Electronic Colloquium on Computational Complexity, Report No. 129 (2020)

A Lower Bound on Determinantal Complexity

Mrinal Kumar* Ben Lee Volk†

Abstract

The determinantal complexity of a polynomial $P \in \mathbb{F}[x_1, \ldots, x_n]$ over a field $\mathbb{F}$ is the dimension of the smallest matrix M whose entries are affine functions in $\mathbb{F}[x_1, \ldots, x_n]$ such that $P = \mathsf{Det}(M)$. We prove that the determinantal complexity of the polynomial $\sum_{i=1}^{n} x_i^n$ is at least $1.5n - 3$.

For every n-variate polynomial of degree d, the determinantal complexity is trivially at least d, and it is a long standing open problem to prove a lower bound which is super linear in $\max\{n, d\}$. Our result is the first lower bound for any explicit polynomial which is bigger by a constant factor than $\max\{n, d\}$, and improves upon the prior best bound of $n + 1$, proved by Alper, Bogart and Velasco [ABV17] for the same polynomial.

1 Introduction

1.1 Computing with Determinants

The *determinantal complexity* of a polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$, denoted $\mathsf{dc}(f)$, is the minimal integer m such that there exists an affine map $L : \mathbb{F}^n \to \mathbb{F}^{m \times m}$ such that $f(\mathbf{x}) = \mathsf{Det}(L(\mathbf{x}))$, where for every square matrix M, $\mathsf{Det}(M)$ denotes the determinant of M.

This notion was first implicitly defined by Valiant [Val79], and it is tightly related to the VP vs. VNP problem, the algebraic analog of the P vs. NP problem. The essence of the VP vs. VNP problem is showing that some explicit polynomials are hard to compute. By defining natural notions of reductions and completeness, Valiant showed that this problem is in fact equivalent to showing that, for fields of characteristic different than two, the determinantal complexity of the permanent polynomial,

$$\mathsf{Perm}_n(X) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} x_{i,\sigma(i)},$$

doesn't grow like a polynomial function in n.[1]

This fact is a consequence of the *completeness* property of the determinant: Valiant showed that if f has an algebraic formula of size s, then the determinantal complexity of f is at most s. This remains true even if f has an *algebraic branching program* (ABP) of size s: ABPs are a natural and more powerful model of computation than formulas. We refer to [SY10] and [Sap15] for more background on algebraic complexity theory and for proofs of these statements.

Thus, Valiant also established en passant the non-obvious fact that the determinantal complexity of every polynomial is finite, and it's at most roughly $\binom{n+d}{n}$ for every n-variate polynomial

*Department of Computer Science & Engineering, IIT Bombay. Email: mrinal@cse.iitb.ac.in

†Department of Computer Science, University of Texas at Austin, USA. Part of this work done while at the Center for the Mathematics of Information, California Institute of Technology, USA. Email: benleevolk@gmail.com

[1] Strictly speaking, the VP vs. VNP question is equivalent to showing that the determinantal complexity of the Perm_n is at least $n^{\omega(\log n)}$, but we skip over this fine grained detail for now.

ISSN 1433-8092

of degree d. Standard counting arguments also show that this estimate is close to being tight for almost every such polynomial.

The benefit of this reformulation of the VP vs. VNP problem is that it appears to strip away altogether the notion of "computation": indeed, this problem can be stated without even defining a computational model in any standard sense of the word, and thus it can potentially be proved without having to argue about the topology or structure of every possible arithmetic computation.

In practice, however, proving lower bounds on determinantal complexity is (unsurprisingly) difficult. Currently, for n-variate polynomials, there are no known lower bounds which are super-linear in n (see Section 1.2 for more details on previous work). Due to the completeness property mentioned above, a lower bound of s on the determinantal complexity of f will imply the same lower bound for algebraic formulas and even algebraic branching programs. However, super-linear lower bounds for formulas are well-known for decades [Kal85], and super-linear lower bounds for ABPs were recently established in [CKSV19], so there doesn't seem to be any major complexity-theoretic barrier for proving such lower bounds for determinantal complexity: the main obstacle is seemingly lack of techniques for reasoning about computations using determinants, and hence it is important to study this model and to develop techniques to understand it and to prove lower bounds, for the permanent as well as for other explicit polynomials.

Even for the purpose of separating VP and VNP, one need not necessarily prove a lower bound on the determinantal complexity of the permanent; the same conclusion will hold if the lower bound on determinantal complexity is shown for any "explicit" polynomial (formally, in the class VNP, which we don't define here) in lieu of the permanent.

Before we describe the previous work concerning determinantal complexity, we provide a brief remark about the notion of a "trivial" lower bound in this context which is worth remembering when evaluating the previous results (and our result). Unlike most standard computational models, observe that for an n-variate polynomial of degree d, even a lower bound of n is non-trivial for determinantal complexity. This is because every coordinate of the affine map L can depend on all n variables. Nevertheless, since the determinant of an $m \times m$ matrix is a degree m polynomial, and thus $\mathsf{Det}(L(\mathbf{x}))$ is a degree m polynomial for every affine map L, the degree d *is* a trivial lower bound on the determinantal complexity of f. Therefore, it is natural to consider polynomial families in which $d \leq n$ or alternatively to hope to prove lower bounds stronger than $\max\{n, d\}$.

