A Quadratic Lower Bound for Homogeneous Algebraic Branching Programs*

Mrinal Kumar

Rutgers University, Newark, NJ, USA
mrinal.kumar@rutgers.edu

Abstract

An algebraic branching program (ABP) is a directed acyclic graph, with a start vertex s, and end vertex t and each edge having a weight which is an affine form in variables $x_1, x_2, \ldots, x_n$ over an underlying field. An ABP computes a polynomial in a natural way, as the sum of weights of all paths from s to t, where the weight of a path is the product of the weights of the edges in the path. An ABP is said to be homogeneous if the polynomial computed at every vertex is homogeneous. In this paper, we show that any homogeneous algebraic branching program which computes the polynomial $x_1^n + x_2^n + \ldots + x_n^n$ has at least $\Omega(n^2)$ vertices (and edges).

To the best of our knowledge, this seems to be the first non-trivial super-linear lower bound on the number of vertices for a general *homogeneous* ABP and slightly improves the known lower bound of $\Omega(n \log n)$ on the number of edges in a general (possibly *non-homogeneous*) ABP, which follows from the classical results of Strassen (1973) and Baur & Strassen (1983).

On the way, we also get an alternate and unified proof of an $\Omega(n \log n)$ lower bound on the size of a *homogeneous* arithmetic circuit (follows from [Strassen, 1973] and [Baur & Strassen, 1983]), and an $n/2$ lower bound (n over reals) on the determinantal complexity of an explicit polynomial [Mignon & Ressayre, 2004], [Cai, Chen & Li, 2010], [Yabe, 2015]. These are currently the best lower bounds known for these problems for any explicit polynomial, and were originally proved nearly two decades apart using seemingly different proof techniques.

1998 ACM Subject Classification I.1.1 Expressions and Their Representation

Keywords and phrases algebraic branching programs, arithmetic circuits, determinantal complexity, lower bounds

Digital Object Identifier 10.4230/LIPIcs.CCC.2017.19

1 Introduction

The question of proving superpolynomial lower bounds on the size of arithmetic circuits for an explicit polynomial family is a fundamental problem in the area of algebraic complexity theory. Unfortunately, the state of art for this problem is quite unsatisfying and the best lower bound known for general arithmetic circuits is an $\Omega(n \log d)$ lower bound for the polynomial $P_{(n,d)} = \sum_{i=1}^{n} x_i^d$, proved by Strassen [16] and Baur & Strassen [2] more than three decades ago. The absence of substantial progress on the general question has led to focus on the question of proving better lower bounds for interesting restricted classes of arithmetic circuits. Arithmetic formula, non-commutative circuits, bounded depth circuits, multilinear formulas and monotone arithmetic circuits are some restricted classes of arithmetic circuits which have been studied from this point of view, and for many of these classes substantial progress has been made on the question of proving lower bounds. We refer the reader to the surveys

* Research supported in part by a Simons Graduate Fellowship.

32nd Computational Complexity Conference (CCC 2017).
Editor: Ryan O'Donnell; Article No. 19; pp. 19:1–19:16

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

of Shpilka-Yehudayoff [13] and Saptharishi [11] and the references therein for an overview of these results. One such restricted model of computation, which will be the primary focus of this paper is the model of algebraic branching programs (ABP), which we define now.

▶ **Definition 1** (Algebraic Branching Programs (ABP))**.** An algebraic branching program in variables $\{x_1, x_2, \ldots, x_n\}$ over a field $\mathbb{F}$ is a directed acyclic graph with a designated *starting vertex* s with in degree zero, a designated *end vertex* t with out degree zero, and the edge between any two vertices is labeled by an affine form from $\mathbb{F}[x_1, x_2, \ldots, x_n]$.

We say that the ABP is homogeneous, if the polynomial computed at every vertex is a homogeneous polynomial.

The weight of any (directed) path in an ABP is the product of labels of the edges in the path. The polynomial computed at a particular vertex v is the sum of weights of all paths from the starting vertex s to v. The polynomial computed by the ABP is the polynomial computed at the end vertex t.

In terms of their power of computation, ABPs lie somewhere between arithmetic formula and general arithmetic circuits, in the following precise sense. An arithmetic formula can be converted into an ABP such that the number of vertices in the ABP is at most the number of vertices in the formula. On the other hand, an ABP can be transformed into an arithmetic circuit such that the number of vertices in the circuit is at most the sum of the number of edges and the number of vertices in the ABP[1]. Since arithmetic formula and ABP seem to be weaker models of computation than general arithmetic circuits, it is conceivable that proving lower bounds for them could be a more tractable challenge than proving lower bounds for general arithmetic circuits. In a way, this reflects in the current state of art where we know almost quadratic lower bounds for arithmetic formula [7, 13], whereas the best lower bounds known for arithmetic circuits or even ABPs continue to be the weakly super-linear [16, 2]. Moreover, to the best of our knowledge, even for *homogeneous* ABPs, prior to the results in this paper, no non-trivial super-linear lower bounds seem to be known on the number of vertices, whereas for the number of edges, the results in [16, 2] give an $\Omega(n \log n)$ lower bound[2]. We remark that in the setting of boolean circuit complexity it is possible to extend the formula lower bound of Nechiporuk [9] to show an $\Omega(n^{1+\epsilon})$ lower bounds for both deterministic and non-deterministic branching programs. However, such an extension is not known in the algebraic setting. The key difference stems from the fact that the edge labels for a boolean branching program are just individual literals or constants, as opposed to arbitrary affine forms as in the case of an algebraic branching program. And, indeed if we restrict Definition 1 so that every edge label is a field constant or an affine form in a single variable (and not a general affine form), then the formula lower bounds of Kalorkoti [7] do extend to such special cases and give a super-linear lower bound on the number of edges in an ABP. However, transforming a general ABP given by Definition 1 to this form seems to incur a blowup of factor n in the number of edges, and it is unclear if something non-trivial can be recovered via this approach.

We would like to remark that even though not much seems to be known for lower bounds for general algebraic branching programs, much progress has been made on the understanding

[1] These transformations also preserve homogeneity.

[2] Note that if an ABP computes a degree d polynomial, it must have at least $d+1$ vertices, since every edge contributes degree at most 1, and there must be a path with at least d edges to push the degree up to d. So, we think of this lower bound of $\Omega(d)$ on an ABP as *trivial*. Because of this, whenever we mention a (homogeneous) ABP lower bound for an n variate polynomial of degree d, we think of $d \leq n$, so that the trivial lower bound of d is at most linear in n.

of many restricted and more structured variants of algebraic branching programs; both from the point of view of lower bounds and deterministic polynomial identity testing. For instance, strongly superpolynomial lower bounds are known for non-commutative ABPs [10] and read k-oblivious ABPs [1]. For an overview of known polynomial identity testing results for read once oblivious algebraic branching programs, we refer the reader to the PhD thesis of Michael Forbes [6].

