Electronic Colloquium on Computational Complexity, Report No. 218 (2026)

A Quadratic Lower Bound on Determinantal Complexity

Mrinal Kumar* Ben Lee Volk†

Abstract

We prove an $\Omega(n^2)$ lower bound on the determinantal complexity of the power sum polynomial $\sum_{i=1}^{n} x_i^n$ over the field of complex numbers.

A similar result was claimed in a recent paper of Sheshadri [She26], via an AI-assisted and AI-written proof. Assuming its correctness, this was the first super-linear lower bound for this fundamental algebraic problem for any explicit polynomial. However, the authors of this note were unable to follow the details and verify the argument in [She26] in spite of considerable effort on their part.

The proof we provide here is short, (almost) self-contained and seemingly simpler.

AI Use: ChatGPT Astra was used by the authors on multiple occasions to parse through some of the parts of Sheshadri's proof in [She26] and the outline of the proof in this note came out of this exercise. The final exposition as well as some of the final details in this note are due to its human authors.

1 Introduction

Determinantal Complexity. The *determinantal complexity* of a polynomial $F(\mathbf{x}) \in \mathbb{C}[\mathbf{x}]$ is the smallest $m \in \mathbb{N}$ such that there is an $m \times m$ matrix $M(\mathbf{x})$, whose entries are polynomials of degree at most one in $\mathbb{C}[\mathbf{x}]$ such that $\det(M(\mathbf{x}))$ equals F.

Early interest in obtaining small determinantal representations can be traced back to Pólya [Pól13] and Szegő [Sze13]. The importance of this notion, however, was first highlighted by Valiant [Val79] who laid the foundations for algebraic complexity theory.

Valiant [Val79] established the fact that every polynomial has a finite determinantal representation, and observed that such representations can be seen as a natural computational model. This fact, together with appropriate notions of reductions and completeness, played a crucial role in Valiant's project of developing a complexity theory for algebraic computation. The question of proving that the determinantal complexity of the permanent polynomial of a symbolic $n \times n$ matrix (over fields of characteristic not equal to two) is superpolynomially growing in n has served as a guiding light in much of the research in algebraic complexity over the last five decades, as it can be seen as a natural algebraic analog of the P vs. NP problem.

While it isn't entirely surprising that this question, or more generally the question of proving a super-polynomial lower bound on the determinantal complexity of *any* explicit polynomial is still open, it is surprising that till very recently, no super-linear lower bound was known for this

*Tata Institute of Fundamental Research, Mumbai, India. Email: mrinal@tifr.res.in. Research supported by the Department of Atomic Energy, Government of India, under project number RTI400112, and in part by research grants from Google and Premji Invest.

†Efi Arazi School of Computer Science, Reichman University, Israel. Email: benleevolk@gmail.com. The research leading to these results has received funding from the Israel Science Foundation (grant number 843/23).

ISSN 1433-8092

complexity measure. Mignon and Ressayre [MR04] famously showed a quadratic lower bound on the determinantal complexity of the $n \times n$ permanent polynomial (see also Cai, Chen and Li [CCL10]). These lower bounds, however, while being quadratic in the degree of the polynomial (which serves as the trivial lower bound on determinantal complexity for any polynomial), are proved for a polynomial with n^2 variables, so they are in fact not larger than the number of variables of the polynomial. Therefore, in the setting of discussing super-linear or similar such weak lower bounds for this complexity measure we prefer to concentrate on n-variate polynomials of degree at most n.

The best lower bound on the determinantal complexity of an explicit n-variate polynomial known till recently (as a function of the number of variables n) was a bound of (roughly) $1.5n$ shown by the authors of this paper for the polynomial $\sum_{i=1}^{n} x_i^n$ in a prior work ([KV22]).

This state of the art is especially surprising in the light of the fact that we have known super-linear lower bounds on fairly strong algebraic circuit models for some time, including algebraic circuits [Str73b, BS83], algebraic formulas [Kal85] and algebraic branching programs (ABPs) [Kum19, CKSV22]. While determinantal complexity and ABP complexity are polynomially equivalent, the polynomial blow-up implies that the lower bound for ABP complexity does not immediately carry over for determinantal complexity (see also [CKV24]).