1.2 Previous work

The early work on determinantal complexity mostly focused on proving lower bounds for the permanent. Recall that the $n \times n$ permanent, Perm_n, is a degree n polynomial, so the trivial lower bound is $\mathsf{dc}(\mathsf{Perm}_n) \geq n$. Since over characteristic 2 the permanent and determinant coincide, the results described here hold for characteristic not equal to 2.

Already in 1913, Szegő [Sze13], answering a question of Pólya [Pól13], showed that there's no way to generalize the 2×2 identity

$$\mathsf{Perm}\begin{pmatrix} x_{1,1} & x_{1,2} \\ x_{2,1} & x_{2,2} \end{pmatrix} = \mathsf{Det}\begin{pmatrix} x_{1,1} & x_{1,2} \\ -x_{2,1} & x_{2,2} \end{pmatrix}$$

by affixing $\pm$ signs to an $n \times n$ matrix of variables for $n \geq 3$.

Marcus and Minc [MM61] strengthened this result by showing that for every n, $\mathsf{dc}(\mathsf{Perm}_n) > n$. Subsequent work by von zur Gathen [vzG87], Babai and Seress (see [vzG87]), Cai [Cai90] and Meshulam [Mes89] obtained the slightly stronger lower bound $\mathsf{dc}(\mathsf{Perm}_n) \geq \sqrt{2}n$.

Mignon and Ressayre [MR04] greatly improved the lower bound by proving $\mathsf{dc}(\mathsf{Perm}_n) \geq n^2/2$, over the complex numbers. Cai, Chen and Li [CCL10] extended this lower bound to fields of positive characteristic different than two, and Landsberg, Manivel and Ressayre [LMR13]

extended this result to the *border* version of determinantal complexity, that is, they showed that the permanent is not even in the closure of polynomials with determinantal complexity less than $n^2/2$. Finally, Yabe [Yab15] obtained an improved lower bound of $(n-1)^2+1$ over the real numbers.

However, while these lower bounds are quadratic in the degree, Perm_n is a polynomial with n^2 many variables, and notably none of these lower bounds is larger than the number of variables. In particular, these results don't even recover a weak form of the n^3 formula lower bound of Kalorkoti for Perm_n [Kal85].

Landsberg and Ressayre [LR17] considered determinantal representations that respect certain symmetries (which they called *equivariant determinantal complexity* and denoted edc), and proved that $\mathsf{edc}(\mathsf{Perm}_n)$ is exponential in n. It's unclear how stringent the symmetry requirement is; Ladnsberg and Ressayre put forward the ambitious conjecture that edc and dc are polynomially related, which, if true, would imply $\mathsf{VP} \neq \mathsf{VNP}$. To the best of our knowledge, this conjecture remains open, but it's worth mentioning that in the context of *regular determinantal complexity*, another notion defined and studied by [LR17], it can be shown unconditionally that requiring symmetry may result in a super-polynomial blow-up.[2]

The question of lower bounds for other explicit polynomial was also considered: Mignon and Ressayre [MR04] proved that the determinantal complexity of quadratic polynomials of rank r is *exactly* $\lceil (r+1)/2 \rceil$ (this, of course, cannot give a lower bound beyond $\lceil (n+1)/2 \rceil$). Chen, Kayal and Wigderson [CKW11] observed that the technique of Mignon and Ressayre implies an $n/2$ lower bound on the determinantal complexity of the elementary symmetric polynomial of degree 2, $\sum_{1 \leq i < j \leq n} x_i x_j$. Kumar [Kum19] used a different technique to prove a similar lower bound for the power symmetric polynomials $\sum_i x_i^d$ for $d \geq 2$ over $\mathbb{C}$.

The last lower bound was improved in a recent work of Alper, Bogart and Velasco [ABV17]: an immediate corollary of their main theorem is that $\mathsf{dc}\left(\sum_i x_i^d\right) \geq n+1$, for every $d \geq 2$. Note that this lower bound is (only slightly) larger than the number of variables n, and until this work, this is the only lower bound we're aware of that has this feature. The results of Alper et al. are more general, and are stated as a function of the co-dimension of the singular locus of the polynomial, a notion we use as well (see Section 3). In particular they are able to prove that $\mathsf{dc}(\mathsf{Perm}_3) = 7$, but their main statement can't imply any lower bound stronger than $n+1$ for an n-variate polynomial.

1.3 Our result

Our main result is the following theorem.

Theorem 1.1. *For every natural number $n \geq 6$, the determinantal complexity of the polynomial $\sum_{i=1}^{n} x_i^n$ over the field of complex numbers is at least $1.5n - 3$.*

Although for simplicity we state our results for the complex numbers, all the results in this paper also hold for algebraically closed fields of positive characteristic p, as long as p doesn't divide n. This assumption is not only an artifact of the proof. For example, when $n = p^k$, and