In this paper, we study the question of proving an improved lower bound for general algebraic branching programs. Our main result is a quadratic lower bound on the number of vertices for a general *homogeneous* ABP. To the best of our knowledge, this is the first such non-trivial superlinear lower bound. Also, this immediately implies a quadratic lower bound on the number of edges, improving the earlier bound of $\Omega(n \log n)$ [16, 2]. We now precisely state the theorem.

▶ **Theorem 2.** *Let $\mathbb{F}$ be a field of characteristic zero or relatively prime to d. Let B be a homogeneous algebraic branching program over the field $\mathbb{F}$ which computes the polynomial $P_{(n,d)}(\mathbf{x})$. Then, the number of vertices in B is at least $\Omega(nd)$.*

▶ Remark. Theorem 2 holds for a slightly more general class of branching programs than homogeneous branching programs. Our proof continues to hold if the number of non-trivial affine linear forms on any path from the start vertex s to the end vertex t is at most the degree of the polynomial computed. For our proofs, we consider this slightly more general model. In some sense, this generalization is a more natural model to study since the model is closed under affine transformations.

Picking $d = \Theta(n)$ would give us the desired quadratic lower bound. Based on the known results, there are two natural approaches to try for ABP lower bounds. The first would be to try and extend the proof of formula lower bounds in [7] to a general ABP. It is not clear if this approach can be made to work[3]. One major obstacle seems to be that the edge labels in the ABP are general affine forms, which seems to make it tricky to analyse the complexity measure used in [7] for an ABP. Another approach would be try and use the special structure of an ABP, and aim to get an improved analysis of the circuit lower bound obtained in [16, 2]. It is unclear to us if the original proofs in [16, 2] can be used to this end. One of the challenges with adapting the proofs in [16, 2] to obtain better ABP lower bounds seems to be that in the obvious conversion of an ABP to a circuit, the number of vertices in the circuit obtained is the sum of the number of vertices and the number of edges in the ABP. It seems tricky to extract any non-trivial bound on the number of vertices of the ABP from this transformation since the degree of every vertex in an ABP is unbounded in general. Even in the setting of number of edges, it is not apriori clear if a better lower bound can be proved using the proof in [16, 2].

For our proof in this paper, we essentially follow this high level strategy. On the way, we give an alternate proof of an $\Omega(n \log n)$ lower bound for homogeneous arithmetic circuits. The ideas in this proof turn out to be a bit more malleable and sensitive to the underlying model of computation than the original one, and indeed for a homogeneous ABP we obtain a better lower bound by a direct analysis which crucially relies on the structure of the ABP. Formally, we give an alternate proof of the following result.

[3] However, we do not know how to formally show that there is a nearly linear size ABP which has high complexity in terms of the measure used in [7].

▶ **Theorem 3** ([16, 2]). *Let $\mathbb{F}$ be a field of characteristic zero or relatively prime to d. Then, any homogeneous arithmetic circuit which computes the polynomial $P_{(n,d)}$ has at least $\Omega(n \log d)$ gates.*

The statement above is a special case of a classical result [16, 2], where they show a similar lower bound for all (not necessarily homogeneous) arithmetic circuits. For the original proof, Baur & Strassen [2] showed that if an n variate polynomial can be computed by an arithmetic circuit of size s, then all its partial derivatives can be computed by a multi-output circuit of size $O(s)$. They combined this structural result with an $\Omega(n \log d)$ lower bound on the size of multi-output arithmetic circuits, proved by Strassen [16]. Strassen's proof, in turn relies on a beautiful application of Bezout's theorem. Our proof does not rely on the Bezout's theorem directly but uses some other elementary properties of algebraic varieties. We enumerate the properties used in Section 2. It is not clear to us if our proof is any more elementary than the proof in [16, 2] or vice versa, although as we alluded to, it does seem to be more flexible to the underlying model than the original proof.

In a short and beautiful paper, Smolensky [15] gave a completely elementary proof of the $\Omega(n \log n)$ lower bound for general circuits. Smolensky's proof uses just elementary linear algebra, and therefore is definitely simpler than our proof of Theorem 3. However, it is not clear if this proof can be strengthened to show Theorem 2.

Determinantal Complexity

Another well known model of computation in algebraic complexity theory, which is relevant to the results in this paper is the notion of *determinantal complexity*, defined as follows.

▶ **Definition 4** (Determinantal complexity). Let $P \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ be a polynomial of degree d. The determinantal complexity of P is the smallest k such that there is a $k \times k$ matrix M with entries being affine forms in $\mathbb{F}[x_1, x_2, \ldots, x_n]$ such that $\text{Determinant}(M) = P$.

Perhaps not surprisingly, the state of known lower bounds on determinantal complexity is also fairly modest, with the best lower bound known being an $\frac{n}{2}$ lower bound for an n variate polynomial family [8, 4]. Over the field of real numbers, this bound was recently improved to n by Yabe [17].

We now state our last result where we give a simple proof of the lower bound for determinantal complexity of $P_{(n,d)}$.

▶ **Theorem 5** ([8, 4]). *Let $\mathbb{F}$ be a field of characteristic zero or characteristic $p \neq 2$ such that $2 \leq d < p$. Then, the determinantal complexity of $P_{(n,d)}$ over the field $\mathbb{F}$ is at least $n/2$.*

The original proofs of Theorem 5 of an $n/2$ lower bound on the determinantal complexity of the permanent of an $\sqrt{n} \times \sqrt{n}$ matrix due to Mignon and Ressayre [8] over fields of characteristic zero, and due to Cai, Chen and Li [4] over all fields of characteristic not equal to 2, both rely on analysing the rank of the Hessian matrix associated to the permanent. On the other hand, for our proof, we will formulate a criterion for proving determinantal complexity lower bound upto $n - o(n)$ for an n variate polynomial using elementary linear algebra. This part of the proof is completely elementary. We then show that the polynomial $P_{(n,d)}$ satisfies this criterion for some weaker choice of parameters. Also, our argument essentially remains the same over all fields. Interestingly, over the field of real numbers, we get a lower bound of n for $P_{(n,d)}$ as long as d is even. This matches an improvement of factor 2 shown recently by Yabe [17] for the determinantal complexity of the permanent over the field of real numbers. For the reals, our proof of an n lower bound turns out to be extremely simple.

