sigma\Pi$ circuit computing it, with $k = n$. Then C can be represented as

$$C = \sum_{i=1}^{T} \prod_{j=1}^{t} Q_{ij} .$$

From definitions, we know that for every $i \in [T]$, the algebraic rank of the set $\{Q_{i1}, Q_{i2}, \dots, Q_{it}\}$ of polynomials is at most $k (= n)$. We want to give a lower bound on the size of C.

Instead of proving our result directly for $\Sigma\Pi^{(k)}\Sigma\Pi$ circuits, it will be very useful for us to go to the significantly strengthened class of $\Sigma\Gamma^{(k)}\Sigma\Pi$ circuits and prove our result for that class. Thus we think of our circuit C as being expressed as

$$C = \sum_{i=1}^{T} C_i(Q_{i1}, Q_{i2}, \dots, Q_{it})$$

where the C_i can be arbitrary polynomial functions of the inputs feeding into them. Note that we define the size of a $\Sigma\Gamma^{(k)}\Sigma\Pi$ circuit to be the maximum of the top fan-in T, and the maximum of the number of monomials in any of the polynomials Q_{ij} feeding into the circuit. Thus we completely disregard the complexities of the various polynomial function gates at the second level. If we are able to prove a lower bound for this notion of size, then if the original circuit is actually a $\Sigma\Pi^{(k)}\Sigma\Pi$ circuit then it will also be as good a lower bound for the usual notion of size.

Our lower bound has two key steps. In the first step we prove the result in the special case where $t \leq n^2$. In the second step we show how to "almost" reduce to the case of $t \leq n^2$.

Step (1) : $t \leq n^2$. In the representation of C as a $\Sigma\Gamma^{(k)}\Sigma\Pi$ circuit, the value of t is at most n^2. Lower bounds for this case turn out to be similar to lower bounds for homogeneous depth-4 circuits. In this case we borrow ideas from prior works [13, 18, 29] and show that the *dimension of projected shifted partial derivatives of* C is not too large. Most importantly, we can use the chain rule for partial derivatives to obtain good bounds for this complexity measure, independent of the complexity of the various C_i.

Recall however that in our final result, t can be actually much larger than n^2. Indeed the circuit C can be very far from being homogeneous, and for general depth-4 circuits, we do not know good upper bounds on the complexity of shifted partial derivatives or projected shifted partial derivatives. Also, in general, it is not clear if these measures are really small for general depth-4 circuits.[13] It is here that the low algebraic rank of $\{Q_{i1}, Q_{i2}, \dots, Q_{it}\}$ proves to be useful, and that brings us to the crux of our argument.

[13] Indeed, as an earlier result of the authors [26] shows, even homogeneous depth-4 circuits can have very large shifted partial derivative complexity.

Step (2) : Reducing to the case where $t \le n^2$. A key component of our proof, which is formalized in Lemma 3.5 shows that over any field of characteristic zero (or sufficiently large characteristic), up to a translation, every polynomial in a set of polynomials can be written as a function of the homogeneous components of the polynomials in the transcendence basis.

More formally, there exists an $\overline{a} \in \mathbb{F}^N$ such that $C(\overline{X}+\overline{a})$ can be expressed as

$$C(\overline{X}+\overline{a}) = \sum_{i=1}^{T} C'_i(\mathsf{Hom}[Q_{i1}(\overline{X}+\overline{a})], \mathsf{Hom}[Q_{i2}(\overline{X}+\overline{a})], \ldots, \mathsf{Hom}[Q_{ik}(\overline{X}+\overline{a})])$$

where for a degree-d polynomial F, $\mathsf{Hom}[F]$ denotes the $d+1$-tuple of homogeneous components of F. Moreover, $Q_{i1}, Q_{i2}, \ldots, Q_{ik}$ are the polynomials in the transcendence basis.

The crucial gain in the above transformation is that the arity of each of the polynomials C'_i is $(d+1) \times k$ and not t (where d is an upper bound on the degrees of the Q_{ij}). Now by assumption $k \le n$, and moreover without loss of generality we can assume $d \le n$ since homogeneous components of Q_{ij} of degree larger than n can be dropped since they do not contribute to the computation of a degree-n polynomial. Thus we have essentially reduced to the case where $t \le n^2$.

One loss by this transformation is that the polynomials $\{C'_i\}$ might be much more complex and with much higher degrees than the original polynomials $\{C_i\}$. However this will not affect the computation of our complexity measure. Another loss is that we have to deal with the translated polynomial $C(\overline{X}+\overline{a})$. This introduces some subtleties into our computation as it could be that $Q_{ij}(\overline{X})$ is a sparse polynomial but $Q_{ij}(\overline{X}+\overline{a})$ is far from being sparse. Neither of these issues is very difficult to deal with, and we are able to get strong bounds for the measure, based on projected shifted partial derivatives, for such circuits. The proof of Lemma 3.5 essentially follows from Lemma 1.10.

The proof of Lemma 1.10 crucially uses a result of Dvir, Shpilka and Yehudayoff [8] which shows that up to some minor technical conditions (which are not very hard to satisfy), factors of a polynomial $f \in \mathbb{F}[X_1, X_2, \ldots, X_N, Y]$ of the form $Y - p(X_1, X_2, \ldots, X_N)$ where $p \in \mathbb{F}[X_1, X_2, \ldots, X_N]$ can be expressed as polynomials in the coefficients when viewing f as an element of $\mathbb{F}[X_1, X_2, \ldots, X_N][Y]$. This is relevant since if a set of t polynomials is algebraically dependent, then there is a non-zero t-variate polynomial which vanishes when composed with this tuple. We use this *vanishing* to prove the lemma.

The PIT results follows a similar initial setup and use of Lemma 1.10. We then use a result of Forbes [9] to show that the polynomial computed by C has a monomial of small support, which is then detected using the standard idea of using Shpilka-Volkovich generators [40].

1.5 Organization of the paper

The rest of the paper is organized as follows. In Section 2, we state some preliminary definitions and results that are used elsewhere in the paper. In Section 3, we describe our use of low algebraic rank and prove Lemma 3.5. We prove Theorem 1.5 in Section 4 and Theorem 1.8 in Section 5. We end with some open questions in Section 6.

2 Preliminaries

In this section we introduce some notation and definitions for the rest of the paper.

2.1 Notation

1. For an integer i, we denote the set $\{1,2,\ldots,i\}$ by $[i]$.
2. By $\overline{X}$, we mean the set $\{X_1,X_2,\ldots,X_N\}$ of variables.
3. For a field $\mathbb{F}$, we use $\mathbb{F}[\overline{X}]$ to denote the ring of all polynomials in $X_1,X_2,\ldots,X_N$ over the field $\mathbb{F}$. For brevity, we denote a polynomial $P(X_1,X_2,\ldots,X_N)\in\mathbb{F}[\overline{X}]$ by $P(\overline{X})$.
4. The support of a monomial α is the set of variables which appear with a non-zero exponent in α.
5. We say that a function $f(N)$ is quasipolynomially bounded in N if there exists a positive absolute constant c, such that for all N sufficiently large, $f(N) < \exp(\log^c N)$. For brevity, if f is quasipolynomially bounded in N, we say that f is quasipolynomial in N.
6. In this paper, unless otherwise stated, $\mathbb{F}$ is a field of characteristic zero.
7. Given a polynomial P and a valid monomial ordering Π, the leading monomial of P is the monomial with a nonzero coefficient in P which is maximal according to Π. Similarly, the trailing monomial in P is the monomial which is minimal among all monomials in P according to Π.
8. All our logarithms are to the base e.

2.2 Algebraic independence

We formally defined the notion of algebraic independence and algebraic rank in Definition 1.1. For more on algebraic independence and related discussions, we refer the reader to the excellent survey by Chen, Kayal and Wigderson [4] and earlier papers [3, 1].

For a tuple $\mathcal{Q}=(Q_1,Q_2,\ldots,Q_t)$ of algebraically dependent polynomials, we know that there is a nonzero t-variate polynomial R (called a $\mathcal{Q}$-annihilating polynomial) such that $R(Q_1,Q_2,\ldots,Q_t)$ is identically zero. A natural question is to ask, what kind of bounds on the degree of R can we show, in terms of the degrees of Q_i. The following lemma of Kayal [16] gives an upper bound on the degree of annihilating polynomials of a set of degree-d polynomials. The bound is useful to us in our proof.

Lemma 2.1 (Kayal [16]). *Let $\mathbb{F}$ be a field and let $\mathcal{Q}=\{Q_1,Q_2,\ldots,Q_t\}$ be a set of polynomials of degree-d in N variables over the field $\mathbb{F}$ having algebraic rank k. Then there exists a $\mathcal{Q}$-annihilating polynomial of degree at most $(k+1)\cdot d^k$.*

2.3 Complexity of homogeneous components

We start by defining the homogeneous components of a polynomial.

Definition 2.2. For a polynomial P and a positive integer i, we represent by $\mathsf{Hom}^i[P]$, the homogeneous component of P of degree equal to i. By extension, we define $\mathsf{Hom}^{\leq i}[P]$ and $\mathsf{Hom}^{\geq i}[P]$ as follows.

$$\mathsf{Hom}^{\leq i}[P] \equiv \sum_{j=0}^{i} \mathsf{Hom}^{j}[P] .$$

$$\mathsf{Hom}^{\geq i}[P] \equiv \sum_{j=i}^{\deg(P)} \mathsf{Hom}^{j}[P] .$$

We define $\mathsf{Hom}[P]$ as the ordered tuple of homogeneous components of P, i. e.,

$$\mathsf{Hom}[P] \equiv \left(\mathsf{Hom}^{d}[P], \mathsf{Hom}^{d-1}[P], \dots, \mathsf{Hom}^{0}[P] \right) ,$$

where d is the degree of P.