[2] The *regular* determinantal complexity of a polynomial f is the smallest integer m such that there is an $m \times m$ matrix $M(\mathbf{x})$ of linear forms such that $f(\mathbf{x}) = \mathsf{Det}(M(\mathbf{x}))$ and $\mathsf{rank}(M(\mathbf{0})) = m-1$. This definition is motivated by the fact that for the permanent and for many other polynomials, every determinantal representation is regular, without loss of generality (see Lemma 3.5). The regular determinantal complexity of every polynomial f with size s formula is at most $s+1$, as can be witnessed by the reductions in Exercise 13.2 of [CKW11] or Section 3.3.1 of [Sap15], which satisfy the regularity property. Since the determinant polynomial Det_n has a formula of size $n^{O(\log n)}$, this implies a similar upper bound on its regular determinantal complexity, while Landsberg and Ressayre [LR17] proved that the *equivariant* regular determinantal complexity of Det_n is exponential.

over characteristic p,

$$\sum_{i=1}^{p^k} x_i^{p^k} = \left(\sum_{i=1}^{p^k} x_i\right)^{p^k}$$

has determinantal complexity at most $n = p^k$; it is also a polynomial of degree n, so its determinantal complexity is at least, and hence equals, n.

As discussed in Section 1.2, this is the first non-trivial[3] lower bound of the form $(1+\epsilon)n$, for any $\epsilon > 0$ for any explicit n variate polynomial family, and improves the previous best bound of $n+1$ by Alper, Bogart and Velasco [ABV17] by a constant factor.

This result, of course, is not fully satisfactory. The best upper bound we're aware of for $\mathsf{dc}(\sum_{i=1}^n x_i^n)$ is $O(n^2)$, which follows from converting the natural algebraic formula or ABP computing this polynomial to a determinantal expression. We suspect that the true complexity might be $\Omega(n^2)$ or at the very least $\omega(n)$.

Quantitatively, the situation here is somewhat similar to the case of lower bounds on the rank of 3-dimensional tensors, where the best lower bounds are only a constant factor away from the trivial lower bound, and proving super-linear lower bounds remains a challenging open problem (cf. [AFT11, BD80, Blä99, Shp01], among others).

We now give an outline of the main ideas in our proof.

1.4 Overview of the proof

Let $M \in \mathbb{F}[x_1, x_2, \ldots, x_n]^{m\times m}$ matrix of affine functions such that $\sum_{i=1}^n x_i^n = \mathsf{Det}(M(\mathbf{x}))$. Theorem 1.1 shows a lower bound of $1.5n-3$ on m. There are essentially three main ingredients to the proof of Theorem 1.1, and we now discuss them in some more detail.

Converting the matrix M into a normal form

Let $M_0 \in \mathbb{F}^{m\times m}$ be the *constant part* of the matrix M, i.e. $M_0 = M(\mathbf{0})$. As a first step of our proof, we show (in Lemma 3.2) that without loss of generality, M_0 can be assumed to be a diagonal matrix of rank equal to $m-1$. We a say that a matrix M is in *normal form* if it has this additional structure.

Is is quite easy to observe that the rank of M_0 is at most $m-1$. However, for technical reasons, we actually need the lower bound on the rank as well, and this fact is a consequence of comparing the dimensions (as algebraic varieties) of the singular locus (which is just the the set of zeroes of a polynomial of multiplicity at least two) of the determinant and that of the polynomial $\sum_{i=1}^n x_i^n$. Observations of this nature have been used in the context of determinantal complexity lower bounds before, and indeed, we crucially rely on a well known lemma of von zur Gathen (see Fact 3.4) for the proof. The details can be found in Section 3.1.

Determinantal complexity of higher degree polynomial maps

As the key ingredient of our proof, we show that for any matrix $M(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]^{m\times m}$ where the entries of M are polynomials of degree at most $n-1$ and M is in normal form, if $\mathsf{Det}(M(\mathbf{x})) = \sum_{i=1}^n x_i^n$, then $m \geq n/2$. Moreover, roughly the same lower bound continues to hold as long as $\det(M) = (\sum_{i=1}^n x_i^n)\,(1+Q)$ for any polynomial Q, with $Q(\mathbf{0}) = 0$.

Thus, this is a significant generalization of the $n/2$ lower bound on the standard notion determinantal complexity (where the entries of M are affine functions) of $\sum_{i=1}^n x_i^n$ as shown in [Kum19]: this shows that roughly the same lower bound continues to hold even when the entries

[3] This means that the degree of the polynomials is at most the number of variables.

of the matrix are arbitrary polynomials of degree as high as $n-1$ and the determinant of the matrix equals an arbitrary multiple of $\sum_{i=1}^{n} x_i^n$ with a non-zero constant term.

The proof of the lemma relies on the observation that the polynomial $\sum_{i=1}^{n} x_i^n$ does not vanish with multiplicity at least two very often. This seemingly simple observation has been previously used in the context of lower bounds on algebraic branching programs computing this polynomial [Kum19, CKSV19] in a crucial way. See Section 3.2 for further details.

Trading dimension of the matrix for degree

As the final ingredient of our proof, we use a well known property of determinants (Lemma 3.8) to show that if there is an $m \times m$ matrix M whose entries are affine functions and $\mathsf{Det}(M) = \sum_{i=1}^{n} x_i^n$, then there is an $(m-n+2) \times (m-n+2)$ matrix N whose entries are polynomials of degree at most $n-1$ and $\mathsf{Det}(N) = (\sum_{i=1}^{n} x_i^n)(1+Q)$ for a polynomial Q which vanishes at zero. Moreover, if the matrix M is in normal form, then the matrix N continues to be in normal form.