Sheshadri's recent proof [She26]. In one of the relatively early instances of the use of AI in computational complexity, Karthik Sheshadri claimed in an AI-assisted proof [She26] that the determinantal complexity of the polynomial $\sum_{i=1}^{n} x_i^n$ is $\Omega(n^2)$. However, at least the authors of this paper were unable to follow the argument, or check the correctness of the claims in spite of substantial effort on their part. The writing of the paper appeared to be heavily AI-based, with substantial use of either advanced algebraic-geometric notions, or non-standard technical jargon in many places, making the result inaccessible to an algebraic complexity theory audience.

Assuming the correctness of the argument, this proof provided the first super-linear lower bound on the determinantal complexity of any explicit n-variate polynomial. Given the significance of such a result, and the substantial interest in understanding the ideas in the proof within the algebraic complexity research community, there appeared to be merit in obtaining a simpler proof (or a simpler exposition) of this result.

The purpose of this note is to provide such a proof. The proof presented here indeed happens to be short, simple, to a large extent intuitive, and self-contained apart from the use of a slightly uncommon (and yet, classical) form of Bézout's theorem. While we do not really follow the ideas in Sheshadri's proof enough to say this with any degree of confidence, our impression is that the proof in this note is quite close to (or even exactly the same as) the intended proof in [She26]. It is quite conceivable that the simplicity of the description of the proof in this note is an artifact of us looking only for asymptotic bounds, as opposed to the proof in [She26] where attention is also paid to the constants obtained in the bound. We urge the curious reader to look at the proof in [She26] to form their opinion on this.

We start by stating the theorem below, discuss some intuition behind the main ideas in the proof in Section 2, followed by the formal details in Section 3. In the interest of keeping this note short, we also refer the reader to [KV22] for a more detailed discussion on the prior work on determinantal complexity.

Theorem 1.1. *For all sufficiently large $n \in \mathbb{N}$, the following is true.*

Let $M_0, M_1, \ldots, M_n \in \mathbb{C}^{m \times m}$ be matrices and let $M(\mathbf{x})$ be defined as $M(\mathbf{x}) := M_0 + \sum_{i=1}^{n} x_i M_i$. If $\det(M(\mathbf{x})) = \sum_{i=1}^{n} x_i^n$, then $m = \Omega(n^2)$.

Acknowledgements. We are thankful to Abhranil Chatterjee, Ramprasad Saptharishi and Shubhangi Saraf for many insightful discussions on determinantal complexity over the years. Many thanks to Amir Shpilka for his sanguine advice on why it was important to write and

share this proof in this rapidly evolving and utterly confusing world of theory research in the age of AI.

2 Intuition and overview

The proof proceeds by constructing a system of polynomial equations with finitely many solutions, and bounding the size of this set from above and below. We first prove a lower bound on the size of this set using the properties of the polynomial $F(\mathbf{x}) := \sum_{i=1}^{n} x_i^n$, and then prove an upper bound on the size of this set using the properties of the determinantal representation and Bézout's theorem. Comparing these bounds immediately gives us an $\Omega(n \log n)$ lower bound on the size of the representation. To extend this bound to $\Omega(n^2)$, we replace the use of the vanilla Bézout's theorem by a stronger version that uses some structural properties of the polynomials in the polynomial system.

Strassen's lower bound: At a high level, the proof of Theorem 1.1 is motivated by and is similar to Strassen [Str73a] and Baur-Strassen's [BS83] proof of super-linear lower bounds for general algebraic circuits. The idea there is to consider the system of polynomial equations given by

$$\frac{\partial F}{\partial x_i}(\mathbf{x}) = 1, \quad i \in [n]$$

and count the number of solutions to this system. From the structure of the polynomial, the set of solutions to this system is finite and is in fact of size at least $\exp(\Omega(n \log n))$. The key conceptual idea is to show that if F is computable by an algebraic circuit of size s, then this system can have at most $\exp(O(s))$ solutions. Comparing these bounds gives us an $\Omega(n \log n)$ bound on s.