We will use the following simple lemma whose proof is fairly standard using interpolation, and can be found in the paper [28], for instance. We sketch the proof here for completeness.

Lemma 2.3. *Let $\mathbb{F}$ be a field of characteristic zero, and let $P \in \mathbb{F}[X_1, X_2, \dots, X_N]$ be a polynomial of degree at most d, in N variables, such that P can be represented as*

$$P = C(Q_1, Q_2, \dots, Q_t) ,$$

where for every $j \in [t]$, Q_j is a polynomial in N variables, and C is an arbitrary polynomial in t variables. Then, there exist polynomials $\{Q'_{ij} : i \in [d+1], j \in [t]\}$, and for every ℓ such that $0 \leq \ell \leq d$, there exist polynomials $C'_{\ell,1}, C'_{\ell,2}, \dots, C'_{\ell,d+1}$ satisfying

$$\mathsf{Hom}^{\ell}[P] = \sum_{i=1}^{(d+1)} C'_{\ell,i}(Q'_{i1}, Q'_{i2}, \dots, Q'_{it}) .$$

Moreover,

- *if each of the polynomials in the set $\{Q_j : j \in [t]\}$ is of degree at most Δ, then every polynomial in the set $\{Q'_{ij} : i \in [d+1], j \in [t]\}$ is also of degree at most Δ;*
- *if the algebraic rank of the set $\{Q_j : j \in [t]\}$ of polynomials is at most k, then for every $i \in [d+1]$, the algebraic rank of the set $\{Q'_{ij} : j \in [t]\}$ of polynomials is also at most k.*

Proof. The key idea is to start from $P \in \mathbb{F}[\overline{X}]$ and obtain a new polynomial $P' \in \mathbb{F}[\overline{X}][Z]$ such that for every ℓ such that $0 \leq \ell \leq d$, the coefficient of Z^{ℓ} in P' equals $\mathsf{Hom}^{\ell}[P]$. Here, Z is a new variable. Such a P' is obtained by replacing every occurrence of the variable X_j (for each $j \in [N]$) in P by $Z \cdot X_j$. It is not hard to verify that such a P' has the stated property. We now view P' as a univariate polynomial in Z with the coefficients coming from $\mathbb{F}(\overline{X})$. Notice that the degree of P' in Z is at most d. So, to recover the coefficients of a univariate polynomial of degree at most d, we can evaluate P' at $d+1$ distinct values of Z over $\mathbb{F}(\overline{X})$ and take an $\mathbb{F}(\overline{X})$ linear combination. In fact, if the field $\mathbb{F}$ is large enough, we can assume that all these distinct values of Z lie in the base field $\mathbb{F}$ and we only take an $\mathbb{F}$ linear combination. The properties in the "moreover" part of the lemma immediately follow from this construction, and we skip the details. $\square$

2.4 Roots of polynomials

We will crucially use the following result of Dvir, Shpilka, Yehudayoff [8].

Lemma 2.4 (Lemma 3.1 in Dvir, Shpilka, Yehudayoff [8]). *For a field $\mathbb{F}$, let $P \in \mathbb{F}[X_1, X_2, \ldots, X_N, Y]$ be a non-zero polynomial of degree at most k in Y. Let $f \in \mathbb{F}[X_1, X_2, \ldots, X_N]$ be a polynomial such that $P(X_1, X_2, \ldots, X_N, f) = 0$ and $\frac{\partial P}{\partial Y}(0, 0, \ldots, 0, f(0, 0, \ldots, 0)) \neq 0$. Let*

$$P = \sum_{i=0}^{k} C_i(X_1, X_2, \ldots, X_N) \cdot Y^i .$$

Then, for every $t \geq 0$, there exists a polynomial $R_t \in \mathbb{F}[Z_1, Z_2, \ldots, Z_{k+1}]$ of degree at most t such that

$$\mathsf{Hom}^{\leq t}[f(X_1, X_2, \ldots, X_N)] = \mathsf{Hom}^{\leq t}[R_t(C_0, C_1, \ldots, C_k)] . \tag{2.1}$$

We also use the following standard result about zeroes of polynomials.

Lemma 2.5 (Schwartz, Zippel, DeMillo, Lipton [5]). *Let P be a non-zero polynomial of degree-d in N variables over a field $\mathbb{F}$. Let S be an arbitrary subset of $\mathbb{F}$, and let $x_1, x_2, \ldots, x_N$ be random elements from S chosen independently and uniformly at random. Then*

$$\Pr[P(x_1, x_2, \ldots, x_N) = 0] \leq \frac{d}{|S|} .$$

The following corollary easily follows from the lemma above.

Corollary 2.6. *Let $P_1, P_2, \ldots, P_t$ be non-zero polynomials of degree-d in N variables over a field $\mathbb{F}$. Let S be an arbitrary subset of $\mathbb{F}$ of size at least $2td$, and let $x_1, x_2, \ldots, x_N$ be random elements from S chosen independently and uniformly at random. Then*

$$\Pr[\forall i \in [t], P_i(x_1, x_2, \ldots, x_N) \neq 0] \geq \frac{1}{2} .$$

2.5 Approximations

We will use the following lemma of Saptharishi [35] for numerical approximations in our calculations.

Lemma 2.7 (Saptharishi [35]). *Let n and ℓ be parameters such that $\ell = (n/2)(1-\varepsilon)$ for some $\varepsilon = o(1)$. For any a, b such that $a, b = O(\sqrt{n})$,*

$$\binom{n-a}{\ell-b} = \binom{n}{\ell} \cdot 2^{-a} \cdot (1+\varepsilon)^{a-2b} \cdot \exp(O(b \cdot \varepsilon^2)) .$$

3 Utilizing low algebraic rank

Let $\mathcal{Q} = \{Q_1, Q_2, \ldots, Q_t\}$ be a set of polynomials in N variables and degree at most d such that the algebraic rank of $\mathcal{Q}$ equals k. Without loss of generality, let us assume that $\mathcal{B} = \{Q_1, Q_2, \ldots, Q_k\}$ are an algebraically independent subset of $\mathcal{C}$ of maximal size. We now show that, in some sense, this implies that all the polynomials in $\mathcal{Q}$ can be represented as functions of polynomials in the set $\mathcal{B}$. We make this notion formal in the lemma below, which is a restatement of Lemma 1.10.

Lemma 3.1 (Lemma 1.10 restated)**.** *Let $\mathbb{F}$ be any field of characteristic zero or sufficiently large. Let $\mathcal{Q} = \{Q_1, Q_2, \ldots, Q_t\}$ be a set of polynomials in N variables such that the algebraic rank of $\mathcal{Q}$ equals k. Let $d_i = \deg(Q_i)$ ($i \in [t]$) and let $\mathcal{B} = \{Q_1, Q_2, \ldots, Q_k\}$ be a maximal algebraically independent subset of $\mathcal{Q}$. Then, there exists an $\overline{a} = (a_1, a_2, \ldots, a_N)$ in $\mathbb{F}^N$ and polynomials $F_{k+1}, F_{k+2}, \ldots, F_t$ in k variables such that $\forall i \in \{k+1, k+2, \ldots, t\}$*

$$Q_i(\overline{X} + \overline{a}) = \mathsf{Hom}^{\leq d_i}\left[F_i(Q_1(\overline{X} + \overline{a}), Q_2(\overline{X} + \overline{a}), \ldots, Q_k(\overline{X} + \overline{a}))\right] .$$

Proof. Let d be defined as $\max_i\{d_i\}$. Let us consider any i such that $i \in \{k+1, k+2, \ldots, t\}$. From the statement of the lemma, it follows that the set of polynomials in the set $\mathcal{B} \cup \{Q_i\}$ are algebraically dependent. Therefore, there exists a nonzero polynomial A_i in $k+1$ variables such that $A_i(Q_1, Q_2, \ldots, Q_k, Q_i) \equiv 0$. Without loss of generality, we choose such a polynomial with the smallest total degree. From the upper bound on the degree of the annihilating polynomial from Lemma 2.1, we can assume that the degree of A_i is at most $(k+1)d^k$. Consider the polynomial $A_i'(\overline{X}, Y)$ defined by

$$A_i'(\overline{X}, Y) = A_i(Q_1(\overline{X}), Q_2(\overline{X}), \ldots, Q_k(\overline{X}), Y) .$$

We have the following observation about properties of A_i'.

Observation 3.2. A_i' satisfies the following conditions.

- A_i' is not identically zero.
- The Y degree of A_i' is at least one.
- $Q_i(\overline{X})$ is a root of the polynomial A_i', when viewing it as a polynomial in the Y variable with coefficients coming from $\mathbb{F}(\overline{X})$.

Proof. We prove the items in sequence.