Thus, we are in a setup where we can invoke the lower bound in Lemma 3.9 discussed earlier and we get that the dimension of N which equals $m-n+2$ must be at least $n/2-1$, thereby implying that m is at least $1.5n-3$. The details of this step can be found in Section 3.3.

2 Preliminaries

In this paper $\mathbb{F}$ always denotes an algebraically closed field. We use $\mathbf{x}$ to denote a tuple of n variables $x_1, \ldots, x_n$, where n is understood from the context (or is otherwise explicitly mentioned).

We consider polynomial maps $M : \mathbb{F}^n \to \mathbb{F}^{m \times m}$ given by m^2 polynomials $(M_{i,j})_{i,j \in [m]}$. The same object can be thought of as a matrix of polynomials $M(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]^{m \times m}$ and we use both points of view interchangeably. The degree of M is the maximum degree of its coordinates, i.e., $\deg M = \max_{i,j} \deg M_{i,j}$.

Each $M(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]^{m \times m}$ can be uniquely written as $M(\mathbf{x}) = M'(\mathbf{x}) + M_0$, where $M_0 \in \mathbb{F}^{m \times m}$ and in all m^2 coordinates of M', the constant term is zero. We then call M_0 the *constant part* of the map. A polynomial in which the constant term is zero is called *constant free*, and a polynomial map is called constant free if all of its coordinates are constant free, i.e., in the above decomposition, $M_0 = 0$.

We denote the determinant polynomial by Det. In cases where it is important to emphasize the dimension of the matrices in question we write it in the subscript, so for example the $m \times m$ determinant polynomial is denoted by Det_m.

Determinantal Complexity

We now formally define the notion of determinantal complexity, which is the focus of this paper.

Definition 2.1 (Determinantal Complexity)**.** *The determinantal complexity of a polynomial $P \in \mathbb{F}[\mathbf{x}]$ is defined as the minimum $m \in \mathbb{N}$ such that there is a $m \times m$ matrix $M \in \mathbb{F}[\mathbf{x}]$ whose entries are polynomials of degree at most one such that*

$$P = \mathsf{Det}(M)\,. \qquad \Diamond$$

Remark 2.2. *The above definition naturally generalizes to a family of polynomials in the following sense. A family $\{P_n\}_{n \in \mathbb{N}}$ of polynomials is said to have determinantal complexity at most $f(n) : \mathbb{N} \to \mathbb{N}$ if there exists an $n_0 \in \mathbb{N}$, such that for every $n \geq n_0$, the determinantal complexity of P_n is at most $f(n)$.* $\Diamond$

3 A lower bound on determinantal complexity

This section will be devoted for a proof of Theorem 1.1. We begin with the following lemma, which was instrumental in the recent proofs of lower bounds for algebraic formulas and algebraic branching programs.

Lemma 3.1 ([CKSV19, Kum19])**.** *Let $d \geq 2$ be a natural number. Let $P_1, P_2, \ldots, P_t, Q_1, \ldots, Q_t$, $R \in \mathbb{C}[\mathbf{x}]$ be polynomials such that $\deg(R) < d$, $P_1, \ldots, P_t, Q_1, \ldots, Q_t$ have a common zero and*

$$\sum_{i=1}^{n} x_i^d = R + \sum_{j=1}^{t} P_j(\mathbf{x}) Q_j(\mathbf{x}) \,.$$

Then, $t \geq n/2$.

We now show that without loss of generality, the constant part of every polynomial map M such that $\sum_{i=1}^{n} x_i^d = \mathsf{Det}_m(M(\mathbf{x}))$ has a very special form: is it an $m \times m$ diagonal matrix with 0 in the $(1,1)$ coordinate and 1 in all diagonal entries.

3.1 Reducing the matrix M to a normal form

This claim is not entirely new and very similar statements were proved, for example, in [MR04, ABV17]. For completeness, and since the exact statement we need is slightly more general, we provide a proof.

Lemma 3.2. *Let $d \geq 2$ be a natural number and let $M(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]^{m \times m}$ be a polynomial map such that*

$$\mathsf{Det}_m(M(\mathbf{x})) = \sum_{i=1}^{n} x_i^d \,.$$

Then, there exists a matrix $\tilde{M}(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]^{m \times m}$ with $\deg(\tilde{M}) \leq \deg(M)$,

$$\mathsf{Det}_m(\tilde{M}(\mathbf{x})) = \sum_{i=1}^{n} x_i^d \,,$$

and the constant part of $\tilde{M}$ is a diagonal $m \times m$ matrix $\tilde{M}_0$ such that $(\tilde{M}_0)_{1,1} = 0$ and $(\tilde{M}_0)_{i,i} = 1$, for $2 \leq i \leq m$.

To prove Lemma 3.2 we require a few preliminaries. We begin with the definition of a singular locus of a polynomial (or a hypersurface).

Definition 3.3. *Let $f \in \mathbb{F}[\mathbf{x}]$ be a polynomial. The* singular locus *of f, denoted $\mathrm{Sing}(f)$, is the variety defined by*

$$\mathrm{Sing}(f) = \left\{ \mathbf{a} : \frac{\partial f}{\partial x_i}(\mathbf{a}) = 0, 1 \leq i \leq n \right\}. \qquad \Diamond$$

The singular locus of the determinant was studied by von zur Gathen, who proved the following fact.