Proof outline

The proofs of all the three theorems crucially rely on a structural property of the polynomial $P_{(n,d)}$, which we summarize in Lemma 6. A special case of this lemma, (see Corollary 14) is already quite interesting and sufficient for the *homogeneous* ABP and circuit lower bound proofs and appears to be known [12][4]. Our proof is along similar lines, but needs some more ideas.

▶ **Lemma 6.** *Let $\mathbb{F}$ be an algebraically closed field of characteristic zero or relatively prime to d. Let $\{Q_1, Q_2, \ldots, Q_k, R_1, R_2, \ldots, R_k\}$ be a set of polynomials in $\mathbb{F}[\mathbf{x}]$ such that the set of their common zeros $V = \mathbb{V}(Q_1, Q_2, \ldots, Q_k, R_1, R_2 \ldots, R_k)$ is non-empty. Let P be any polynomial in $\mathbb{F}[\mathbf{x}]$ of degree at most $d-1$, such that*

$$P_{(n,d)} = P + \sum_{i=1}^{k} Q_i \cdot R_i \,.$$

Then, $k \geq n/2$.

For the proofs of the main theorems, we use the linear algebraic and combinatorial structure of the models at hand (namely homogeneous ABP, homogeneous circuits and determinantal complexity) to reduce to an application of Lemma 6. Proofs of Theorem 2, Theorem 3 rely on multiple applications of Lemma 6, while the proof of Theorem 5 relies on a single application of a very special case of Lemma 6, which in itself has a very simple proof. The proof of Lemma 6 requires some properties of the dimension of varieties defined by polynomials of a special form, and we give a simple (though not completely self contained[5]) proof in Section 3.1.

Theorem 3 and Theorem 5 are two fundamental lower bounds in algebraic complexity theory and have been at the frontier of our understanding of lower bounds for these models for the past many years. Improving these bounds is perhaps one of the most important open problems in this line of research. Therefore, it seems desirable to have newer and alternative proofs of these results. Moreover, the original proofs of Theorem 5 and Theorem 3 were quite different from each other and the results themselves were proved almost two decades apart. On the other hand, it is interesting to note that the proofs in this paper give essentially unified arguments for both these statements, as well as for homogeneous ABP lower bounds (even though we can show a super-linear lower bound only for homogeneous arithmetic circuits). We would also like to remark that since the proof of Lemma 6 relies on the dimension of varieties, a quantity always upper bounded by the number of variables, it appears likely that we would need new ideas to push the lower bound on k to anything larger than n.

Organization of the paper

We set up some notations and preliminaries in Section 2 and prove some technical claims needed for the proofs in Section 3.1. We prove Theorem 2 and Theorem 3 in Section 3.2 and Theorem 5 in Section 3.3.

[4] Saptharishi attributes the proof to Kayal.
[5] The proof uses some known standard properties of algebraic varieties, which we do not prove here.

2 Preliminaries

We now list some notations that we follow.

- $\mathbb{F}$ denotes a general field, and $\mathbb{C}$ denotes the field of complex numbers.
- Without loss of generality, for the results in this paper, we think of the field $\mathbb{F}$ to be algebraically closed. This is because an arithmetic circuit, a branching program or a matrix over a field $\mathbb{F}$ can be viewed to be over the algebraic closure of $\mathbb{F}$.
- The degree of a monomial $x_i^{e_1}x_2^{e_2}\cdots x_n^{e_n}$ is defined to be equal to $\sum_{i=1}^{n} e_i$.
- The degree of a polynomial P is the degree of the highest degree monomial in P with a non-zero coefficient.
- We denote the set $\{x_1, x_2, \ldots, x_n\}$ by the set $\mathbf{x}$.
- We denote the set $\{1, 2, 3, \ldots, t\}$ by $[t]$.
- An affine form in $\mathbb{F}[\mathbf{x}]$ is a polynomial of the form $\alpha_0+\sum_{i=1}^{n}\alpha_i x_i$, where $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}$.
- We say that a polynomial P has *no constant term* if the homogeneous component of degree 0 of P is 0. In particular, for any polynomial $P \in \mathbb{F}[\mathbf{x}]$ with no constant term, $P(0, 0, \ldots, 0) = 0$.
- For a square matrix M, we denote the determinant of M by $\det(M)$.
- For every gate (or vertex) g in an arithmetic circuit or an algebraic branching program, we denote by $[g]$, the polynomial computed at g. For the starting vertex s of an ABP, we define the polynomial computed at s, denoted by $[s]$ to be 1.
- For any set $\{Q_1, Q_2, \ldots, Q_t\}$ of polynomials in $\mathbb{F}[\mathbf{x}]$, we denote by $\mathbb{V}(Q_1, Q_2, \ldots, Q_t)$ the affine variety (or simply variety) of $Q_1, Q_2, \ldots, Q_t$ in $\mathbb{F}^n$, which is defined as follows:

$$\mathbb{V}(Q_1, Q_2, \ldots, Q_t) = \{\mathbf{a} \in \mathbb{F}^n : \forall i \in [t], Q_i(\mathbf{a}) = 0\} .$$

- For any set $\{Q_1, Q_2, \ldots, Q_t\}$ of polynomials in $\mathbb{F}[\mathbf{x}]$, we define the ideal generated by $Q_1, Q_2, \ldots, Q_t$ defined as follows:

$$\mathbb{I}(Q_1, Q_2, \ldots, Q_t) = \left\{ \sum_{i=1}^{t} R_i \cdot Q_i : \forall i \in [t], R_i \in \mathbb{F}[\mathbf{x}] \right\} .$$

- For any variety $V \subseteq \mathbb{F}^n$, we define the ideal associated to this variety, denoted by $\mathbb{I}(V)$ as follows:

$$\mathbb{I}(V) = \{R : R \in \mathbb{F}[\mathbf{x}], \text{ and } \forall \mathbf{a} \in V, R(\mathbf{a}) = 0\} .$$

Algebraic branching programs, arithmetic circuits and determinantal complexity

We have already defined an algebraic branching program and determinantal complexity in Section 1.

We now recall the definition of an arithmetic circuit.

▶ **Definition 7** (Arithmetic circuits)**.** An arithmetic circuit on variables $\mathbf{x}$ over a field $\mathbb{F}$ is a directed acyclic graph, where the vertices (also called gates) with in-degree zero (called input gates or leaves) are labeled either by constants over $\mathbb{F}$ or with variables in $\mathbf{x}$. The internal vertices all have in-degree (or fan-in) 2 and are labeled by $+$ or $\times$, which indicate summation and multiplication operations over the field $\mathbb{F}$. The edges feeding into a $+$ gate can be labeled by field constants.