- If A_i' is identically zero, then it follows that $Q_1, Q_2, \ldots, Q_k$ are algebraically dependent, which is a contradiction.
- If $A_i'(\overline{X}, Y)$ does not depend on the variable Y, then by definition, it follows that $A_i(Q_1, Q_2, \ldots, Q_k, Y)$ does not depend on Y. Hence, $A_i(Q_1, Q_2, \ldots, Q_k, Q_i)$ does not depend on Q_i but is identically zero. This contradicts the algebraic independence of $Q_1, Q_2, \ldots, Q_k$.
- This item follows from the fact that the polynomial obtained by substituting Y by Q_i in A_i' equals $A_i(Q_1, Q_2, \ldots, Q_k, Q_i)$, which is identically zero. □

Our aim now is to invoke Lemma 2.4 for the polynomial A'_i, but first, we need to verify that the conditions in the hypothesis of Lemma 2.4 are satisfied. Let the polynomial A''_i be defined as the first order derivative of A'_i with respect to Y. Formally,

$$A''_i = \frac{\partial A'_i}{\partial Y}.$$

We proceed with the following claim, the proof of which we defer to the end.

Claim 3.3. *The polynomial A''_i is not an identically zero polynomial and $A''_i|_{Y=Q_i}$ is not identically zero.*

For the ease of notation, we define

$$L_i(\overline{X}) = A''_i|_{Y=Q_i}.$$

Observe that L_i is a polynomial in the variables $\overline{X}$ which is not identically zero and is of degree at most $(k+1)d^{k+1}$. Let H be a subset of $\mathbb{F}$ of size $2t(k+1)d^{k+1}$. Then, for a uniformly random point $\overline{a}_i$ picked from H^N, the probability that L_i vanishes at $\overline{a}_i$ is at most $1/2t$. We call the set of all points $\overline{a}_i \in H^N$ where L_i vanishes as bad. Then, with a probability at least $1-1/2t$, a uniformly random element of H^N is not bad. Let $\overline{a}_i \in \mathbb{F}^N$ be a "not bad" element. We can replace X_j by $X_j + \gamma$, where γ is the j^{th} coordinate of a_i and then for the resulting polynomial $L_i(\overline{X}+\overline{a}_i)$, the point $(0,0,\dots,0)$ is not bad.

We are now ready to apply Lemma 2.4. Let

$$A'_i(\overline{X},Y) = \sum_{j=0}^{(k+1)d^k} C_j(\overline{X}) \cdot Y^j.$$

Here, for every j, $C_j(\overline{X}) = C'_j\left(Q_1(\overline{X}), Q_2(\overline{X}), \dots, Q_k(\overline{X})\right)$ is a polynomial in the $\overline{X}$ variables and is the coefficient of Y^j in $A'_i(\overline{X},Y)$ when viewed as an element of $\mathbb{F}[\overline{X}][Y]$. From the discussion above, we know that the following are true.

1. The polynomial $A'_i(\overline{X}+\overline{a}_i, Q_i(\overline{X}+\overline{a}_i))$ is identically zero.
2. The first derivative of $A'_i(\overline{X}+\overline{a}_i, Y)$ with respect to Y does not vanish at $(0,0,\dots,0,Q_i(0,0,\dots,0))$.

Therefore, by Lemma 2.4, it follows that there is a polynomial G_i such that

$$Q_i(\overline{X}+\overline{a}_i) = \mathsf{Hom}^{\leq d_i}\left[G_i(C_0(\overline{X}+\overline{a}_i), C_1(\overline{X}+\overline{a}_i), \dots, C_{(k+1)d^k}(\overline{X}+\overline{a}_i))\right].$$

We also know that for every $j \in \{0,1,\dots,(k+1)d^k\}$, $C_j(\overline{X}+\overline{a}_i)$ is a polynomial in the polynomials $Q_1(\overline{X}+\overline{a}_i), Q_2(\overline{X}+\overline{a}_i), \dots, Q_k(\overline{X}+\overline{a}_i)$. In other words,

$$Q_i(\overline{X}+\overline{a}_i) = \mathsf{Hom}^{\leq d_i}\left[F_i(Q_1(\overline{X}+\overline{a}_i), Q_2(\overline{X}+\overline{a}_i), \dots, Q_k(\overline{X}+\overline{a}_i))\right]$$

for a polynomial F_i.

In order to prove the lemma for all values of $i \in \{k+1, k+2, \dots, t\}$, we observe that we can pick a single value of the translation $\overline{a}$, which works for every $i \in \{k+1, k+2, \dots, t\}$. Such an $\overline{a}$ exists because the probability that a uniformly random $p \in H^N$ is bad for some i is at most $t \cdot 1/2t = 1/2$ and the translation corresponding to any such element $\overline{a}$ in H^N which is not bad for every i will work. The statement of the lemma then immediately follows. $\square$

We now prove Claim 3.3.

Proof of Claim 3.3. We observed from the second item in Observation 3.2 that the degree of Y in A_i' is at least 1. Hence, A_i'' is not identically zero. If $A_i''|_{Y=Q_i}$ is identically zero, then it follows that $\{Q_1, Q_2, \ldots, Q_k, Q_i\}$ have an annihilating polynomial of degree smaller than the degree of A_i, which is a contradiction to the choice of A_i, as a minimum degree annihilating polynomial. □

Lemma 3.1 lets us express all polynomials in a set of polynomials as a function of the polynomials in the transcendence basis. However, the functional form obtained is slightly cumbersome for us to use in our applications. We now derive the following corollary, which is easier to use in our applications.

Corollary 3.4. *Let $\mathbb{F}$ be any field of characteristic zero or sufficiently large. Let $\mathcal{Q} = \{Q_1, Q_2, \ldots, Q_t\}$ be a set of polynomials in N variables such that the for every $i \in [t]$, the degree of Q_i is equal to $d_i < d$ and the algebraic rank of $\mathcal{Q}$ equals k. Let $\mathcal{B} = \{Q_1, Q_2, \ldots, Q_k\}$ be a maximal algebraically independent subset of $\mathcal{Q}$. Then, there exists an $\overline{a} = (a_1, a_2, \ldots, a_N)$ in $\mathbb{F}^N$ and polynomials $F_{k+1}, F_{k+2}, \ldots, F_t$ in at most $k(d+1)$ variables such that $\forall i \in \{k+1, k+2, \ldots, t\}$*

$$Q_i(\overline{X}+\overline{a}) = F_i(\mathsf{Hom}[Q_1(\overline{X}+\overline{a})], \mathsf{Hom}[Q_2(\overline{X}+\overline{a})], \ldots, \mathsf{Hom}[Q_k(\overline{X}+\overline{a})]) .$$

Proof. Let i be such that $i \in \{k+1, k+2, \ldots, t\}$. From Lemma 3.1, we know that there exists an $\overline{a} \in \mathbb{F}^N$ and a polynomial W_i such that

$$Q_i(\overline{X}+\overline{a}) = \mathsf{Hom}^{\leq d_i}\left[W_i(Q_1(\overline{X}+\overline{a}), Q_2(\overline{X}+\overline{a}), \ldots, Q_k(\overline{X}+\overline{a}))\right] . \tag{3.1}$$

We will now show that $\mathsf{Hom}^{\leq d_i}\left[W_i(Q_1(\overline{X}+\overline{a}), Q_2(\overline{X}+\overline{a}), \ldots, Q_k(\overline{X}+\overline{a}))\right]$ is actually a polynomial in the homogeneous components of the various $Q_j(\overline{X}+\overline{a})$ by the following procedure, which is essentially univariate polynomial interpolation.

- Let $R(\overline{X}) = W_i(Q_1(\overline{X}+\overline{a}), Q_2(\overline{X}+\overline{a}), \ldots, Q_k(\overline{X}+\overline{a}))$. We replace every variable X_j in R by $Z \cdot X_j$ for a new variable Z. We view the resulting polynomial R' as an element of $\mathbb{F}(\overline{X})[Z]$, i. e., a univariate polynomial in Z with coefficients coming from the field of rational functions in the $\overline{X}$ variables.

- Now, observe that for any ℓ, the homogeneous component of degree-ℓ of R is precisely the coefficient of Z^ℓ in R'. Hence, we can evaluate R' for sufficiently many distinct values of Z in $\mathbb{F}(\overline{X})$, and then take an $\mathbb{F}(\overline{X})$ linear combination of these evaluations to express the homogeneous components. Moreover, since $\mathbb{F}$ is an infinite field, without loss of generality, we can pick the values of Z to be scalars in $\mathbb{F}$, and in this case, we will just be taking an $\mathbb{F}$ linear combination.

The catch here is that after replacing X_j by $Z \cdot X_j$ and substituting different values of $Z \in \mathbb{F}$, the polynomials $Q_{i'}(\overline{X}+\overline{a})$ could possibly lead to distinct polynomials. In general, this is bad, since our goal is to show that every polynomial in a set of algebraically dependent polynomials in a function of *few* polynomials. However, the following observation comes to our rescue. Let P be any polynomial in $\mathbb{F}[\overline{X}]$ of degree-Δ and let P' be the polynomial obtained from P by replacing X_j by $Z \cdot X_j$. Then,

$$P'(\overline{X}+\overline{a}) = \sum_{\ell=0}^{\Delta} Z^\ell \cdot \mathsf{Hom}^\ell[P(\overline{X}+\overline{a})] . \tag{3.2}$$

In particular, the set of polynomials obtained from P' for different values of Z are all in the linear span of homogeneous components of P.

Therefore, any homogeneous component of R can be expressed as a function of the set

$$\bigcup_{i=1}^{k} \mathsf{Hom}\left[Q_i(\overline{X}+\overline{a})\right]$$

of polynomials. This completes the proof of the corollary. □

We now prove the following lemma, which will be directly useful in the our applications to polynomial identity testing and lower bounds in the following sections.