Fact 3.4 ([vzG87])**.** *Let $\mathbb{F}$ be an algebraically closed field and let Det_m denote the $m \times m$ determinant polynomial. Then $\mathrm{Sing}(\mathsf{Det}_m) \subseteq \mathbb{F}^{m \times m}$ is precisely the set of matrices of rank at most $m-2$, and $\dim \mathrm{Sing}(\mathsf{Det}_m) = m^2 - 4$.*

The following is a slight generalization of a lemma of von zur Gathen (cf. also [ABV17]).

Lemma 3.5. *Let $f \in \mathbb{F}[\mathbf{x}]$ be a polynomial, and let $M : \mathbb{F}^n \to \mathbb{F}^{m \times m}$ be a polynomial map such that $f(\mathbf{x}) = \mathsf{Det}_m(M(\mathbf{x}))$. Suppose further that $\dim(\mathrm{Sing}(f)) < n - 4$. Then $\mathrm{Im}(M) \cap \mathrm{Sing}(\mathsf{Det}_m) = \emptyset$. Furthermore, all matrices in $\mathrm{Im}(M)$ have rank at least $m-1$.*

Proof. Let $y_{i,j}$ denote the coordinates of $\mathbb{F}^{m\times m}$ and write $M = (M_{i,j})_{i,j\in[m]}$. Using the chain rule, we compute

$$\frac{\partial f}{\partial x_k} = \sum_{i,j\in[m]} \frac{\partial \mathsf{Det}_m}{\partial y_{i,j}}(M(\mathbf{x})) \cdot \frac{\partial M_{i,j}}{\partial x_k}(\mathbf{x}), \quad k \in [n]. \tag{3.6}$$

Suppose $A \in \mathrm{Im}(M) \cap \mathrm{Sing}(\mathsf{Det}_m)$, and let B be such that $A = M(B)$. By definition of $\mathrm{Sing}(\mathsf{Det}_m)$, $\frac{\partial \mathsf{Det}_m}{\partial y_{i,j}}(M(B)) = 0$ for all $i, j \in [m]$, and by (3.6) we get that $B \in \mathrm{Sing}(f)$. Thus $M^{-1}(\mathrm{Sing}(\mathsf{Det}_m)) \subseteq \mathrm{Sing}(f)$, and $\dim(M^{-1}(\mathrm{Sing}(\mathsf{Det}_m))) \leq \dim \mathrm{Sing}(f) < n-4$. On the other hand, using a standard lower bound on the dimension of pre-images of polynomial maps (see Theorem 17.24 of [Har95]), if $\mathrm{Im}(M)$ and $\mathrm{Sing}(\mathsf{Det}_m)$ aren't disjoint,

$$\dim(M^{-1}(\mathrm{Sing}(\mathsf{Det}_m))) \geq n + (m^2 - 4) - m^2 = n - 4.$$

This contradiction implies that $\mathrm{Im}(M) \cap \mathrm{Sing}(\mathsf{Det}_m) = \emptyset$. The "furthermore" part of the theorem follows from Fact 3.4. □

We will also need the following easy fact which shows that $\sum_{i=1}^n x_i^d$ satisfies that assumption of Lemma 3.5.

Fact 3.7 ([Kum19, CKSV19])**.** *For every $d \geq 2$,* $\dim(\mathrm{Sing}(\sum_{i=1}^n x_i^d)) = 0$.

We are now ready to prove Lemma 3.2.

Proof of Lemma 3.2. Let $f = \sum_{i=1}^n x_i^d$ and let $M : \mathbb{F}^n \to \mathbb{F}^{m\times m}$ be a polynomial map such that $f(\mathbf{x}) = \mathsf{Det}_m(M(\mathbf{x}))$, and write $M = M' + M_0$ where M_0 is the constant part of M.

First, observe that

$$0 = f(\mathbf{0}) = \mathsf{Det}_m(M(\mathbf{0})) = \mathsf{Det}_m(M_0),$$

which implies that $\mathsf{rank}(M_0) < m$. By Lemma 3.5 and Fact 3.7, we also know that $\mathsf{rank}(M_0) = \mathsf{rank}(M(\mathbf{0})) \geq m - 1$, so $\mathsf{rank}(M_0) = m - 1$.

By performing Gaussian elimination on the rows and on the columns, we can find two $m \times m$ matrices G_1, G_2 such that $\det(G_i) = \pm 1$ for $i = 1, 2$ and $N_0 := G_1 M_0 G_2$ is a diagonal matrix such that $(N_0)_{1,1} = 0$ and $(N_0)_{i,i} \neq 0$ for $2 \leq i \leq m$.

Now define a diagonal $m \times m$ matrix Δ such that $\Delta_{i,i} = 1/(N_0)_{i,i}$ for $2 \leq i \leq m$, and

$$\Delta_{1,1} = \mathsf{Det}(G_1) \cdot \mathsf{Det}(G_2) \cdot \prod_{i=2}^m (N_0)_{i,i}.$$

It readily follows that $\mathsf{Det}(\Delta) = \mathsf{Det}(G_1) \cdot \mathsf{Det}(G_2)$, and that $\tilde{M}_0 := (G_1 M_0 G_2)\Delta$ is a diagonal matrix such that $(\tilde{M}_0)_{1,1} = 0$ and $(\tilde{M}_0)_{i,i} = 1$ for all $2 \leq i \leq m$.