An arithmetic circuit formally computes a polynomial in the natural way. A circuit is said to be *homogeneous* if the polynomial computed at every vertex in the circuit is a homogeneous polynomial. The number of vertices in a circuit is the size of the circuit. Since we restrict ourselves to fan-in two circuits in this paper, the number of edges and the number of vertices are within a constant factor of each other. We refer the reader to the excellent survey by Shpilka and Yehudayoff [13] for an introduction to arithmetic circuits, and an over view of prior work in this area.

For an algebraic branching program, we note that the number of vertices and the number of edges need not be within a constant fraction of each other, since the in-degree and out-degree of internal vertices is both unrestricted. In this sense, a super-linear lower bound on the number of edges in an ABP need not necessarily imply a super-linear lower bound on the number of vertices. We also remark that that without loss of generality, we can assume that the underlying graph of an ABP is simple, i.e there is at most one edge between any pair of vertices. This follows from the fact that multiple edges can be combined into a single edge whose weight is the sum of weight of the original edges. Since edge weights are allowed to be arbitrary affine forms, this is a valid transformation for an ABP.

Ideals and varieties

A useful notion for our proofs will be that of an affine variety (or simply variety). For a field $\mathbb{F}$, a variety $V \subseteq \mathbb{F}^n$ is simply the set of common zeros of a set of polynomials in $\mathbb{F}[x_1, x_2, \ldots, x_n]$. Another relevant notion is the notion of an ideal. For a variety V, the ideal associated to V, denoted by $\mathbb{I}(V)$ is the set of all polynomials in $\mathbb{F}[\mathbf{x}]$ which vanish on V.

A fundamental property associated to an affine variety is its *dimension*, which takes a value between 0 and n. We do not formally define this, but this can be thought of as an appropriate generalization of the notion of dimension for linear spaces.

We refer the reader to the book by Cox, Little and O'Shea [5] for more on algebraic varieties and ideals and connections between them. For the proofs in this paper, we will rely on the following properties of dimension of a variety.

▶ **Lemma 8** (Section 2.8 in [14]). *Let S be a set of polynomials in n variables over an algebraically closed field $\mathbb{F}$ such that $|S| \leq n$. Let $V = \mathbb{V}(S)$ be the set of common zeros of polynomials in S.*

$$V = \{\mathbf{a} \in \mathbb{F}^n : \forall f \in S, f(\mathbf{a}) = 0\} .$$

If V is non-empty, then, the dimension of $V(S)$ is at least $n - |S|$.

The following two facts are basic properties of the dimension of a variety and can be found in Section 4 of Chapter 9 in [5].

▶ **Lemma 9.** *Let $\mathbb{F}$ be an algebraically closed field, and let $V_1 \subseteq \mathbb{F}^n$ and $V_2 \subseteq \mathbb{F}^n$ be two affine varieties such that $V_1 \subseteq V_2$. Then, the dimension of V_1 is at most the dimension of V_2.*

▶ **Lemma 10.** *Let $\mathbb{F}$ be an algebraically closed field and let $V \subseteq \mathbb{F}^n$ be an affine variety. Then, the dimension of V is zero if and only if V is finite.*

3 Proofs of main theorems

We now proceed to prove the results. We start with a technical lemma, which proves to be critical for all our main results. A special case of the lemma where each of the polynomials

Q_i and R_i is homogeneous and the polynomial P is identically zero seems to be known [12]. The statement in Lemma 6 is a generalization of this special case. The proof is along very similar lines, but needs a few more ideas.

3.1 Technical claims

For this section, we work over the field $\mathbb{C}$ of complex numbers, but the results continue to hold over any algebraically closed field of characteristic p such that p does not divide the parameter d. This ensures that certain partial derivatives which come up in the proofs do not vanish. We start with the following lemma.

▶ **Lemma 11** (Restatement of Lemma 6). *Let $\{Q_1, Q_2, \ldots, Q_k, R_1, R_2, \ldots, R_k\}$ be a set of polynomials in $\mathbb{C}[\mathbf{x}]$ such that the set of their common zeros $V = \mathbb{V}(Q_1, Q_2, \ldots, Q_k, R_1, R_2 \ldots, R_k)$ is non-empty. Let P be any polynomial in $\mathbb{C}[\mathbf{x}]$ of degree at most $d-1$, such that*

$$P_{(n,d)} = P + \sum_{i=1}^{k} Q_i \cdot R_i \,.$$

Then, $k \geq n/2$.

Proof. We prove the lemma via contradiction. If possible, let $k < n/2$. This implies that $n - 2k > 0$. From the hypothesis of the lemma, $\mathbb{V}(Q_1, Q_2, \ldots, Q_k, R_1, R_2, \ldots, R_k)$ is non-empty. Therefore, by Lemma 8, the dimension of $\mathbb{V}(Q_1, Q_2, \ldots, Q_k, R_1, R_2, \ldots, R_k)$ is at least $n - 2k > 0$.

For any variable $x_j \in \mathbf{x}$, observe that

$$\frac{\partial P_{(n,d)}}{\partial x_j} = \frac{\partial P}{\partial x_j} + \sum_{i=1}^{k} \frac{\partial Q_i}{\partial x_j} \cdot R_i + \sum_{i=1}^{k} Q_i \cdot \frac{\partial R_i}{\partial x_j} \,.$$

This implies that

$$dx_j^{d-1} - \frac{\partial P}{\partial x_j} = \sum_{i=1}^{k} \frac{\partial Q_i}{\partial x_j} \cdot R_i + \sum_{i=1}^{k} Q_i \cdot \frac{\partial R_i}{\partial x_j} \,.$$

It is easy to see that for every $x_j \in \mathbf{x}$, the right hand side in the equality above vanishes on every point in $\mathbb{V}(Q_1, Q_2, \ldots, Q_k, R_1, R_2, \ldots, R_k)$. Therefore,

$$\mathbb{V}(Q_1, Q_2, \ldots, Q_k, R_1, R_2, \ldots, R_k) \subseteq \mathbb{V}\left(\left\{dx_j^{d-1} - \frac{\partial P}{\partial x_j} : x_j \in \mathbf{x}\right\}\right) .$$