Lemma 3.5. *Let $\mathbb{F}$ be any field of characteristic zero or sufficiently large. Let $P \in \mathbb{F}[\overline{X}]$ be a polynomial in N variables, of degree equal to n, such that P can be represented as*

$$P = \sum_{i=1}^{T} F_i(Q_{i1}, Q_{i2}, \ldots, Q_{it})$$

and such that the following are true.

- *For each $i \in [T]$, F_i is a polynomial in t variables.*
- *For each $i \in [T]$ and $j \in [t]$, Q_{ij} is a polynomial in N variables of degree at most d.*
- *For each $i \in [T]$, the algebraic rank of the set $\{Q_{ij} : j \in [t]\}$ of polynomials is at most k and $\mathcal{B}_i = \{Q_{i1}, Q_{i2}, \ldots, Q_{ik}\}$ is a maximal algebraically independent subset of $\{Q_{ij} : j \in [t]\}$.*

Then, there exists an $\overline{a} \in \mathbb{F}^N$ and polynomials F_i' in at most $k(d+1)$ variables such that

$$P(\overline{X}+\overline{a}) = \sum_{i=1}^{T} F_i'(\mathsf{Hom}[Q_{i1}(\overline{X}+\overline{a})], \mathsf{Hom}[Q_{i2}(\overline{X}+\overline{a})], \ldots, \mathsf{Hom}[Q_{ik}(\overline{X}+\overline{a})])\,.$$

Proof. The proof would essentially follow from the application of Corollary 3.4 to each of the summands on the right hand side. The only catch is that the translations $\overline{a}$ could be different for each one of them. Since we are working over infinite fields, without loss of generality, we can assume that there is a good translation $\overline{a}$ which works for all the summands. □

4 Application to lower bounds

In this section , we prove Theorem 1.5. But, first we discuss the definitions of the complexity measure used in the proof, the notion of random restrictions and the family of hard polynomials that we work with.

4.1 Projected shifted partial derivatives

The complexity measure that we use to prove the lower bounds in this paper is the notion of *projected shifted partial derivatives* of a polynomial introduced by Kayal et al. in [18] and subsequently used in a number of following papers [29, 19, 28].

For a polynomial P and a monomial γ, $\frac{\partial P}{\partial \gamma}$ is the partial derivative of P with respect to γ and for a set of monomials $\mathcal{M}$, $\partial_{\mathcal{M}}(P)$ is the set of partial derivatives of P with respect to monomials in $\mathcal{M}$. The space of $(\mathcal{M}, m)$-projected shifted partial derivatives of a polynomial P is defined below.

Definition 4.1 ($(\mathcal{M}, m)$-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

$$\langle \partial_{\mathcal{M}}(P) \rangle_m \stackrel{\text{def}}{=} \mathbb{F}\text{-span}\left\{ \mathsf{Mult}\left[\prod_{i \in S} X_i \cdot g \right] : g \in \partial_{\mathcal{M}}(P), S \subseteq [N], |S| = m \right\}. \tag{4.1}$$

Here, $\mathsf{Mult}[P]$ of a polynomial P is the projection of P on the multilinear monomials in its support. We use the dimension of projected shifted partial derivative space of P with respect to some set of monomials $\mathcal{M}$ and a parameter m as a measure of the complexity of a polynomial. Formally,

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

From the definitions, it is straightforward to see that the measure is subadditive.

Lemma 4.2 (Subadditivity)**.** *Let P and Q be any two multivariate polynomials in $\mathbb{F}[X_1, X_2, \ldots, X_N]$. Let $\mathcal{M}$ be any set of monomials and m be any positive integer. Then, for all scalars α and β*

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

In the proof of Theorem 1.5, we need to upper bound the dimension of the span of projected shifted partial derivatives of the homogeneous component of a fixed degree of polynomials. The following lemma comes to our rescue there.

Lemma 4.3. *Let P be a polynomial of degree at most d. Then for every $0 \leq i \leq d$, and for every choice of parameters m, r and a set $\mathcal{M}$ of monomials of degree equal to r, the following inequality is true.*

$$\phi_{\mathcal{M},m}(P) \geq \phi_{\mathcal{M},m}(\mathsf{Hom}^i[P]).$$

Proof. Since $\mathcal{M}$ is a subset of monomials of degree equal to r, all the partials derivatives are shifted by monomials of degree equal to m and the operation $\mathsf{Mult}[]$ either sets a monomial to zero or leaves it unchanged, it follows that the span of projected shifted partial derivatives of $\mathsf{Hom}^i[P]$ coincides with the span of the homogeneous components of degree-$(i-r)m$ in the space of span of projected shifted partial derivatives of P itself. The lemma then follows from the fact that dimension of a linear space of polynomials is at least as large as the dimension of the space obtained by restricting all polynomials to some fixed homogeneous component. $\square$

In the next lemma, we prove an upper bound on the polynomials which are obtained by a composition of low arity polynomials with polynomials of small support. Gupta et al. [13] first proved such a bound for homogeneous depth-4 circuit with bounded bottom fan-in.

Lemma 4.4. *Let s be a parameter and $Q_1, Q_2, \ldots, Q_t$ be polynomials in $\mathbb{F}[\overline{X}]$ such that for every $i \in [t]$, the support of every monomial in Q_i is of size at most s. Then, for every polynomial F in t variables, every choice of parameters r, m such that $m + rs \le N/2$, and every set $\mathcal{M}$ of monomials of degree equal to r,*

$$\Phi_{\mathcal{M},m}(F(Q_1, Q_2, \ldots, Q_t)) \le N \cdot \binom{t+r}{r} \cdot \binom{N}{m+rs}.$$

Proof. By the chain rule for partial derivatives, every derivative of order r of $F(Q_1, Q_2, \ldots, Q_t)$ can be written as a linear combination of products of the form

$$\left(\frac{\partial F(Y_1, Y_2, \ldots, Y_t)}{\partial \beta_0}|_{Y_i = Q_i}\right) \cdot \prod_{1 \le j \le r'} \frac{\partial P_j}{\partial \beta_j}$$

where

1. r' is at most r,
2. β_0 is a monomial in variables $Y_1, Y_2, \ldots, Y_t$ of degree at most r,
3. for every $1 \le j \le r$, the polynomial P_j is an element of $\{Q_1, Q_2, \ldots, Q_t\}$, and
4. for every $1 \le j \le r$, β_j is a monomial in variables $X_1, X_2, \ldots, X_N$.

Since every monomial in each Q_i is of support at most s, every monomial in each of the products

$$\prod_{1 \le j \le r} \frac{\partial P_j}{\partial \beta_j}$$

is of support at most rs. Therefore, for shifts of degree- m, the projected shifted partial derivatives of $F(Q_1, Q_2, \ldots, Q_t)$ (with respect to monomials in $\mathcal{M}$ which are of degree-r) are in the linear span of polynomials of the form

$$\mathsf{Mult}\left[\left(\frac{\partial F(Y_1, Y_2, \ldots, Y_t)}{\partial \beta_0}|_{Y_i = Q_i}\right) \cdot \alpha\right]$$

where α is a multilinear monomial[14] of degree at most $m + rs$. Therefore, the dimension of this space is upper bounded by the number of possible choices of β_0 and α. Hence

$$\Phi_{\mathcal{M},m}(F(Q_1, Q_2, \ldots, Q_t)) \le N \cdot \binom{t+r}{r} \cdot \binom{N}{m+rs}. \qquad \square$$

[14] If α is not multilinear, the term is set to zero.

4.2 Target polynomials for the lower bound

In this section, we define the family of polynomials for which we prove our lower bounds. The family is a variant of the Nisan-Wigderson polynomials which were introduced by Kayal et al. in [20], and subsequently used in many other results [29, 19, 28]. We start with the following definition.

Definition 4.5 (Nisan-Wigderson polynomial families)**.** Let n, q, e be arbitrary parameters with q being a power of a prime, and $n, e \leq q$. We identify the set $[q]$ with the field $\mathbb{F}_q$ of q elements. Observe that since $n \leq q$, we have that $[n] \subseteq \mathbb{F}_q$. The Nisan-Wigderson polynomial with parameters n, q, e, denoted by $\mathsf{NW}_{n,q,e}$ is defined as

$$\mathsf{NW}_{n,q,e}(\overline{X}) = \sum_{\substack{p(t) \in \mathbb{F}_q[t] \\ \deg(p) < e}} X_{1,p(1)} \dots X_{n,p(n)} \,.$$

The number of variables in $\mathsf{NW}_{n,q,e}$ as defined above is $N = q \cdot n$. The lower bounds in this paper will be proved for the polynomial $\mathsf{NW} \circ \mathsf{Lin}$ which is a variant of the polynomial $\mathsf{NW}_{n,q,e}$ defined as follows.

Definition 4.6 (Hard polynomials for the lower bound)**.** Let $\delta \in (0,1)$ be an arbitrary constant, and let $p = N^{-\delta}$. Let

$$\gamma = \frac{N}{p} = N^{1+\delta} \,.$$

The polynomial $\mathsf{NW} \circ \mathsf{Lin}_{\mathsf{q,n,e,p}}$ is defined as

$$\mathsf{NW} \circ \mathsf{Lin}_{\mathsf{q,n,e,p}} = \mathsf{NW}_{q,n,e}\left(\sum_{i=1}^{\gamma} X_{1,1,i}, \sum_{i=1}^{\gamma} X_{1,2,i}, \dots, \sum_{i=1}^{\gamma} X_{n,q,i}\right) .$$

For brevity, we will denote $\mathsf{NW} \circ \mathsf{Lin}_{\mathsf{q,n,e,p}}$ by $\mathsf{NW} \circ \mathsf{Lin}$ for the rest of the discussion. The advantage of using this trick[15] of composing with linear forms is that it becomes cleaner to show that the polynomial $\mathsf{NW} \circ \mathsf{Lin}$ is robust under random restrictions where every variable is kept alive with a probability p. Since δ is an absolute constant, the number of variables in $\mathsf{NW} \circ \mathsf{Lin}$ is at most $N^{O(1)}$. We now formally define our notion of random restrictions.