Finally, define $\tilde{M} = G_1 M G_2 \Delta$. We verify that indeed

$$\begin{aligned}\mathsf{Det}(\tilde{M}(\mathbf{x})) &= \mathsf{Det}(G_1) \cdot \mathsf{Det}(M(\mathbf{x})) \cdot \mathsf{Det}(G_2) \cdot \mathsf{Det}(\Delta) \\ &= \mathsf{Det}(M(\mathbf{x})) \cdot (\mathsf{Det}(G_1) \cdot \mathsf{Det}(G_2))^2 = \mathsf{Det}(M(\mathbf{x})) = f(\mathbf{x}).\end{aligned}$$

We also have that

$$\tilde{M} = G_1(M' + M_0)G_2\Delta = G_1 M' G_2 D + G_1 M_0 G_2 \Delta = G_1 M' G_2 \Delta + \tilde{M}_0.$$

Since $G_1, G_2, \Delta \in \mathbb{F}^{m\times m}$, it also holds that $\tilde{M}' := G_1 M' G_2 \Delta$ is a matrix of constant-free polynomials, and that $\deg \tilde{M} \leq \deg M$. □

We will also use the following simple and well known property of the determinant of a block matrix.

Lemma 3.8. *Let $M \in \mathbb{F}^{m\times m}$ be a matrix, and let $A \in \mathbb{F}^{t\times t}, B \in \mathbb{F}^{t\times m-t}, C \in \mathbb{F}^{m-t\times t}, D \in \mathbb{F}^{m-t\times m-t}$ be its submatrices as follows:*

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

If D is invertible, then

$$\mathsf{Det}(M) = \mathsf{Det}(A - BD^{-1}C) \cdot \mathsf{Det}(D)\,.$$

Proof. Follows directly from the decomposition

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A - BD^{-1}C & BD^{-1} \\ 0 & I_{m-t} \end{pmatrix} \cdot \begin{pmatrix} I_t & 0 \\ C & D \end{pmatrix}$$

and the multiplicativity of the determinant. □

3.2 Determinantal complexity of higher degree polynomial maps

In the following lemma we prove a lower bound of $n/2$ on the determinantal complexity in a more general model than the standard model. This is a generalization with respect to two properties. First, the entries of the matrix are no longer constrained to be polynomials of degree at most 1, and can have degree as high as $d-1$, while computing the degree d polynomial $\left(\sum_{i=1}^n x_i^d\right)$. Moreover, the determinant of the matrix M does not even have to compute the candidate hard polynomial $\left(\sum_{i=1}^n x_i^d\right)$ exactly. It suffices if the determinant is equal to a polynomial of the form $\left(\sum_{i=1}^n x_i^d\right) \cdot (\beta + Q)$ where β is a non-zero field constant and Q is an arbitrary polynomial (of potentially very high degree!) which is constant free, i.e. $Q(\mathbf{0}) = 0$.

Lemma 3.9. *Let $d \geq 2$ be a natural number and let $M(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]^{m\times m}$ such that $\deg(M) \leq d-1$, and the constant part of M is a diagonal matrix M_0 such that $(M_0)_{1,1} = 0$ and $(M_0)_{i,i} = 1$ for $2 \leq i \leq m$. Suppose that*

$$\mathsf{Det}(M) = \left(\sum_{i=1}^n x_i^d\right) \cdot (\beta + Q)\,,$$

where $\beta \in \mathbb{F}$ is non-zero and Q is a constant free polynomial. Then $m \geq n/2 - 1$.

Proof. Using the Laplace expansion of $\mathsf{Det}(M)$ along the first row, we get

$$\mathsf{Det}(M) = \sum_{j=1}^{m} (-1)^{(j+1)} M_{1,j} \cdot \mathsf{Det}(N_{1,j})\,,$$

where $N_{i,j}$ is the submatrix of M obtained by deleting the i-th row and the j-th column. For every $j \in [m]$, $j > 1$, we claim that $\mathsf{Det}(N_{1,j})$ is a constant free polynomial, i.e.

$$\mathsf{Det}(N_{1,j})(\mathbf{0}) = \mathsf{Det}\left(N_{1,j}(\mathbf{0})\right) = 0\,.$$

To see this, we observe that for every $j \in [m] \setminus \{1\}$, $N_{1,j}(\mathbf{0})$ is a $(m-1)\times(m-1)$ matrix, which has at most $m-2$ non-zero entries. This follows since M_0 has at most $m-1$ non-zero entries and in obtaining $N_{1,j}$ from M, we drop the entry $M_{j,j}$, which is one of the $(m-1)$ entries of M with a non-zero constant term, and hence one of the $(m-1)$ non-zero entries of M_0. However, we note that $N_{1,1}(\mathbf{0})$ is the $(m-1)\times(m-1)$ identity matrix, so the constant term of $\mathsf{Det}(N_{1,1})$ is 1, and we write $\mathsf{Det}(N_{1,1}) = 1 + P(\mathbf{x})$ where P is constant free. Therefore, we have

$$\left(\sum_{i=1}^n x_i^d\right) \cdot (\beta + Q) = \mathsf{Det}(M) = M_{1,1}(1+P) + \sum_{j=2}^{m} (-1)^{(j+1)} M_{1,j} \cdot \mathsf{Det}(N_{1,j})$$