The upper bound on the set of solutions is obtained by showing that the size of this set is equal to the size of the set of solutions of another system of polynomial equations (that we refer to as the *proxy system*, in contrast to the *original system*), this time on $(n + s)$ variables and $O(s)$ equations, where every equation has degree at most 2. The classical Bézout theorem implies an $\exp(O(s))$ upper bound on the size of the solution set. The crucial facts used here were

- the new system had polynomials of degree at most a constant independent of n,
- the number of equations was at most $O(s)$,
- and the number of solutions was finite and equal to the number of solutions in the original system.

Working with determinantal representation: The high level strategy in the proof of Theorem 1.1 is to understand whether the above approach can be adapted when we have a small determinantal representation for F, instead of a small circuit.

A natural first attempt is to start with the same polynomial system as in Strassen's proof, where we set all the first-order partial derivatives of $\mathbb{F}(\mathbf{x})$ to 1. The key technical issue in analyzing this system is that we do not know of a way of upper bounding the size of the solution set using a proxy system based on the determinantal representation. However, it turns out that a related system of equations, again based on the first-order partial derivatives of F, is easier to work with. The intuition that directs us towards this system is incidentally an elementary linear algebraic fact that follows from Jacobi's formula. Let M be an $m \times m$ matrix whose entries are linear forms in $\mathbf{x}$ such that $F(\mathbf{x}) = \det(M(\mathbf{x}))$. Furthermore, let $M_0, M_1, \ldots, M_n \in \mathbb{C}^{m \times m}$ be constant matrices such that $M = M_0 + \sum_i x_i M_i$. Then, the following lemma is true.

Lemma 2.1. *Let $\mathbf{a} \in \mathbb{C}^n$ be such that rank of $M(\mathbf{a})$ equals $(m-1)$. Let $\mathbf{u}, \mathbf{v}$ be arbitrary non-zero vectors in $\mathbb{C}^m$ such that $\mathbf{u}^T$ is in the left kernel of $M(\mathbf{a})$ and $\mathbf{v}$ is in the right kernel of $M(\mathbf{a})$.*

Then, there exists a non-zero constant $\lambda \in \mathbb{C}$ such that for every $i \in [n]$,

$$\frac{\partial F}{\partial x_i}(\mathbf{a}) = \lambda \mathbf{u}^T M_i \mathbf{v}.$$

The key takeaway from Lemma 2.1 is that at points $\mathbf{a} \in \mathbb{C}^n$ where the rank of $M(\mathbf{a})$ equals $(m-1)$, the first order partial derivatives of F do indeed behave like a degree 2 polynomial in a new set of auxiliary variables $\mathbf{u}, \mathbf{v}$ coming from the left and right kernel spaces of $M(\mathbf{a})$. Note that we have $2m$ such variables, corresponding to the coordinates of $\mathbf{u}, \mathbf{v}$, and thus the size of the determinantal representation makes an appearance. So, we modify the original polynomial system involving setting all first order derivatives to 1, in order to ensure that we are dealing with $\mathbf{a}$ such that $M(\mathbf{a})$ has rank exactly $(m-1)$, and then consider the $2m$ auxiliary variables $\mathbf{u}, \mathbf{v}$ and get a proxy system involving them.

The original polynomial system that we work with is given by the following definition.

Definition 2.2. *Let F be the n-variate polynomial $\sum_{i=1}^{n} x_i^n$. Let $\mathcal{S} \subseteq \mathbb{C}^n$ be the set of solutions to the system of equations given by*

1. $F(\mathbf{x}) = 0$
2. $x_{n-1} = 1$
3. *For every $i \leq (n-2)$, $\frac{\partial F}{\partial x_i} = \frac{\partial F}{\partial x_{n-1}}$*

This system clearly has a finite number of solutions, and this number is $\exp(\Theta(n \log n))$. We observe that the first two conditions ensure that any solution $\mathbf{a}$ to this system satisfies $M(\mathbf{a})$ has rank *equal* to $(m-1)$. This is shown in Claim 3.5. This implies the existence of non-zero vectors in the left and the right kernels (which are one-dimensional spaces) of $M(\mathbf{a})$. Using these vectors, Lemma 2.1 tells us that constraints on the first order derivatives of F in the system can be written as degree-2 constraints in the coordinates of $\mathbf{u}, \mathbf{v}$. The proxy system that we construct in variables $\mathbf{x}, \mathbf{u}, \mathbf{v}$ captures this in a natural way. We need to impose a few more constraints in this system to ensure that the number of solutions of the proxy system is finite. The final description of this system is in Definition 3.7.