Let $\mathcal{V}$ be the set of variables in the polynomial $\mathsf{NW} \circ \mathsf{Lin}$. We now define a distribution $\mathcal{D}_p$ over the subsets of $\mathcal{V}$.

The distribution $\mathcal{D}_p$: Each variable in $\mathcal{V}$ is independently kept alive with a probability $p = N^{-\delta}$.

The random restriction procedure samples a $V \leftarrow \mathcal{D}$ and then keeps only the variables in V alive. The remaining variables are set to 0. We denote the restriction of the polynomial obtained by such a restriction as $\mathsf{NW} \circ \mathsf{Lin}|_V$. Observe that a random restriction also results in a distribution over the restrictions of a circuit computing the polynomial $\mathsf{NW} \circ \mathsf{Lin}$. We denote by $C|_V$ the restriction of a circuit C obtained by setting every input gate in C which is labeled by a variable outside V to 0.

We now show that with a high probability over restrictions sampled according to $\mathcal{D}_p$, the projected shifted partial derivative complexity of $\mathsf{NW} \circ \mathsf{Lin}$ remains high. We need the following lower bound on the dimension of projected shifted partial derivatives of $\mathsf{NW}_{n,q,e}$.

[15] This idea came up during discussions with Ramprasad Saptharishi.

Lemma 4.7 ([29, 25]). *For every n and $r = O(\sqrt{n})$ there exists parameters q, e, ε such that $q = \Omega(n^2)$, $N = qn$ and $\varepsilon = \Theta(\log(n)/\sqrt{n})$ with*

$$q^r \geq (1+\varepsilon)^{2(n-r)},$$
$$q^{e-r} = \left(\frac{2}{1+\varepsilon}\right)^{n-r} \cdot \mathrm{Poly}(q).$$

For any $\{n, q, e, r, \varepsilon\}$ satisfying the above constraints, and for $m = (N/2)(1-\varepsilon)$, over any field $\mathbb{F}$, we have

$$\Phi(\mathsf{NW}_{n,q,e}) \geq \binom{N}{m+n-r} \cdot \exp(-O(\log^2 n)).$$

We will instantiate the lemma above with the following choice of parameters.

- $\varepsilon = \frac{4\log n}{\sqrt{n}}$,
- $r = \sqrt{n}$,
- $q = n^{10}$.
- We will set the parameter s to be equal to $\frac{\sqrt{n}}{100}$.

It is straightforward to check that for the above choice of parameters, there is a choice of e such that

$$q^r \geq (1+\varepsilon)^{2(n-r)},$$
$$q^{e-r} = \left(\frac{2}{1+\varepsilon}\right)^{n-r} \cdot \mathrm{Poly}(q).$$

Therefore, for $m = (N/2)(1-\varepsilon)$, over any field $\mathbb{F}$, we have

$$\Phi(\mathsf{NW}_{n,q,e}) \geq \binom{N}{m+n-r} \cdot \exp(-O(\log^2 n)).$$

We are now ready to prove our main lemma for this section.

Lemma 4.8. *With a probability at least $1-o(1)$ over $V \leftarrow \mathcal{D}_p$, there exists a subset of variables $V' \subseteq V$ such that $|V'| = N$ and*

$$\Phi(\mathsf{NW} \circ \mathsf{Lin}|_{V'}) \geq \binom{N}{m+n-r} \cdot \exp(-O(\log^2 n)).$$

Proof. To prove the lemma, we first show that with a high probability over the random restrictions, the polynomial $P|_V$ has the polynomial $\mathsf{NW}_{n,q,e}$ as a projection by setting some variables to zero. Combining this with Lemma 4.7 would complete the proof. We now fill in the details.

Let $i \in [N]$. Then, the probability that all the variables in the set $A_{i,j} = \{X_{i,j,\ell} : \ell \in [\gamma]\}$ are set to zero by the random restrictions is equal to $(1-p)^\gamma \leq \exp(-\Theta(N))$. Therefore, the probability that there exists an $i \in [n], j \in [q]$ such that all the variables in the set $A_{i,j}$ are set to zero by the random restrictions, is at most $N \cdot \exp(-\Theta(N)) = o(1)$. We now argue that if this event does not happen (which is the case with probability at least $1-o(1)$), then the dimension of the projected shifted partial derivatives is large.

For every i, j, let $A'_{i,j}$ be the subset of $A_{i,j}$ which has not been set to zero. We know that for every i, j, $A'_{i,j}$ is non-empty. Now, for every i, j, we set all the elements of $A'_{i,j}$ to zero except one. Observe that the polynomial obtained from $\mathsf{NW} \circ \mathsf{Lin}$ after this restriction is exactly the polynomial $NW_{n,q,e}$ up to a relabeling of variables. Now, from Lemma 4.7, our claim follows. □

4.3 Proof of Theorem 1.5

To prove our lower bound, we show that under a random restriction from the distribution $\mathcal{D}_p$, the dimension of the linear span of projected shifted partial derivatives of any $\Sigma\Pi^{(n)}\Sigma\Pi$ circuit C is small with a high probability if the size of the C is *not too large*. Comparing this with the lower bound on the dimension of projected shifted partials of the polynomial $\mathsf{NW} \circ \mathsf{Lin}$ under random restrictions from Lemma 4.8, the lower bound follows. We now proceed along this outline and prove the following lemma.

Lemma 4.9 (Upper bound on complexity of circuits)**.** *Let m, r, s be parameters such that $m + rs \leq N/2$. Let $\mathcal{M}$ be any set of multilinear monomials of degree-r. Let C be an arithmetic circuit computing a homogeneous polynomial of degree-n such that*

$$C = \sum_{i=1}^{T} C_i(Q_{i1}, Q_{i2}, \ldots, Q_{it})$$

where

- *for each $i \in [T]$, C_i is a polynomial in t variables, and*
- *for each $i \in [T]$, the algebraic rank of the set $\{Q_{ij} : j \in [t]\}$ of polynomials is at most k.*

For each $i \in [T]$ and $j \in [t]$, let S_{ij} be the set of monomials with nonzero coefficients in Q_{ij}. If

$$\left| \bigcup_{i \in [T], j \in [t]} S_{ij} \right| \leq N^{\frac{\delta s}{2}}$$

then, with a probability at least $1 - o(1)$ over $V \leftarrow \mathcal{D}_p$[16] *for all subsets V' of V of size at most N*

$$\Phi(C|_{V'}) \leq TN \binom{k(n+1)+r}{r} \binom{N}{m+rs}.$$

Proof. We prove the lemma by first using random restrictions to simplify the circuit into one with bounded bottom support, and then utilizing the tools tools developed in Section 3 and Section 4.1 to conclude that the dimension of the space of projected shifted partial derivatives of the resulting circuit is small.

[16] This is the distribution defined in Section 4.2, where every variable is kept alive with a probability $N^{-\delta}$ for a constant $\delta \in (0,1)$.

Step (1): Random restrictions. From the definition of random restrictions, every variable is kept alive independently with a probability $p = N^{-\delta}$. So, the probability that a monomial of support at least s survives the restrictions is at most $N^{-\delta s}$. Therefore, by linearity of expectations, the expected number of monomials of support at least s in $\bigcup_{i\in[T],j\in[t]} S_{ij}$ which survive the random restrictions is at most

$$\left|\bigcup_{i\in[T],j\in[t]} S_{ij}\right| \cdot N^{-\delta s} \leq N^{-\frac{\delta s}{2}} .$$

So, by Markov's inequality, the probability that at least one monomial of support at least s in $\bigcup_{i\in[T],j\in[t]} S_{ij}$ survives the random restrictions is $o(1)$. Let V' be any subset of the surviving set of variables of size N. For the rest of the proof, we assume that all the variables outside the set V' are set to zero. Restrictions which set all monomials of support at least s in $\bigcup_{i\in[T],j\in[t]} S_{ij}$ to zero are said to be good.