In particular, Lemma 9 implies that the dimension of $\mathbb{V}\left(\left\{dx_j^{d-1} - \frac{\partial P}{\partial x_j} : x_j \in \mathbf{x}\right\}\right)$ is at least $n - 2k$. Since P is a polynomial of degree at most $d-1$, each first order partial derivative of P is of degree at most $d-2$. Now, it follows from Lemma 12, (which we prove below) that the dimension of $\mathbb{V}\left(\left\{dx_j^{d-1} - \frac{\partial P}{\partial x_j} : x_j \in \mathbf{x}\right\}\right)$ is zero. Therefore, $n - 2k \leq 0$, but this is a contradiction for $k < n/2$. ◀

▶ **Lemma 12.** *Let d be a positive natural number. For every choice of polynomials $g_1, g_2, \ldots, g_n \in \mathbb{C}[\mathbf{x}]$ of degree at most $d-1$, the dimension of the variety $\mathbb{V}(x_1^d - g_1, x_2^d - g_2, \ldots, x_n^d - g_n)$ is zero.*

Proof. Let $V = \mathbb{V}(x_1^d - g_1, x_2^d - g_2, \ldots, x_n^d - g_n)$. To prove the lemma, we use Lemma 10. We show that the cardinality of V is at most $T = \binom{n+n(d-1)}{n}$. We prove this via contradiction. If the cardinality of V is larger than T, then we focus our attention on an arbitrary subset $S \subseteq V$ of size equal to $T+1$. Now, consider the linear space of polynomial functions from S to $\mathbb{C}$. Clearly, the dimension of this linear space must be at least $T+1$, since the indicator function of every point in S can be expressed as a sufficiently high degree polynomial and these polynomials are linearly independent. We now argue that the dimension of the linear space of all polynomial functions from V to $\mathbb{C}$ (and therefore from S to C) is upper bounded by T. This completes the proof by contradiction. To this end, we prove the following claim. Let $I = \mathbb{I}(V)$ be the ideal corresponding to V. Clearly, for every $i \in [n]$, $x_i^d - g_i \in I$.

▶ **Claim 13.** *Let P be any polynomial in $\mathbb{C}[\mathbf{x}]$ of degree Δ strictly larger than $n(d-1)$. Then, there exists a polynomial P'' of degree at most $n(d-1)$ and polynomials $h_1, h_2, \ldots, h_n$ such that*

$$P = P'' + \sum_{i=1}^{n} (x_i^d - g_i) \cdot h_i$$

Proof. Note that for every $x_i \in \mathbf{x}$, the polynomial P' obtained from P by replacing every occurrence of x_i^d by g_i is equivalent to P mod the ideal I, since $P - P'$ is divisible by $x_i^d - g_i$, which is in the ideal. So, we can keep performing this replacement while still maintaining equivalence modulo the ideal I. Note that the process terminates eventually, since x_i^d is being replaced by a polynomial of strictly smaller degree. Let P'' be the polynomial obtained when the process terminates. It follows that the individual degree of every variable x_i in P'' is upper bounded by $d-1$, and hence the degree of P'' is at most $n(d-1)$. This proves the claim. ◀

Therefore, the space of all polynomial functions from V to $\mathbb{C}$ is spanned by a subset of polynomials in $\mathbb{C}[\mathbf{x}]$ of degree at most $n(d-1)$. Hence, the dimension of this linear space is at most the number of monomials of degree at most $n(d-1)$ in n variables, which is equal to T. ◀

The following corollary of Lemma 6 is already interesting and seems to be well known [12].

▶ **Corollary 14.** *For every set $\{Q_1, Q_2, \ldots, Q_k, R_1, R_2, \ldots, R_k\}$ of homogeneous polynomials of degree at least 1, if*

$$P_{(n,d)} = \sum_{i=1}^{k} Q_i \cdot R_i \,.$$

Then, $k \geq n/2$.

3.2 Lower bound for homogeneous algebraic branching programs

In this section, we prove Theorem 2. We will in fact show that the theorem is true for a class of algebraic branching programs which are slightly more general than homogeneous ABPs. We say that an ABP has *formal degree* at most d, if the number of non-constant edge weights on any path from s to t is at most d. In general, we define the formal degree of any vertex v in an ABP to be the maximum number of non-constant edge weights along any path from s to v. We first argue that we can convert a homogeneous ABP computing a polynomial of degree d to an ABP of formal degree d.

▶ **Lemma 15.** *Let B be a homogeneous ABP with r vertices which computes a homogeneous polynomial P of degree d. Then, there is an ABP B' computing P such that B' has at most r vertices and has formal degree at most d.*

We defer the proof of this lemma to the end of this section, and use it to complete the proof of Theorem 2. We now prove the following structural lemma for ABPs of formal degree d.

▶ **Lemma 16.** *Let B be an algebraic branching program of formal degree at most d with b vertices, which computes an n-variate polynomial P of degree d. For any $i \in \{1, 2, 3, \ldots, d-1\}$, let $S_i = \{u_1, u_2, \ldots, u_m\}$ be the set of all vertices in B which compute a polynomial of degree equal to i. Then, there exist polynomials $h_1, h_2, \ldots, h_m$ and R of degree at most $d-1$ such that*

$$P = \sum_{j=1}^{m} [u_j] \cdot h_j + R$$

Proof. Let us consider all paths from the starting vertex s of B to the end vertex t of B which passes through some $u_j \in S_i$. The polynomial computed by the sum of weights of only these paths can be written as $[u_j] \cdot h_j$ where h_j is the polynomial given by the sum of weights of all paths from u_j to t. Now, we claim that the degree of h_j is at most $d - d_{u_j}$. This follows from the fact that if the degree of h_j was larger than $d - d_{u_j}$, then the formal degree of t will be larger than d which would contradict the hypothesis that B is of formal degree at most d.

We now use this observation to complete the proof of the lemma. Without loss of generality, let us assume that the vertices $u_1, u_2, \ldots, u_m$ are ordered in such a way that there is no directed path from u_j to $u_{j'}$ for any $j' > j$. We prove the following claim by a simple induction.