This system has $O(n+m)$ polynomial constraints in it, each of which has constant degree. Thus, by Bézout's theorem, this system has at most $\exp(O(n+m))$ solutions. Comparing this to the lower bound of $\exp(\Theta(n \log n))$ on the number of solutions of the original system in Definition 2.2 immediately gives us a lower bound of $\Omega(n \log n)$ on m. We then observe that this bound can be improved further for the proxy-system we have since the equations in the system happen to be (essentially) set multilinear with respect to the variables $\mathbf{x}, \mathbf{u}, \mathbf{v}$. This allows us to use a version of Bézout's theorem for such systems (Theorem 3.11) that gives a better bound on the number of solutions, leading to the proof of Theorem 1.1.

We provide the details in the next section.

3 The formal proof

3.1 A lower bound from the polynomial

Recall that we denote by $\mathcal{S}$ the set of solutions to the system of polynomial equations in Definition 2.2. We first observe that for all $n \geq 2$, the set $\mathcal{S}$ is finite, and compute a lower bound on its size.

Claim 3.1. *The set of solutions $\mathcal{S}$ to the polynomial system in Definition 2.2 is finite, and $|\mathcal{S}| \geq (n-1)^{n-2}$.*

Proof. From the definition of F, we get that $\frac{\partial F}{\partial x_i} = n \cdot x_i^{n-1}$. So, the system of equations stated in Definition 2.2 is just

$$F(\mathbf{x}) = 0, \quad x_{n-1} = 1$$

and

$$x_i^{n-1} = 1, \quad i \in [n-2]$$

The $(n-2)$ equations based on the derivatives clearly give us $(n-1)^{n-2}$ distinct settings of values of $x_1, x_2, \ldots, x_{n-2}$. The variable x_{n-1} is forced to be one, and for each of these settings of the first $(n-1)$ variables, the variable x_n has at least one and at most n possible assignments that satisfy the first equation $F(\mathbf{x}) = 0$. Thus, we get that the set $\mathcal{S}$ is finite and

$$|\mathcal{S}| \geq (n-1)^{n-2}. \qquad \square$$

3.2 An upper bound from the determinantal representation

We now use the $m \times m$ determinantal representation $M(\mathbf{x})$ of F to prove an upper bound on the size of $\mathcal{S}$. To this end, we first construct an alternative system of polynomial equations based on $M(\mathbf{x})$ such that the number of solutions of the new system is an upper bound on the size of $\mathcal{S}$. We start by making some simple linear algebraic claims.

Claim 3.2. *Let* $\mathbf{a} \in \mathbb{C}^n$ *be such that* $\mathrm{rank}(M(\mathbf{a})) = m - 1$.

For any non-zero vectors $\mathbf{u} = \mathbf{u}(\mathbf{a}), \mathbf{v} = \mathbf{v}(\mathbf{a})$ *in* $\mathbb{C}^m$ *such that* $\mathbf{u}^T$ *is in the left kernel of* $M(\mathbf{a})$, $\mathbf{v}$ *is in the right kernel of* $M(\mathbf{a})$, *there is a non-zero constant* λ *such that*

$$\mathrm{Adj}(M(\mathbf{a})) = \lambda \mathbf{v}\mathbf{u}^T.$$

Proof. By the assumption, any non-zero $\mathbf{u}$ in the left kernel is a basis for the kernel, and any non-zero $\mathbf{v}$ in the right kernel is a basis for the right kernel.

By the definition of adjugate of a matrix, we get that

$$\mathrm{Adj}(M(\mathbf{a})) \cdot M(\mathbf{a}) = M(\mathbf{a}) \cdot \mathrm{Adj}(M(\mathbf{a})) = \det(M(\mathbf{a})) \cdot I_m,$$

where I_m is the $m \times m$ identity matrix. Since $\det(M(\mathbf{a})) = 0$, every column of $\mathrm{Adj}(M(\mathbf{a}))$ is in the right kernel of $M(\mathbf{a})$. Similarly, every row is in the left kernel. By the assumption, the left and right kernels of $M(\mathbf{a})$ are one-dimensional spaces. We therefore get that the rows of $\mathrm{Adj}(M(\mathbf{a}))$ are in the span of $\mathbf{u}$ and the columns are in the span of $\mathbf{v}$. Thus, there exists a non-zero constant λ such that $\mathrm{Adj}(M(\mathbf{a})) = \lambda \mathbf{v}\mathbf{u}^T$. Here, the non-zeroness of λ follows from the fact that the rank of $M(\mathbf{a})$ equals $(m-1)$, and hence, $\mathrm{Adj}(M(\mathbf{a}))$ is non-zero. $\square$