In other words,

$$\left(\sum_{i=1}^{n} x_i^d\right) \cdot (\beta + Q) = \mathsf{Det}(M) = M_{1,1} + M_{1,1} \cdot P + \sum_{j=2}^{m} (-1)^{(j+1)} M_{1,j} \cdot \mathsf{Det}(N_{1,j})$$

Slightly rearranging (and using $\beta \neq 0$), we get

$$\sum_{i=1}^{n} x_i^d = \frac{1}{\beta}\left(-\left(\sum_{i=1}^{n} x_i^d\right) \cdot Q + M_{1,1} + M_{1,1} \cdot P + \sum_{j=2}^{m} (-1)^{(j+1)} M_{1,j} \cdot \mathsf{Det}(N_{1,j})\right)$$

Since, $\deg(M_{1,1}) < d$ and $M_{1,1}, P, M_{1,2}, \mathsf{Det}(N_{1,2}), \ldots, M_{1,k}, \mathsf{Det}(N_{1,k}), Q$ are all constant free (and hence share a common zero, namely $\mathbf{0}$), we have from Lemma 3.1 that $m \geq n/2 - 1$. □

3.3 Completing the proof of Theorem 1.1

We are now ready to complete the proof of Theorem 1.1.

Proof of Theorem 1.1. Let M be a $m \times m$ matrix with $\deg(M) \leq 1$ such that

$$\sum_{i=1}^{n} x_i^n = \mathsf{Det}(M)\,.$$

From Lemma 3.2, we can assume without loss of generality that the constant part M_0 of M is a diagonal matrix such that $(M_0)_{1,1} = 0$ and $(M_0)_{i,i} = 1$ for $2 \leq i \leq m$. In particular, all the off diagonal entries of M and $M_{1,1}$ are homogeneous linear forms or zero, and $M_{j,j} \neq 0$ for $j > 1$.

Observe that for every $t \leq m-1$, the principle minor D_t of M which is obtained by deleting the first $m-t$ rows and columns of M are all invertible over the field of rational functions $\mathbb{F}(\mathbf{x})$. To see this, observe that the matrix $D_t(\mathbf{0})$ is the identity matrix, which implies that $\mathsf{Det}(D_t)$ is a non-zero polynomial. Moreover, since every entry of M has degree at most 1, and $\mathsf{Det}(M)$ has degree n, we know that $m \geq n$. So, we conclude that the principle minor $D := D_{(n-2)}$ of M is invertible over $\mathbb{F}(\mathbf{x})$. Thus, if B and C are respectively the submatrices of M defined as

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

then by Lemma 3.8 we have

$$\mathsf{Det}(M) = \mathsf{Det}(A - BD^{-1}C) \cdot \mathsf{Det}(D)\,. \tag{3.10}$$

Since $D^{-1} = \mathrm{adj}(D)/\det(D)$, where $\mathrm{adj}(D)$ is the adjugate matrix of D, the entries of D^{-1} can be written as as a ratio of two polynomials, where the numerator has degree at most $n-3$ and the denominator, which is equal to $\mathsf{Det}(D)$, has degree at most $n-2$. Moreover, as discussed earlier in the proof, the constant part of D is the identity matrix, so there is a constant free polynomial $Q \in \mathbb{F}[\mathbf{x}]$ such that

$$\mathsf{Det}(D) = 1 + Q\,.$$

Thus, every entry of the $(m-n+2) \times (m-n+2)$ matrix $A - BD^{-1}C$ can be written as a ratio of two polynomials with the numerator being a polynomial of degree at most $n-1$ and the denominator being equal to $\mathsf{Det}(D) = 1 + Q$. Therefore, by clearing the denominators and using (3.10), we get that

$$\mathsf{Det}(M) \cdot (1+Q)^{m-n+2} = \mathsf{Det}(N) \cdot (1+Q)\,,$$

where N is the matrix with polynomial entries of degree at most $n-1$ obtained by multiplying every entry of $A - BD^{-1}C$ by $1+Q$. Simplifying further, we get

$$\left(\sum_{i=1}^{n} x_i^n\right) \cdot (1+Q)^{m-n+1} = \mathsf{Det}(M) \cdot (1+Q)^{m-n+1} = \mathsf{Det}(N)\,.$$

We are almost ready to invoke Lemma 3.9 to obtain a lower bound on the size of N (and hence M), but to do that we need to ensure that the constant part of N, N_0, is a diagonal matrix with $(N_0)_{1,1} = 0$ and $(N_0)_{i,i} = 1$ for $2 \le i \le m-n+2$. We now verify that this is indeed the case.

Recall that by the structure of the constant part M_0 of M, all the entries of B and C and the $(1,1)$ entry of A are constant free, and the constant term of $A_{i,i}$ is 1 for $2 \le i \le m-n+2$. Thus, every entry of the matrix $BD^{-1}C$ is a rational function with a constant free numerator, and hence all the off-diagonal entries in $A - BD^{-1}C$ as well as its $(1,1)$ entry are rational functions with a constant free numerator. Moreover, the denominator of all the entries $\left(A - BD^{-1}C\right)$ equals $\mathsf{Det}(D) = 1+Q$, for a constant free polynomial Q. So, expressing each element of $A - BD^{-1}C$ as a quotient of polynomials, the constant term of each numerator on the diagonal is 1 except for the $(1,1)$ entry, which has a constant free numerator. Finally, observe that eliminating the denominator of the entries of $\left(A - BD^{-1}C\right)$ by multiplying every entry by $(1+Q)$ gives us the matrix N.