Step (2): Using low algebraic rank. In this step, we assume that we are given a good restriction C' of the circuit C. Let

$$C' = \sum_{i=1}^{T} C'_i(Q'_{i1}, Q'_{i2}, \dots, Q'_{it})$$

where for every $i \in [T], j \in [t]$, all monomials of Q'_{ij} have support at most s. Observe that random restrictions cannot increase the algebraic rank of a set of polynomials. Therefore, for every $i \in [T]$, the algebraic rank of the set $\{Q'_{ij} : j \in [t]\}$ of polynomials is at most k. For ease of notation, let us assume that the algebraic rank is equal to k. Without loss of generality, let the set $\mathcal{B}_i = \{Q'_{i1}, Q'_{i2}, \dots, Q'_{ik}\}$ be the set guaranteed by Lemma 3.5. We know that there exists an $\overline{a} \in \mathbb{F}^N$ and polynomials $\{F'_i : i \in [T]\}$ such that

$$C'(\overline{X}+\overline{a}) = \sum_{i=1}^{T} F'_i\left(\mathsf{Hom}\left[Q'_{i1}(\overline{X}+\overline{a})\right], \mathsf{Hom}\left[Q'_{i2}(\overline{X}+\overline{a})\right], \dots, \mathsf{Hom}\left[Q'_{ik}(\overline{X}+\overline{a})\right]\right). \tag{4.2}$$

Moreover, since $C(\overline{X})$ (and hence $C'(\overline{X})$) is a homogeneous polynomial of degree-n, the following is true.

$$C'(\overline{X}) = \mathsf{Hom}^n\left[\sum_{i=1}^{T} F'_i\left(\mathsf{Hom}\left[Q'_{i1}(\overline{X}+\overline{a})\right], \mathsf{Hom}\left[Q'_{i2}(\overline{X}+\overline{a})\right], \dots, \mathsf{Hom}\left[Q'_{ik}(\overline{X}+\overline{a})\right]\right)\right]. \tag{4.3}$$

An important observation here is that for the rest of the argument, we can assume that the degree of every polynomial $Q'_{ij}(\overline{X}+\overline{a})$ is at most n. If not, we can simply replace any such high degree $Q'_{ij}(\overline{X}+\overline{a})$ by

$$\mathsf{Hom}^{\leq n}\left[Q'_{ij}(\overline{X}+\overline{a})\right] .$$

We claim that the equality 4.3 continues to hold. This is because the higher degree monomials of Q_{ij} do not participate in the computation of the lower degree monomials. The only monomials which could potentially change by this substitution are the ones with degree strictly larger than n.

Step (3): Upper bound on $\Phi_{\mathcal{M},m}(C'(\overline{X}))$. Let R be defined the polynomial

$$R = \sum_{i=1}^{T} F_i'(\mathsf{Hom}\left[Q_{i1}'(\overline{X}+\overline{a})\right], \mathsf{Hom}\left[Q_{i2}'(\overline{X}+\overline{a})\right], \ldots, \mathsf{Hom}\left[Q_{ik}'(\overline{X}+\overline{a})\right]). \tag{4.4}$$

Note that if the support of every monomial in a polynomial $Q_{ij}'(\overline{X})$ is at most s, then for every translation $\overline{a} \in \mathbb{F}^N$ the support of every monomial in $Q_{ij}'(\overline{X}+\overline{a})$ is also at most s. From Lemma 4.4 and from Lemma 4.2, it is easy to see that

$$\Phi_{\mathcal{M},m}(R) \leq TN\binom{k(n+1)+r}{r}\binom{N}{m+rs}.$$

From Lemma 4.3, it follows that

$$\Phi_{\mathcal{M},m}(C'(\overline{X})) \leq \Phi_{\mathcal{M},m}(R) \leq TN\binom{k(n+1)+r}{r}\binom{N}{m+rs}.$$

Observe that steps (2) and (3) of the proof are always successful if the restriction in step 1 is good, which happens with a probability at least $1-o(1)$. So, the lemma follows. □

We now complete the proof of Theorem 1.5.

Proof of Theorem 1.5. If the size of the circuit C is at least $N^{(\delta/2)\sqrt{n}}$, then we are done. Else, the size of C is at most $N^{(\delta/2)\sqrt{n}}$. This implies that the total number of monomials in all the polynomials Q_{ij} together is at most $N^{(\delta/2)\sqrt{n}}$. From Lemma 4.9 and Lemma 4.8, it follows that there exists a subset V' of variables of size N such that both the following inequalities are true.

$$\Phi_{\mathcal{M},m}(C|_{V'}) \leq TN\binom{k(n+1)+r}{r}\binom{N}{m+rs} \tag{4.5}$$

and

$$\Phi_{\mathcal{M},m}(\mathsf{NW}\circ\mathsf{Lin}|_{V'}) \geq \binom{N}{m+n-r}\cdot\exp(-\log^2 n). \tag{4.6}$$

Since C computes $\mathsf{NW}\circ\mathsf{Lin}$, it must be the case that

$$T \geq \frac{\binom{N}{m+n-r}\cdot\exp(-\log^2 n)}{N\binom{k(n+1)+r}{r}\binom{N}{m+rs}}.$$

Plugging in the value of the parameters from Section 4.2, and approximating using Lemma 2.7, we immediately get

$$\binom{N}{m+n-r} = \binom{N}{m}\cdot(1+\varepsilon)^{2(n-r)}\cdot\exp(O((n-r)\cdot\varepsilon^2))$$

and

$$\binom{N}{m+rs} = \binom{N}{m}\cdot(1+\varepsilon)^{2rs}\cdot\exp(O(rs\cdot\varepsilon^2)).$$

Moreover, $\binom{k(n+1)+r}{r} \leq (enk)^r \leq \exp(2\sqrt{n}\cdot\log n)$. Taking the ratio and substituting the values of the parameters, we get

$$T \geq \exp(\Omega(\sqrt{n}\log N)).$$ □

5 Application to polynomial identity testing

In this section we give an application of the ideas developed in Section 3 to the question of polynomial identity testing and prove Theorem 1.8. We start by formally defining the notion of a hitting set.

Hitting set. Let $\mathcal{S}$ be a set of polynomials in N variables over a field $\mathbb{F}$. Then, a set $\mathcal{H} \subseteq \mathbb{F}^N$ is said to be a *hitting set* for the class $\mathcal{S}$, if for every polynomial $P \in \mathcal{S}$ such that P is not identically zero, there exists a $p \in \mathcal{H}$ such that $P(p) \neq 0$.

For our PIT result, we show that any nonzero polynomial P in the circuit class we consider, has a monomial of low support. A hitting set can then be constructed by the standard techniques using the Shpilka-Volkovich generator [40].

Lemma 5.1 (Shpilka-Volkovich generator [40][17])**.** *Let $\mathbb{F}$ be a field of characteristic zero. For every ℓ, d, N, there exists a set $\mathcal{H} \subseteq \mathbb{F}^N$ of size at most $(O(Nd))^\ell$ such that for every nonzero polynomial P of degree at most d in N variables which contains a monomial of support at most ℓ, there exists an $h \in \mathcal{H}$ such that $P(h) \neq 0$. Moreover, the set $\mathcal{H}$ can be constructed in time* $\mathrm{Poly}(N,d,\ell) \cdot (O(Nd))^\ell$.

The following lemma is our main technical claim.

Lemma 5.2. *Let $\mathbb{F}$ be a field of characteristic zero. Let P be a homogeneous polynomial of degree-Δ in N variables such that P can be represented as*

$$P = \sum_{i=1}^{T} C_i(Q_{i1}, Q_{i2}, \dots, Q_{it})$$

such that the following are true.

- *For each $i \in [T]$, C_i is a polynomial in t variables.*
- *For each $i \in [T]$ and $j \in [t]$, Q_{ij} is a polynomial of degree at most d in N variables.*
- *For each $i \in [T]$, the algebraic rank of the set $\{Q_{ij} : j \in [t]\}$ of polynomials is at most k.*

Then, the trailing monomial of P has support at most

$$2\mathrm{e}^3 d \cdot (\ln(T(\Delta+1)) + (d+1)k \ln(2(d+1)k) + 1) .$$

Here, e *is Euler's constant.*

In order to prove Lemma 5.2, we follow the outline of proving *robust* lower bounds for arithmetic circuits, described and used by Forbes [9]. This essentially amounts to showing that the trailing monomial of P has small support. We use the following result of Forbes [9] in a blackbox manner which greatly simplifies our proof.

[17] See Corollary 3.15 in [9].

Lemma 5.3 (Proposition 4.18 in Forbes [9]). *Let $R(\overline{X})$ be a polynomial in $\mathbb{F}[\overline{X}]$ such that*

$$R(\overline{X}) = \sum_{i=1}^{T} F_i(Q_{i1}, Q_{i2}, \ldots, Q_{it})$$

and for each $i \in [T]$ and $j \in [t]$, the degree of Q_{ij} is at most d. Let α be the trailing monomial of R. Then, the support of α is at most $2\mathrm{e}^3 d(\ln T + t \ln 2t + 1)$, where e is Euler's constant.

We now proceed to prove Lemma 5.2.

Proof of Lemma 5.2. Recall that our goal is to show that the polynomial P, which can be represented as

$$P = \sum_{i=1}^{T} C_i(Q_{i1}, Q_{i2}, \ldots, Q_{it}),$$

has a trailing monomial of small support.