The following classical claim is known as Jacobi's formula. For completeness, we provide a direct proof.

Claim 3.3 (Jacobi's formula)**.** *For every* i,

$$\frac{\partial F(\mathbf{x})}{\partial x_i} = \mathrm{Trace}(\mathrm{Adj}(M(\mathbf{x})) \cdot M_i).$$

Proof. Since $F(\mathbf{x}) = \det(M(\mathbf{x}))$, expanding the determinant in terms of the monomials, and differentiating with respect to x_i, we get that

$$\frac{\partial F}{\partial x_i} = \sum_{\sigma \in S_m} (-1)^{\mathrm{sign}(\sigma)} \left(\sum_{j=1}^{m} \frac{\partial (M(\mathbf{x})_{j,\sigma(j)})}{\partial x_i} \prod_{\ell \neq j} M(\mathbf{x})_{\ell,\sigma(\ell)} \right).$$

Here S_m is the set of permutations on m elements. Rearranging the summation, we get

$$\frac{\partial F}{\partial x_i} = \sum_{j,j'} \frac{\partial (M(\mathbf{x})_{j,j'}}{\partial x_i} \left(\sum_{\sigma \in S_m : \sigma(j) = j'} (-1)^{\text{sign}(\sigma)} \prod_{\ell \neq j} M(\mathbf{x})_{\ell,\sigma(\ell)} \right).$$

Now, the internal summation within the brackets is really just equal to $\text{Adj}(M(\mathbf{x}))_{j',j}$, and the partial derivative $\frac{\partial (M(\mathbf{x})_{j,j'}}{\partial x_i}$ equals $(M_i)_{j,j'}$ since the entries of M have degree at most one in $\mathbf{x}$. Thus, we get

$$\frac{\partial F}{\partial x_i} = \sum_{j,j'} (M_i)_{j,j'} \cdot \text{Adj}(M(\mathbf{x}))_{j',j},$$

which equals the trace of the matrix $(\text{Adj}(M)M_i)$ as claimed. □

An immediate consequence of Claims 3.2 and 3.3 is the following useful corollary.

Corollary 3.4. *For every* $\mathbf{a}$ *such that* $\text{rank}(M(\mathbf{a})) = m-1$*, and non-zero vectors* $\mathbf{u}, \mathbf{v}$ *such that* $\mathbf{u}^T$ *is in the left kernel of* $M(\mathbf{a})$*,* $\mathbf{v}$ *is in the right kernel of* $M(\mathbf{a})$*, the following is true: there exists a non-zero constant* λ *such that for every* $i \in [n]$*,*

$$\frac{\partial F}{\partial x_i}(\mathbf{a}) = \lambda \mathbf{u}^T M_i \mathbf{v}.$$

Proof. We have that

$$\frac{\partial F}{\partial x_i}(\mathbf{a}) = \text{Trace}(\text{Adj}(M(\mathbf{a})) \cdot M_i) = \text{Trace}(\lambda \mathbf{v}\mathbf{u}^T \cdot M_i).$$

The first equality is by Claim 3.3, and the second by Claim 3.2. Further

$$(\mathbf{v}\mathbf{u}^T \cdot M_i)_{j,j} = \sum_{k=1}^{m} (\mathbf{v}\mathbf{u}^T)_{j,k} (M_i)_{k,j} = \sum_{k=1}^{m} \mathbf{v}_j \mathbf{u}_k (M_i)_{k,j}$$

implying that

$$\text{Trace}(\lambda \mathbf{v}\mathbf{u}^T \cdot M_i) = \lambda \sum_{j=1}^{m} (\mathbf{v}\mathbf{u}^T \cdot M_i)_{j,j} = \lambda \sum_{j=1}^{m} \sum_{k=1}^{m} \mathbf{v}_j \mathbf{u}_k (M_i)_{k,j} = \lambda \mathbf{u}^T M_i \mathbf{v}.$$ □

We now give a simple condition that ensures that the rank of $M(\mathbf{a})$ is $m-1$.