▶ **Claim 17.** *Fix any $j \in \{1, 2, 3, \ldots, m\}$. Then, there exists polynomials $h_1, h_2, \ldots, h_j$ of degree at most $d-1$ and a polynomial R_j computed by the ABP B'_j obtained from B by deleting all the vertices in $\{u_1, u_2, \ldots, u_j\}$ such that*

$$P = \sum_{k=1}^{j} [u_k] \cdot h_k + R_j \,.$$

Proof. For $k = 1$ the proof follows from the observation above. For the induction step, observe that in the ABP obtained by deleting the vertices $u_1, u_2, \ldots, u_k$, the polynomial computed by the vertex u_{k+1} is the same as the polynomial computed by the vertex u_{k+1} in the original ABP B. This is true since by our ordering of vertices $u_1, u_2, \ldots, u_m$ there are no directed paths from u_ℓ to $u_{\ell'}$ for any $\ell' > \ell$ in B. ◀

We now argue that the degree of R_m in Claim 17 is at most $d-1$. This would complete the proof of the lemma. Let B' be the ABP obtained from B by deleting all vertices in the set S_i in B. We know that R_t is the polynomial computed by B'. Let us consider any path $s, v_1, v_2, \ldots, v_k, t$ from s to t in B'. Note that all these vertices appear in the original ABP B. Let us consider the minimum j such that v_j has degree at least $i+1$ in B. Observe that the degree of v_{j-1} in B must be at most $i-1$, since we have deleted the vertices in S_i. Therefore, the degree of the monomials in the weight of the path $s, v_1, v_2, \ldots, v_k, t$ is at most $i - 1 + \ell + 1$ where ℓ is the maximum number of non-constant edge weights on any path from v_j to t in B. Now, observe that ℓ is at most $d - i - 1$. This is true since if $\ell \geq d - i$, then there would be a path in B from s to t through v_j such that there are at least $d+1$

non-constant edge weights on this path, thereby contradicting the hypothesis that the formal degree of B is at most d. ◀

We are now ready to complete the proof of Theorem 2.

▶ **Theorem 18** (Restatement of Theorem 2). *Let B be an algebraic branching program of formal degree at most d over $\mathbb{C}$ which computes the polynomial $P_{(n,d)}(\mathbf{x})$. Then, the number of vertices in B is at least $\Omega(nd)$.*

Proof. We partition the set of vertices in the ABP B, into $\Omega(d)$ many sets based on their degree. Then, we argue that each of these sets must have at least $n/2$ vertices. For $i \in \{1, \ldots, d-1\}$, let the set $S_i = \{u_1, u_2, \ldots, u_{t_i}\}$ be the set of all vertices in B which compute a polynomial of degree equal to i. From Lemma 16, we know that there are polynomials $h_{i,1}, h_{i,2}, \ldots, h_{i,t_i}$ and R_i of degree at most $d-1$ such that

$$P_{(n,d)} = \sum_{j=1}^{t_i} [u_j] \cdot h_{i,j} + R_i \,.$$

Let $[u_j]$ and $h_{i,j}$ be written as $[u_j] = [u_j]' + \alpha$ and $h_{i,j} = h'_{i,j} + \beta$ where α, β are constants and $[u_j]'$, $h'_{i,j}$ have no constant terms. Then,

$$[u_j] \cdot h_j = [u_j]' \cdot h'_{i,j} + Q_j$$

where Q_j has degree at most $d-1$. Therefore, without loss of generality, we get that there polynomials $h'_{i,1}, h'_{i,2}, \ldots, h'_{i,t_i}$ and R'_i such that

$$P_{(n,d)} = R'_i + \sum_{j=1}^{t_i} [u_j]' \cdot h'_{i,j}$$

where

- Degree of R'_i is most $d-1$.
- For every j, the constant term of each of the polynomials $[u_j]'$ and $h'_{i,j}$ is equal to zero and they have degree at least 1.

Note that since $[u_j]'$s and $h'_{i,j}$s have degree at least one and have no constant term, it follows that they vanish at the all zero point. In particular, $V = \mathbb{V}([u_1]', [u_2]', \ldots, [u_{t_i}]', h'_{i,1}, h'_{i,2}, \ldots, h'_{i,t_i})$ is non empty. So, by Lemma 6, it follows that t_i is at least $n/2$. Since this holds for all the $\Omega(d)$ values of i, and these sets S_i are all disjoint, this gives the desired lower bound on the number of vertices of B. ◀

We now prove Lemma 15.

Proof of Lemma 15. We will start with the ABP B and obtain an ABP B' by modifying or deleting some of the edge weights in B such that the polynomial computed by B' is the same as the polynomial computed by B. Moreover, B' will have the additional property that the degree of the homogeneous polynomial computed at every vertex v equals the formal degree of v. The proof will be via an induction, where we process vertices in the topological order, i.e we process a vertex v only after processing every vertex u such that (u, v) is an edge in B.

The base case of this induction is trivial as there is nothing to do for the starting vertex s.

For the induction step, we process a vertex v. Let $u_1, u_2, \ldots, u_m$ be all the vertices such that (u_j, v) is an edge in B. Let the weight of (u_j, v) be $\ell_j + \alpha_j$, where ℓ_j is a homogeneous

linear form (which could be identically zero) and α_j is a constant. Also, let d_{u_j} be the degree of $[u_j]$. So, we have the following identity:

$$[v] = \sum_{j=1}^{m} [u_j] \cdot (\ell_j + \alpha_j) \,.$$

We separate out the u_js based on their degree.

$$[v] = \sum_{j:d_v < d_{u_j}} [u_j] \cdot (\ell_j + \alpha_j) + \sum_{j:d_v = d_{u_j}} [u_j] \cdot (\ell_j + \alpha_j) + \sum_{j:d_v > d_{u_j}} [u_j] \cdot (\ell_j + \alpha_j) \,.$$

We now observe that since the polynomial computed at v and every u_j is homogeneous, and $[v]$ has degree d_v, the following identity is also true.

$$[v] = \sum_{j:d_v < d_{u_j}} [u_j] \cdot 0 + \sum_{j:d_v = d_{u_j}} [u_j] \cdot (\alpha_j) + \sum_{j:d_v > d_{u_j}} [u_j] \cdot (\ell_j + \alpha_j) \,.$$

So, in B', we replace the edge weights as follows:

- For every vertex u_j such that $d_{u_j} > d_v$, we delete the edge (u_j, v), and
- for every vertex u_j such that $d_{u_j} = d_v$ with the edge (u_j, v) having weight $\ell_j + \alpha_j$, we relabel it with α_j. ◀

3.2.1 Lower bound for homogeneous arithmetic circuits

The proof of Theorem 3 is along the lines of the proof of Theorem 2 that we described above. The main difference is that we partition the set of vertices in the circuit into $\Omega(\log d)$ sets based on their degrees defined as follows. For $i \in \{1, 2, \ldots, \log(d) - 1\}$, we define the set S_i to be the set of all vertices v in a homogeneous circuit C such that the degree d_v of the polynomial computed at v satisfies $2^i \leq d_v < 2^{i+1} - 1$. For this definition of the set S_i, a structural lemma analogous to Lemma 16 is true, and is easy to prove. Combining this with Lemma 6, would imply that the size of S_i is at least $\Omega(n)$. Since there are $\log d$ such sets, we get a bound of $\Omega(n \log d)$. We skip the rest of the details.