Thus the matrix N satisfies the hypothesis of Lemma 3.9, and hence $(m-n+2) \ge n/2 - 1$. This gives us $m \ge 1.5n - 3$ and completes the proof of Theorem 1.1. □

Acknowledgment

Mrinal thanks Ramprasad Saptharishi for various discussions on determinantal complexity over the years, and in particular for explaining the proof of the result of Mignon and Ressayre to him.

References

[ABV17] Jarod Alper, Tristram Bogart, and Mauricio Velasco. A Lower Bound for the Determinantal Complexity of a Hypersurface. *Found. Comput. Math.*, 17(3):829–836, 2017.

[AFT11] Boris Alexeev, Michael A. Forbes, and Jacob Tsimerman. Tensor Rank: Some Lower and Upper Bounds. In *Proceedings of the 26th Annual IEEE Conference on Computational Complexity (CCC 2011)*, pages 283–291. IEEE Computer Society, 2011.

[BD80] Mark R. Brown and David P. Dobkin. An Improved Lower Bound on Polynomial Multiplication. *IEEE Trans. Computers*, 29(5):337–340, 1980.

[Blä99] Markus Bläser. A $\frac{5}{2}n^2$-Lower Bound for the Rank of $n \times n$ Matrix Multiplication over Arbitrary Fields. In *Proceedings of the 40th Annual IEEE Symposium on Foundations of Computer Science (FOCS 1999)*, pages 45–50, 1999.

[Cai90] Jin-Yi Cai. A Note on the Determinant and Permanent Problem. *Inf. Comput.*, 84(1):119–127, 1990.

[CCL10] Jin-Yi Cai, Xi Chen, and Dong Li. Quadratic Lower Bound for Permanent Vs. Determinant in any Characteristic. *Comput. Complex.*, 19(1):37–56, 2010.

[CKSV19] Prerona Chatterjee, Mrinal Kumar, Adrian She, and Ben Lee Volk. A Quadratic Lower Bound for Algebraic Branching Programs. *CoRR*, abs/1911.11793, 2019. Preprint available at `arXiv:1911.11793`.

[CKW11] Xi Chen, Neeraj Kayal, and Avi Wigderson. Partial Derivatives in Arithmetic Complexity. *Foundations and Trends in Theoretical Computer Science*, 2011.

[Har95] Joe Harris. *Algebraic geometry*, volume 133 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. A first course, Corrected reprint of the 1992 original.

[Kal85] Kyriakos Kalorkoti. A Lower Bound for the Formula Size of Rational Functions. *SIAM Journal of Computing*, 14(3):678–687, 1985.

[Kum19] Mrinal Kumar. A quadratic lower bound for homogeneous algebraic branching programs. *Computational Complexity*, 28(3):409–435, 2019.

[LMR13] Joseph M. Landsberg, Laurent Manivel, and Nicolas Ressayre. Hypersurfaces with degenerate duals and the geometric complexity theory program. *Comment. Math. Helv.*, 88(2):469–484, 2013.

[LR17] J.M. Landsberg and Nicolas Ressayre. Permanent v. determinant: An exponential lower bound assuming symmetry and a potential path towards Valiant's conjecture. *Differential Geometry and its Applications*, 55:146–166, 2017.

[Mes89] Roy Meshulam. On two extremal matrix problems. *Linear Algebra and its Applications*, 114–115:261–271, 1989.

[MM61] Marvin Marcus and Henryk Minc. On the relation between the determinant and the permanent. *Illinois J. Math.*, 5(3):376–381, 09 1961.

[MR04] Thierry Mignon and Nicolas Ressayre. A quadratic bound for the determinant and permanent problem. *International Mathematics Research Notes*, 2004(79):4241–4253, 2004. Available on `citeseer:10.1.1.106.4910`.

[Pól13] George Pólya. Aufgabe 424. *Archiv der Mathematik und Physik*, 20:271, 1913.

[Sap15] Ramprasad Saptharishi. A survey of lower bounds in arithmetic circuit complexity. Github survey, 2015.

[Shp01] Amir Shpilka. Lower Bounds for Matrix Product. In *Proceedings of the 42nd Annual IEEE Symposium on Foundations of Computer Science (FOCS 2001)*, pages 358–367, 2001.

[SY10] 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.

[Sze13] Gábor Szegő. Lösung zu Aufgabe 424. *Archiv der Mathematik und Physik*, 21:291–292, 1913.

[Val79] Leslie G. Valiant. Completeness Classes in Algebra. In *Proceedings of the 11th Annual ACM Symposium on Theory of Computing (STOC 1979)*, pages 249–261, 1979.

[vzG87] Joachim von zur Gathen. Permanent and determinant. *Linear Algebra and its Applications*, 96:87–100, 1987.

[Yab15] Akihiro Yabe. Bi-polynomial rank and determinantal complexity. *CoRR*, abs/1504.00151, 2015. Pre-print available at `arXiv:1504.00151`.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il