Claim 3.5. *Let* $\mathbf{a} \in \mathbb{C}^n$ *be such that* $F(\mathbf{a})$ *equals zero, but at least one of the first order partial derivatives of* F *is non-zero at* $\mathbf{a}$*. Then, the rank of the matrix* $M(\mathbf{a})$ equals $(m-1)$*.*

In particular, for every $\mathbf{a} \in \mathcal{S}$*,* $\text{rank}(M(\mathbf{a})) = m-1$*.*

Proof. Since $F(\mathbf{a}) = 0$, we get that $F(\mathbf{a}) = \det(M(\mathbf{a})) = 0$. So, the rank of $M(\mathbf{a})$ is at most $(m-1)$. We need to argue that it is exactly $(m-1)$.

Suppose the rank of $M(\mathbf{a})$ is at most $(m-2)$. In this case, by the chain rule, every first order partial derivative of F can be written as a linear combination of the $(m-1) \times (m-1)$ determinantal minors of $M(\mathbf{x})$, which would all be zero when evaluated at $\mathbf{a}$, which would be a contradiction. Thus, $\text{rank}(M(\mathbf{a})) = m-1$.

Finally, if $a \in \mathcal{S}$, $F(\mathbf{a}) = 0$ by definition (recall Definition 2.2), and $\mathbf{a}_{n-1} = 1$ implies $\frac{\partial F}{\partial x_{n-1}}(\mathbf{a}) \neq 0$. □

The following claim will enable us to ensure uniqueness of solutions to the proxy polynomial system.

Claim 3.6. *Let* $U = \cup_{\mathbf{a}\in\mathcal{S}}\{\mathbf{u} : \mathbf{u} \neq \mathbf{0}, \mathbf{u}^T M(\mathbf{a}) = \mathbf{0}\}$ *and* $V = \cup_{\mathbf{a}\in\mathcal{S}}\{\mathbf{v} : \mathbf{v} \neq \mathbf{0}, M(\mathbf{a})\mathbf{v} = \mathbf{0}\}$.

Then, there exist vectors $\mathbf{g}, \mathbf{h} \in \mathbb{C}^m$ *such that for every* $\mathbf{u} \in U$ *and* $\mathbf{v} \in V$, $\mathbf{g}^T\mathbf{u} \neq 0$ *and* $\mathbf{h}^T\mathbf{v} \neq 0$.

Proof. By Claim 3.5, for every $\mathbf{a} \in \mathcal{S}$, the set $U_{\mathbf{a}} := \{\mathbf{u} : \mathbf{u}^T M(\mathbf{a}) = \mathbf{0}\}$ is a one-dimensional subspace spanned by a non-zero vector $\mathbf{u}_a$. Therefore, if $\mathbf{g}$ is picked such that $\mathbf{g}^T\mathbf{u}_a \neq 0$ then $\mathbf{g}^T\mathbf{u} \neq 0$ for every non-zero $\mathbf{u} \in U_{\mathbf{a}}$.

Since $\mathcal{S}$ is a finite set, we can pick $\mathbf{g}$ to be a non-root of the non-zero polynomial $P(\mathbf{y}) = \prod_{\mathbf{a}\in\mathcal{S}} \mathbf{y}^T\mathbf{u}_a$ (in variables $\mathbf{y}$).

The argument for $\mathbf{h}$ and V is identical. □

Based on these claims, we are now ready to define the new system of equations.