3.3 Lower bound on determinantal complexity

In this section, we complete the proof of Theorem 5. We start by proving the following lemma.

▶ **Lemma 19.** *Let $Q \in \mathbb{F}[\mathbf{x}]$ be a homogeneous polynomial of degree d. Let M be a $t \times t$ matrix, whose entries are affine forms in the variables $\mathbf{x}$, such that*

$$\det[M] = Q \,.$$

Then, there exists a linear subspace S of dimension at least $n - t$, such that $Q(\mathbf{a}) = 0, \forall \mathbf{a} \in S$.

Proof. Since the entries of M are affine functions in the variables in $\mathbf{x}$, we can write M as

$$M(\mathbf{x}) = M_0 + \sum_{i=1}^{n} M_i x_i \,.$$

Here, $M_0, M_1, \ldots, M_n$ are $t \times t$ matrices over $\mathbb{F}$. Since Q is homogeneous, it follows that

$$Q(0, 0, \ldots, 0) = 0,$$

it follows that $\det[M_0] = 0$. Therefore, M_0 is not full rank. Hence, there is a non-zero vector $v \in \mathbb{F}^t$, which is in the kernel of v, i.e $M_0 v = 0$. Let us consider the set $S \subseteq \mathbb{F}^n$, defined as

$$S = \left\{ (a_1, a_2, \ldots, a_n) \in \mathbb{F}^n : \left(\sum_{i=1}^{n} M_i a_i \right) \cdot v = 0 \right\} .$$

In other words, S is the set of all vectors $\mathbf{a}$ in $\mathbb{F}^n$ such that the vector v is in the kernel of $\sum_{i=1}^{n} M_i a_i$. Observe that this implies that v is in the kernel of $M(\mathbf{a})$, since it is already in the kernel of M_0, by choice. Thus, $M(\mathbf{a})$ is rank deficient for $\mathbf{a} \in S$. Hence, $\det(M(\mathbf{a})) = 0$ for every $\mathbf{a} \in S$. Moreover, since S is a linear space of dimension at least $n - t$, it follows that Q is zero on every point on a subspace of dimension at least $n - t$. ◀

Observe that from the degree requirements, it follows that the determinantal complexity of a degree d polynomial is at least d. Hence, if we can construct an explicit polynomial of degree $d = o(n)$ such that it does not vanish on any linear subspace of dimension larger than $k(n, d)$, then from Lemma 19, we will obtain a lower bound of $n - k$. It is known that at least over small fields a random homogeneous polynomial of degree d in n variables does not vanish on any affine subspace of dimension much larger than $n^{O(1/d)}$ [3]. Therefore, in principle, d can be taken as small as $O(\log n)$ and $k = O(1)$ over such fields. The challenge is to construct such polynomial families explictly. Over small fields constructions of this nature are known, although the parameters seem to be far from what would be true for a random polynomial, see for example [3]. Even beyond the application to minor improvements in known determinantal complexity lower bounds, explicit construction of such *subspace evasive* polynomials is an extremely interesting open question.

We now observe that the polynomial $P_{(n,d)}$ already lets us recover the $n/2$ lower bound on determinantal complexity over the field of complex numbers and any field of characteristic p not equal to 2. For fields of characteristic equal to p, our proof would work, for instance if we pick d such that $2 \leq d < p$. In fact, over reals, we get a lower bound of n for $P_{(n,d)}$ for every even d. As alluded to in the introduction, such a lower bound of n was proved over reals by Yabe [17] for the permanent of an $\sqrt{n} \times \sqrt{n}$ matrix via a very different proof.

A useful notion for the rest of proof will be the notion of a *formal* restriction of a polynomial to a linear space, which is defined using the following observation.

▶ **Observation 20.** *Let $S \subseteq \mathbb{F}^n$ be any linear space of co-dimension equal to t and let P be any polynomial in $\mathbb{F}[\mathbf{x}]$. Then, there exists a subset V of variables $\mathbf{x}$ of size equal to $n - t$ and a polynomial Q_t depending only on the variables in V such that*

- *The degree of Q_t is at most the degree of P.*
- *For every $\mathbf{a} \in S$, $P(\mathbf{a}) = Q_t(\mathbf{a})$.*

Proof. Since S is a linear space of co-dimension t, it follows that there are coordinates $\{i_1, i_2, \ldots, i_t\}$ and linear forms $L_1, L_2, \ldots, L_t$ depending only on variables outside $\{i_1, i_2, \ldots, i_t\}$, such that

$$S = \left\{ \mathbf{a} \in \mathbb{F}^n : \forall j \in [t], a_{i_j} - L_j(\mathbf{a}) = 0 \right\} .$$

We define $V = \mathbf{x} \setminus \{x_{i_1}, x_{i_2}, \ldots, x_{i_t}\}$. Without loss of generality, we assume that $i_j = j$. Let Q_i be obtained from P by replacing the variables $x_1, x_2, \ldots, x_i$ in P by $L_1, L_2, \ldots, L_i$. By induction on i, it can be observed that

$$P - Q_i = \sum_{j=1}^{i} (x_j - L_j) \cdot R_j$$

where R_j is a polynomial of degree at most $d-1$. Moreover, by construction, Q_i does not depend on the variables $x_1, x_2, \ldots, x_i$. Now, from the definitions, we get that for any $\mathbf{a} \in S$,

$$P(\mathbf{a}) = Q(\mathbf{a})\,.$$

Since each Q_i is obtained from P by a linear transformation of the set of variables, the degree does not increase in the process. ◀

We call the polynomial Q_t obtained in the proof to be a formal restriction of P on S. We also get the following useful corollary.

▶ **Corollary 21.** *Let $\mathbb{F}$ be any field with at least $d+1$ elements, and let $P \in \mathbb{F}[\mathbf{x}]$ be any homogeneous polynomial of degree d. If S is a subspace of $\mathbb{F}^n$ of co-dimension t such that P evaluates to zero on S, then, there exist homogeneous linear forms $\ell_1, \ell_2, \ldots, \ell_t$ and homogeneous polynomials $R_1, R_2, \ldots, R_t$ of degree $d-1$ such that*

$$P = \sum_{i=1}^{t} \ell_i \cdot R_i\,.$$

Proof. The polynomial Q_t obtained in Observation 20 satisfies

$$P - Q_t = \sum_{i=1}^{t} (x_i - L_i) \cdot R_i$$

where each L_i is a homogeneous linear form, and each R_i is a homogeneous polynomial of degree $d-1$. Moreover, Q_t depends only on the un-restricted variables $x_{t+1}, x_{t+2}, \ldots, x_n$, and is of degree at most d, and for every $j \in \{1, 2, \ldots, t\}$ and $\mathbf{a} \in S$, $a_j = L_j(\mathbf{a})$. Since P evaluates to zero everywhere on S, it follows that $Q_t \in \mathbb{F}[x_{t+1}, x_{t+2}, \ldots, x_n]$ evaluates to zero everywhere on the grid $\mathbb{F} \times \mathbb{F} \times \ldots \times \mathbb{F}$. Since $\mathbb{F}$ has at least $d+1$ elements and Q_t is of degree at most d, by the Schwartz-Zippel lemma, Q_t must be identically zero. So,

$$P = \sum_{i=1}^{t} (x_i - L_i) \cdot R_i\,.$$ ◀

We now complete the proof of Theorem 5. We present the proof over the field of complex numbers, but it will be clear from the proof that the statement is true for any finite field of characteristic $p \neq 2$ such that the degree d of $P_{(n,d)}$ satisfies $2 \leq d < p$.