For every $i \in [T]$, let $\mathcal{Q}_i = \{Q_{i1}, Q_{i2}, \ldots, Q_{it}\}$ and let $\mathcal{Q}_i$ be of algebraic rank k_i. Without loss of generality, let us assume the sets $\mathcal{B}_i = \{Q_{i1}, Q_{i2}, \ldots, Q_{ik_i}\}$ are the sets guaranteed by Lemma 3.5. This implies that there exist polynomials $F_1, F_2, \ldots, F_T$ and $\overline{a} \in \mathbb{F}^N$ such that

$$P(\overline{X} + \overline{a}) = \left[\sum_{i=1}^{T} F_i(\mathsf{Hom}[Q_{i1}(\overline{X} + \overline{a})], \mathsf{Hom}[Q_{i2}(\overline{X} + \overline{a})], \ldots, \mathsf{Hom}[Q_{ik_i}(\overline{X} + \overline{a})]) \right]. \tag{5.1}$$

Since each $k_i \leq k$, for the ease of notation, we assume that each $k_i = k$. Observe that if P is a homogeneous polynomial of degree $\deg(P) \leq \Delta$, then,

$$\mathsf{Hom}^{\deg(P)}[P(\overline{X} + \overline{a})] \equiv P(\overline{X}).$$

So, from Lemma 2.3, it follows that there exist $k(d+1)$-variate polynomials $F'_1, F'_2, \ldots, F'_{T(\Delta+1)}$ and a set $\{Q'_{ij} : i \in [T(\Delta+1)], j \in [k]\}$ of polynomials such that

$$P(\overline{X}) = \sum_{i=1}^{T(\Delta+1)} F'_i(\mathsf{Hom}[Q'_{i1}(\overline{X} + \overline{a})], \mathsf{Hom}[Q'_{i2}(\overline{X} + \overline{a})], \ldots, \mathsf{Hom}[Q'_{ik}(\overline{X} + \overline{a})]).$$

Moreover, every polynomial in the set $\{Q'_{ij} : i \in [T(\Delta+1)], j \in [k]\}$ has degree at most d. Now, Lemma 5.3 implies that the trailing monomial α of $P(\overline{X})$ has support at most

$$2\mathrm{e}^3 d \cdot (\ln(T(\Delta+1)) + (d+1)k \ln(2(d+1)k) + 1). \qquad \square$$

We are now ready to complete the proof of Theorem 1.8.

Proof of Theorem 1.8. From Definition 1.2, it follows there could be non-homogeneous polynomials $P \in \mathcal{C}$. So, we cannot directly use Lemma 5.2 to say something about them, since the proof relies on homogeneity. But, this is not a problem, since a polynomial is identically zero if and only if all its homogeneous components are identically zero. Moreover, by applying Lemma 2.3 to every summand feeding into the top sum gate of the circuit, we get that every homogeneous component of P[18] can also be computed by a circuit similar in structure to that of P at the cost of a blow up by a factor $\Delta+1$ in the top fan-in. We can then apply Lemma 5.2 to each of these homogeneous components to conclude that if P is not identically zero, then it contains a monomial of support at most

$$2e^3 d \cdot (\ln\left(T(\Delta+1)^2\right) + (d+1)k\ln(2(d+1)k) + 1)\,.$$

Theorem 1.8 immediately follows by detecting the low support monomial using Lemma 5.2 and Lemma 5.1. □

6 Open questions

We conclude with some open questions.

- Prove the lower bounds in the paper for a polynomial in VP. We believe this is true, but it seems that we need a strengthening of the bounds proved in [29]. In particular, it needs to be shown that the lower bound for *IMM* (Iterated matrix multiplication) continues to hold when a depth-4 circuit is not homogeneous but the formal degree is at most the square of the degree of the polynomial itself.

- It would be interesting to see if there are other applications of Lemma 1.10 to questions in complexity theory. The Jacobian characterization of algebraic independence has several very interesting applications [1, 6].

Acknowledgements

Many thanks to Ramprasad Saptharishi for answering numerous questions regarding the results and techniques in [1]. We are also thankful to Michael Forbes for sharing a draft of his paper [9] with us and to anonymous reviewers for comments which helped us in improving the presentation of the paper.

References

[1] MANINDRA AGRAWAL, CHANDAN SAHA, RAMPRASAD SAPTHARISHI, AND NITIN SAXENA: Jacobian hits circuits: hitting-sets, lower bounds for depth-D occur-k formulas and depth-3 transcendence degree-k circuits. *SIAM J. Comput.*, 45(4):1533–1562, 2016. Preliminary version in STOC 2012. [doi:10.1137/130910725, arXiv:1111.0582] 3, 4, 5, 8, 9, 10, 12, 28

[2] MANINDRA AGRAWAL AND V. VINAY: Arithmetic circuits: A chasm at depth four. In *Proc. 49th FOCS*, pp. 67–75. IEEE Comp. Soc. Press, 2008. Available at ECCC. [doi:10.1109/FOCS.2008.32] 2

[18] Only the top fan-in increases by a factor of $\Delta+1$, all other parameters in Definition 1.2 remain the same.

[3] MALTE BEECKEN, JOHANNES MITTMANN, AND NITIN SAXENA: Algebraic independence and blackbox identity testing. *Inform. and Comput.*, 222:2–19, 2013. Preliminary version in ICALP'11. [doi:10.1016/j.ic.2012.10.004, arXiv:1102.2789] 5, 12

[4] XI CHEN, NEERAJ KAYAL, AND AVI WIGDERSON: Partial derivatives in arithmetic complexity and beyond. *Found. and Trends in Theoret. Comput. Sci.*, 6(1-2):1–138, 2011. [doi:10.1561/0400000043] 12

[5] RICHARD A. DEMILLO AND RICHARD J. LIPTON: A probabilistic remark on algebraic program testing. *Inform. Process. Lett.*, 7(4):193–195, 1978. [doi:10.1016/0020-0190(78)90067-4] 14

[6] ZEEV DVIR, ARIEL GABIZON, AND AVI WIGDERSON: Extractors and rank extractors for polynomial sources. *Comput. Complexity*, 18(1):1–58, 2009. Preliminary version in FOCS'07. [doi:10.1007/s00037-009-0258-4] 28

[7] ZEEV DVIR AND AMIR SHPILKA: Locally decodable codes with 2 queries and polynomial identity testing for depth 3 circuits. *SIAM J. Comput.*, 36(5):1404–1434, 2007. Preliminary version in STOC'05. [doi:10.1137/05063605X] 3

[8] ZEEV DVIR, AMIR SHPILKA, AND AMIR YEHUDAYOFF: Hardness-randomness tradeoffs for bounded depth arithmetic circuits. *SIAM J. Comput.*, 39(4):1279–1293, 2009. Preliminary version in STOC'08. [doi:10.1137/080735850] 9, 11, 14

[9] MICHAEL A. FORBES: Deterministic divisibility testing via shifted partial derivatives. In *Proc. 56th FOCS*, pp. 451–465. IEEE Comp. Soc. Press, 2015. [doi:10.1109/FOCS.2015.35] 5, 8, 9, 11, 26, 27, 28

[10] MICHAEL A. FORBES AND AMIR SHPILKA: Quasipolynomial-time identity testing of non-commutative and read-once oblivious algebraic branching programs. In *Proc. 54th FOCS*, pp. 243–252. IEEE Comp. Soc. Press, 2013. Available at ECCC. [doi:10.1109/FOCS.2013.34, arXiv:1209.2408] 3

[11] DIMA GRIGORIEV AND MAREK KARPINSKI: An exponential lower bound for depth 3 arithmetic circuits. In *Proc. 30th STOC*, pp. 577–582. ACM Press, 1998. [doi:10.1145/276698.276872] 4

[12] DIMA GRIGORIEV AND ALEXANDER A. RAZBOROV: Exponential lower bounds for depth 3 arithmetic circuits in algebras of functions over finite fields. *Appl. Algebra Eng. Commun. Comput.*, 10(6):465–487, 2000. Preliminary version in FOCS'98. [doi:10.1007/s002009900021] 4

[13] ANKIT GUPTA, PRITISH KAMATH, NEERAJ KAYAL, AND RAMPRASAD SAPTHARISHI: Approaching the chasm at depth four. *J. ACM*, 61(6):33:1–33:16, 2014. Preliminary versions in CCC'13 and ECCC. [doi:10.1145/2629541] 2, 10, 20

[14] ZOHAR SHAY KARNIN, PARTHA MUKHOPADHYAY, AMIR SHPILKA, AND ILYA VOLKOVICH: Deterministic identity testing of depth-4 multilinear circuits with bounded top fan-in. *SIAM J. Comput.*, 42(6):2114–2131, 2013. Preliminary versions in STOC'10 and ECCC. [doi:10.1137/110824516] 3

[15] ZOHAR SHAY KARNIN AND AMIR SHPILKA: Black box polynomial identity testing of generalized depth-3 arithmetic circuits with bounded top fan-in. *Combinatorica*, 31(3):333–364, 2011. Preliminary version in CCC'08. [doi:10.1007/s00493-011-2537-3] 3

[16] NEERAJ KAYAL: The complexity of the annihilating polynomial. In *Proc. 24th IEEE Conf. on Computational Complexity (CCC'09)*, pp. 184–193. IEEE Comp. Soc. Press, 2009. [doi:10.1109/CCC.2009.37] 12

[17] NEERAJ KAYAL: An exponential lower bound for the sum of powers of bounded degree polynomials. *Electron. Colloq. on Comput. Complexity (ECCC)*, (81):1–5, 2012. Available at ECCC. 3

[18] NEERAJ KAYAL, NUTAN LIMAYE, CHANDAN SAHA, AND SRIKANTH SRINIVASAN: An exponential lower bound for homogeneous depth four arithmetic formulas. *SIAM J. Comput.*, 46(1):307–335, 2017. Preliminary version in FOCS'14. [doi:10.1137/151002423] 3, 8, 10, 19

[19] NEERAJ KAYAL AND CHANDAN SAHA: Lower bounds for depth-three arithmetic circuits with small bottom fanin. *Comput. Complexity*, 25(2):419–454, 2016. Preliminary versions in CCC'15 and ECCC. [doi:10.1007/s00037-016-0132-0] 19, 21

[20] NEERAJ KAYAL, CHANDAN SAHA, AND RAMPRASAD SAPTHARISHI: A super-polynomial lower bound for regular arithmetic formulas. In *Proc. 46th STOC*, pp. 146–153. ACM Press, 2014. Available at ECCC. [doi:10.1145/2591796.2591847] 21