Definition 3.7. *This new system of equations* $\mathcal{E}$ *has three tuples of variables,* $\mathbf{u} = (u_1, \ldots, u_m)$, $\mathbf{v} = (v_1, \ldots, v_m)$ *and* $\mathbf{x} = (x_1, \ldots, x_n)$, *and* $2m + (n + 1)$ *polynomial equations. The equations are as follows.*

1. *The vector* $\mathbf{u}$ *is in the left kernel of* $M(\mathbf{x})$, *i.e.* $\mathbf{u}^T M(\mathbf{x}) = 0$. *Note that this corresponds to* m *polynomial equations, each of which has degree at most one in* $\mathbf{x}$ *and at most one in* $\mathbf{u}$.
2. *The vector* $\mathbf{v}$ *is in the right kernel of* $M(\mathbf{x})$, *i.e.* $M(\mathbf{x})\mathbf{v} = 0$. *This corresponds to* m *polynomial equations, each of which has degree at most one in* $\mathbf{x}$ *and at most one in* $\mathbf{v}$.
3. *For every* $i \leq (n-2)$, $\mathbf{u}^T M_i \mathbf{v} = \mathbf{u}^T M_{n-1}\mathbf{v}$. *Thus, there are* $(n-2)$ *equations of this kind, each being bilinear in* $\mathbf{u}$ *and* $\mathbf{v}$.
4. $x_{n-1} = 1$
5. $\mathbf{g}^T\mathbf{u} = 1$
6. $\mathbf{h}^T\mathbf{v} = 1$

The vectors $\mathbf{g}, \mathbf{h}$ *are picked as in Claim 3.6.*

Let $\mathcal{T} \subseteq \mathbb{C}^{2m+n}$ *denote the set of solutions of the system of equations defined above.*

We represent points in $\mathcal{T}$ as a three-tuple $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ of vectors, where $\mathbf{a} \in \mathbb{C}^n$ is the assignment to $\mathbf{x}$-variables, $\mathbf{b}$ is the assignment to $\mathbf{u}$-variables and $\mathbf{c}$ is the assignment to $\mathbf{v}$ variables.

The next few claims help us understand the structure of $\mathcal{T}$ better and help us relate it to $\mathcal{S}$.

Claim 3.8. *If* $(\mathbf{a}, \mathbf{b}, \mathbf{c}) \in \mathcal{T}$, *then* $\mathbf{a}$ *is in* $\mathcal{S}$.

Proof. By definition, $\mathbf{b}^T, \mathbf{c}$ are in the left and right kernels of $M(\mathbf{a})$ respectively. Furthermore, they are both non-zero since they satisfy $\mathbf{g}^T\mathbf{b} = 1$, $\mathbf{h}^T\mathbf{c} = 1$. Thus, $M(\mathbf{a})$ is singular, and $\det(M(\mathbf{a})) = F(\mathbf{a}) = 0$.

We also know that $\mathbf{a}_{n-1} = 1$. The partial derivative of $F = \det(M(\mathbf{x}))$ with respect to the variable x_{n-1} at the input $\mathbf{a}$ is non-zero. This implies from Claim 3.5 that $\mathrm{rank}(M(\mathbf{a})) = m-1$. From Corollary 3.4, we get that there is a non-zero constant λ such that for every i,

$$\frac{\partial F}{\partial x_i}(\mathbf{a}) = \lambda \mathbf{b}^T M_i \mathbf{c}.$$

Thus, the set of equations $(\mathbf{u}^T M_i \mathbf{v} = \mathbf{u}^T M_{n-1}\mathbf{v})$ in Definition 3.7 implies that for every $i \leq (n-2)$, $\frac{\partial F}{\partial x_i}(\mathbf{a}) = \frac{\partial F}{\partial x_{n-1}}(\mathbf{a})$.

Thus, $\mathbf{a}$ satisfies all the equations in Definition 2.2, and hence $\mathbf{a} \in \mathcal{S}$. □

We claim that every solution $\mathbf{a} \in \mathcal{S}$ "lifts" to a unique solution $(\mathbf{a}, \mathbf{b}, \mathbf{c}) \in \mathcal{T}$.

Claim 3.9. *For every* $\mathbf{a} \in \mathcal{S}$, *there are unique* $\mathbf{b}, \mathbf{c}$ *in* $\mathbb{C}^m$ *such that* $(\mathbf{a}, \mathbf{b}, \mathbf{c}) \in \mathcal{T}$.