Proof of Theorem 5. Let M be a $t \times t$ matrix of affine forms over $\mathbb{C}[\mathbf{x}]$ such that

$$P_{(n,d)} = \det[M]$$

From Lemma 19, it follows that there is a linear subspace $S \in \mathbb{C}^n$ of dimension at least $n - t$ such that

$$P_{(n,d)}(\mathbf{a}) = 0, \forall \mathbf{a} \in S$$

From Corollary 21, it follows that there exist t homogeneous linear forms $\ell_1, \ell_2, \ldots, \ell_t$ and homogeneous polynomials $R_1, R_2, \ldots, R_t$ of degree equal to $d-1$, such that

$$P_{(n,d)} = \sum_{i=1}^{t} \ell_i \cdot R_i$$

From Lemma 6, we get that $t \geq n/2$. ◀

▶ Remark. Over reals, this argument gives a simple proof of the currently best lower bound of n for the polynomial $x_1^2 + x_2^2 + \ldots + x_n^2$ since this polynomial has exactly one zero in $\mathbb{R}^n$ and in particular, is not zero on any linear subspace of non-trivial dimension.

4 Open problems

We end with some open problems.

- The most interesting question here would be to extend the results here and prove a quadratic lower bound for general (possibly non-homogeneous) algebraic branching programs. Lemma 16 is not true for a general ABP and hence the proofs in this paper do not extend to the non-homogeneous setting.
- Another question of interest is to construct explicit polynomials of low degree which do not vanish on very large linear subspaces over all fields. Beyond the application to minor improvements in the determinantal complexity lower bounds, this seems to be a natural algebraic question.
- Of course, improving the lower bounds here is an extremely interesting problem. In fact, it is known that proving a super-quadratic lower bound for general algebraic branching programs implies a super-linear lower bound for determinantal complexity (see for example [17]). Perhaps the first step towards this goal could be to prove super-quadratic lower bound for homogeneous formulas. Currently, no such bounds are known.

Acknowledgments. I am thankful to Prahladh Harsha, Swastik Kopparty and Ramprasad Saptharishi for helpful discussions, and to Josh Grochow for pointing out a reference ([14]) for Lemma 8. Also, many thanks to Pooya Hatami and Mike Saks for sitting through a presentation of the proof and to Prahladh for comments on the writing which helped improve the presentation of the paper.

References

1 Matthew Anderson, Michael A. Forbes, Ramprasad Saptharishi, Amir Shpilka, and Ben Lee Volk. Identity testing and lower bounds for read-k oblivious algebraic branching programs. In *Proceedings of the 31st Annual Computational Complexity Conference (CCC 2016)*, volume 50 of *LIPIcs*, pages 30:1–30:25, 2016. doi:10.4230/LIPIcs.CCC.2016.30.

2 Walter Baur and Volker Strassen. The complexity of partial derivatives. *Theoretical Computer Science*, 22:317–330, 1983. doi:10.1016/0304-3975(83)90110-X.

3 Eli Ben-Sasson and Swastik Kopparty. Affine dispersers from subspace polynomials. *SIAM J. Comput.*, 41(4):880–914, 2012. doi:10.1137/110826254.

4 Jin-yi Cai, Xi Chen, and Dong Li. Quadratic lower bound for permanent vs. determinant in any characteristic. *Computational Complexity*, 19(1):37–56, 2010. doi:10.1007/s00037-009-0284-2.

5 David A. Cox, John B. Little, and Donal O'Shea. *Ideals, Varieties and Algorithms*. Undergraduate texts in mathematics. Springer, 2007. doi:10.1007/978-0-387-35651-8.

6 Michael A. Forbes. *Polynomial Identity Testing of Read-Once Oblivious Algebraic Branching Programs*. PhD thesis, Massachusetts Institute of Technology, 2014.

7 Kyriakos Kalorkoti. A Lower Bound for the Formula Size of Rational Functions. *SIAM Journal of Computing*, 14(3):678–687, 1985. doi:10.1137/0214050.

8 Thierry Mignon and Nicolas Ressayre. A quadratic bound for the determinant and permanent problem. *International Mathematics Research Notes*, 2004(79):4241–4253, 2004. doi:10.1155/S1073792804142566.

9 E. I. Nechiporuk. On a boolean function. *Soviet Math. Dokl.*, pages 999–1000, 1966.

10 Noam Nisan. Lower bounds for non-commutative computation. In *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing (STOC 1991)*, pages 410–418, 1991. doi:10.1.1.17.5067.

11 Ramprasad Saptharishi. A survey of lower bounds in arithmetic circuit complexity. Github survey, 2015. URL: https://github.com/dasarpmar/lowerbounds-survey/releases/.

12 Ramprasad Saptharishi. personal communication, 2016.

13 Amir Shpilka and Amir Yehudayoff. Arithmetic circuits: A survey of recent results and open questions. *Foundations and Trends in Theoretical Computer Science*, 5:207–388, March 2010. doi:10.1561/0400000039.

14 J. Smith. *Introduction to Algebraic Geometry*. Textbooks in Mathematics. Taylor & Francis, 2014.

15 Roman Smolensky. Easy lower bound for a strange computational model. *Computational Complexity*, 6(3):213–216, 1997. doi:10.1007/BF01294255.

16 V. Strassen. Die Berechnungskomplexiät von elementarsymmetrischen Funktionen und von Interpolationskoeffzienten. *Numerische Mathematik*, 20:238–251, 1973.

17 Akihiro Yabe. Bi-polynomial rank and determinantal complexity. *CoRR*, abs/1504.00151, 2015. URL: http://arxiv.org/abs/1504.00151.