[21] NEERAJ KAYAL, CHANDAN SAHA, AND SÉBASTIEN TAVENAS: An almost cubic lower bound for depth three arithmetic circuits. In *Proc. 43rd Internat. Colloq. on Automata, Languages and Programming (ICALP'16)*, pp. 33:1–33:15. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2016. Available at ECCC. [doi:10.4230/LIPIcs.ICALP.2016.33] 3

[22] NEERAJ KAYAL AND SHUBHANGI SARAF: Blackbox polynomial identity testing for depth 3 circuits. In *Proc. 50th FOCS*, pp. 198–207. IEEE Comp. Soc. Press, 2009. Available at ECCC. [doi:10.1109/FOCS.2009.67] 3

[23] NEERAJ KAYAL AND NITIN SAXENA: Polynomial identity testing for depth 3 circuits. *Comput. Complexity*, 16(2):115–138, 2007. Preliminary version in CCC 2016. [doi:10.1007/s00037-007-0226-9] 3

[24] PASCAL KOIRAN: Arithmetic circuits: The chasm at depth four gets wider. *Theoret. Comput. Sci.*, 448:56–65, 2012. [doi:10.1016/j.tcs.2012.03.041, arXiv:1006.4700] 2

[25] MRINAL KUMAR AND RAMPRASAD SAPTHARISHI: An exponential lower bound for homogeneous depth-5 circuits over finite fields. *Electron. Colloq. on Comput. Complexity (ECCC)*, (109):1–36, 2015. Available at ECCC. [arXiv:1507.00177] 22

[26] MRINAL KUMAR AND SHUBHANGI SARAF: The limits of depth reduction for arithmetic formulas: It's all about the top fan-in. *SIAM J. Comput.*, 44(6):1601–1625, 2015. Preliminary version in STOC'14. [doi:10.1137/140999220, arXiv:1311.6716] 10

[27] MRINAL KUMAR AND SHUBHANGI SARAF: Arithmetic circuits with locally low algebraic rank. In *Proc. 31st IEEE Conf. on Computational Complexity (CCC'16)*, pp. 34:1–34:27. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2016. [doi:10.4230/LIPIcs.CCC.2016.34] 1

[28] MRINAL KUMAR AND SHUBHANGI SARAF: Sums of products of polynomials in few variables: lower bounds and polynomial identity testing. In *Proc. 31st IEEE Conf. on Computational Complexity (CCC'16)*, pp. 35:1–35:29. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2016. Available at ECCC. [doi:10.4230/LIPIcs.CCC.2016.35, arXiv:1504.06213] 13, 19, 21

[29] MRINAL KUMAR AND SHUBHANGI SARAF: On the power of homogeneous depth 4 arithmetic circuits. *SIAM J. Comput.*, 46(1):336–387, 2017. Preliminary version in FOCS'14. [doi:10.1137/140999335, arXiv:1404.1950] 3, 8, 10, 19, 21, 22, 28

[30] RAFAEL OLIVEIRA, AMIR SHPILKA, AND BEN LEE VOLK: Subexponential size hitting sets for bounded depth multilinear formulas. *Comput. Complexity*, 25(2):455–505, 2016. Preliminary versions in ECCC and 10.4230/LIPIcs.CCC.2015.304CCC 2015. [doi:10.1007/s00037-016-0131-1, arXiv:1411.7492] 3

[31] JAMES G. OXLEY: *Matroid Theory*. Oxford Univ. Press, 2006. 6

[32] ANURAG PANDEY, NITIN SAXENA, AND AMIT SINHABABU: Algebraic independence over positive characteristic: New criterion and applications to locally low algebraic rank circuits. In *41st Internat. Symp. Mathemat. Found. Comput. Sci. (MFCS'16)*, pp. 74:1–74:15, 2016. [doi:10.4230/LIPIcs.MFCS.2016.74] 9

[33] RAN RAZ: Elusive functions and lower bounds for arithmetic circuits. *Theory of Computing*, 6(7):135–177, 2010. Preliminary version in STOC'08. [doi:10.4086/toc.2010.v006a007] 3, 4

[34] RAMPRASAD SAPTHARISHI: Recent progress on arithmetic circuit lower bounds. *Bull. EATCS*, (114), 2014. 3

[35] RAMPRASAD SAPTHARISHI: A survey of lower bounds in arithmetic circuit complexity, 2014. Available at author's GitHub. 3, 14

[36] SHUBHANGI SARAF AND ILYA VOLKOVICH: Black-box identity testing of depth-4 multilinear circuits. In *Proc. 43rd STOC*, pp. 421–430. ACM Press, 2011. Available at ECCC. [doi:10.1145/1993636.1993693] 3

[37] NITIN SAXENA AND C. SESHADHRI: From Sylvester-Gallai configurations to rank bounds: Improved black-box identity test for deph-3 circuits. In *Proc. 51st FOCS*, pp. 21–29. IEEE Comp. Soc. Press, 2010. [doi:10.1109/FOCS.2010.9] 3

[38] NITIN SAXENA AND C. SESHADHRI: Blackbox identity testing for bounded top-fanin depth-3 circuits: The field doesn't matter. *SIAM J. Comput.*, 41(5):1285–1298, 2012. Preliminary version in STOC'11. [doi:10.1137/10848232] 3

[39] AMIR SHPILKA: Affine projections of symmetric polynomials. *J. Comput. System Sci.*, 65(4):639–659, 2002. Preliminary version in CCC'01. [doi:10.1016/S0022-0000(02)00021-1] 3

[40] AMIR SHPILKA AND ILYA VOLKOVICH: Read-once polynomial identity testing. *Comput. Complexity*, 24(3):477–532, 2015. Preliminary version in RANDOM'09. [doi:10.1007/s00037-015-0105-8] 11, 26

[41] AMIR SHPILKA AND AVI WIGDERSON: Depth-3 arithmetic circuits over fields of characteristic zero. *Comput. Complexity*, 10(1):1–27, 2001. Preliminary version in CCC'99. [doi:10.1007/PL00001609] 3, 4

[42] AMIR SHPILKA AND AMIR YEHUDAYOFF: Arithmetic circuits: A survey of recent results and open questions. *Found. and Trends in Theoret. Comput. Sci.*, 5(3-4):207–388, 2010. [doi:10.1561/0400000039] 2

[43] SÉBASTIEN TAVENAS: Improved bounds for reduction to depth 4 and depth 3. *Inform. and Comput.*, 240:2–11, 2015. Preliminary version in MFCS'13. [doi:10.1016/j.ic.2014.09.004, arXiv:1304.5777] 2

[44] LESLIE G. VALIANT: Completeness classes in algebra. In *Proc. 11th STOC*, pp. 249–261. ACM Press, 1979. [doi:10.1145/800135.804419] 2

AUTHORS

Mrinal Kumar
Rutgers University, New Brunswick, NJ
mrinalkumar08@gmail.com
`https://mrinalkr.bitbucket.io/`

Shubhangi Saraf
Rutgers University, New Brunswick, NJ
shubhangi.saraf@gmail.com
`http://sites.math.rutgers.edu/~ss1984/`

ABOUT THE AUTHORS

MRINAL KUMAR received his Ph. D. in Computer Science in May 2017 from Rutgers University where he was advised by Swastik Kopparty and Shubhangi Saraf. His research interests are in Arithmetic and Boolean circuit complexity and Error Correcting Codes. Mrinal spent his undergrad years at IIT Madras and owes his interest in Complexity Theory to a delightful class on the topic taught by Jayalal Sarma. Apart from theory, he finds great joy in test cricket and in the adventures of Calvin & Hobbes.

SHUBHANGI SARAF grew up in Pune, India. She received her Ph. D. in computer science from the Massachusetts Institute of Technology in 2011 under the guidance of Madhu Sudan. Shubhangi is broadly interested in complexity theory, coding theory and pseudo-randomness. Recently she has been captivated by questions related to understanding the power and limitations of algebraic computation, as well as to understanding the potential of *locality* in algorithms for codes.

Shubhangi discovered her love for mathematics in her high school years at the Bhaskaracharya Pratishthana, an educational and research institute in mathematics in Pune, under the guidance and mentoring of her teacher Mr. Prakash Mulabagal. Mr. Prakash ran an amazing program aimed at getting high school students from across Pune introduced to the joy of math and the sciences beyond what any school curriculum in Pune could possibly attempt to do. Shubhangi owes a great deal of her enthusiasm for math problem solving to Mr. Prakash, and also to being able, through the Bhaskaracharya Pratishthana program, to make close friends in Pune who were into the same thing.

Thanks to this nurturing environment, Shubhangi got involved in math competitions and represented India twice at the International Mathematical Olympiad (IMO), once winning a bronze medal (2002) and once a silver (2003).

She went on to do her undergraduate studies in Mathematics at MIT, graduating in 2007. She did not really know that she wanted to stay on in academia until her junior year when she spent a year abroad as a *mathmo* at Cambridge University in the UK where she took fantastic courses by Tim Gowers and Imre Leader. Once back at MIT, in summer 2006, she did a research project with Igor Pak at MIT, which gave her a lot of confidence and encouragement. She was also fortunate to take some more great courses at MIT; "Randomized algorithms" by David Karger and "Complexity theory" by Madhu Sudan were particularly influential. The support and encouragement from her MIT mentors eventually got her on the path to theoretical computer science.

In her spare time Shubhangi enjoys reading, cooking, long walks, and exploring cafés and restaurants. Her little toddler is a constant source of joy and amazement, and she also makes sure there isn't much time to spare.