Proof. $\mathbf{a} \in \mathcal{S}$ implies that a_{n-1} must equal 1, and hence F has at least one non-zero first order partial derivative at $\mathbf{a}$. Thus, $\mathbf{a}$ immediately satisfies the $x_{n-1} = 1$ constraint in Definition 3.7, and furthermore, from Claim 3.5, we get that $M(\mathbf{a})$ has rank exactly $(m-1)$. Let $\mathbf{b}', \mathbf{c}' \in \mathbb{C}^m$ be non-zero vectors such that $\mathbf{b}'^T$ spans the left kernel of $M(\mathbf{a})$ and $\mathbf{c}'$ spans the right kernel of $M(\mathbf{a})$. Clearly, setting $\mathbf{u}, \mathbf{v}$ to $\mathbf{b}', \mathbf{c}'$ respectively will satisfy the kernel constraints (items 1, 2) in Definition 3.7. Furthermore, from Corollary 3.4, we get that $\mathbf{b}', \mathbf{c}'$ will also satisfy the derivative constraints (item 3) in Definition 3.7.

From the definition of $\mathbf{g}, \mathbf{h}$ in Claim 3.6, we get that $\mathbf{g}^T\mathbf{b}'$ and $\mathbf{h}^T\mathbf{c}'$ are both non-zero. Thus, by scaling $\mathbf{b}', \mathbf{c}'$ appropriately, we get non-zero vectors $\mathbf{b}, \mathbf{c}$ that satisfy

$$\mathbf{g}^T\mathbf{b} = \mathbf{h}^T\mathbf{c} = 1.$$

Moreover, the pair $(\mathbf{b}, \mathbf{c})$ is unique in the respective kernels of $M(\mathbf{a})$, and in particular, $\mathbf{b}, \mathbf{c}$ are independent of $\mathbf{b}', \mathbf{c}'$, and only depend on $\mathbf{a}$. Furthermore, the constraints involving $\mathbf{u}, \mathbf{v}$ in the first three items of Definition 3.7 are all homogeneous in $\mathbf{u}, \mathbf{v}$, and since $(\mathbf{a}, \mathbf{b}', \mathbf{c}')$ satisfied those as argued above, so does $(\mathbf{a}, \mathbf{b}, \mathbf{c})$.

Thus, we have obtained a unique "lift" of $\mathbf{a} \in \mathcal{S}$ to get a point in $\mathcal{T}$. □

From Claims 3.8 and 3.9 and the finiteness of $\mathcal{S}$, we get the following corollary.

Corollary 3.10. *The set $\mathcal{T}$ is finite and*

$$|\mathcal{T}| = |\mathcal{S}|.$$

3.3 A simple $\Omega(n \log n)$ lower bound

We are now ready to build upon the setup so far to conclude the proof of Theorem 1.1. As a first step, we notice that the classical Bézout theorem together with the setup above immediately implies a super-linear lower bound on m. We recall that such a bound wasn't known before Sheshadri's work, in spite of the considerable attention received by the question of proving a super-linear lower bound on determinantal complexity in the algebraic and geometric complexity research.

From Corollary 3.10, since $\mathcal{T}$ is finite, we get from Bézout's theorem that $|\mathcal{T}|$ is at most the product of the degrees of the polynomials in the system of equations, which is at most $2^{2m+(n-1)}$. Comparing this with the lower bound on the size of $\mathcal{S}$, we get that

$$2^{2m+(n-1)} \geq |\mathcal{T}| \geq |\mathcal{S}| \geq (n-1)^{(n-2)}.$$

This immediately implies $m = \Omega(n \log n)$.

3.4 A quadratic lower bound

We now observe that a slightly stronger bound can be obtained by noting that the system of polynomial equations in Definition 3.7 has additional structure: the variables can be partitioned into three sets, and each polynomial constraint depends on at most two of these sets and has degree at most one in each set. For such systems, a stronger form of Bézout's theorem is known in the literature.

To state it, we introduce some definitions. Let $\mathbf{x}_1, \ldots, \mathbf{x}_k$ be k disjoint sets of variables where $|\mathbf{x}_i| = n_i$. A polynomial P has multi-degree $d_1, \ldots, d_k$ if it has degree at most d_i in $\mathbf{x}_i$, for every $i \in [k]$.

The multi-homogeneous Bézout's theorem counts the number of solutions of a system of N such polynomials. It is usually attributed to Shafarevich [Sha13, Section 2.1]. We also refer to [Wik26] and to [JS07, Section 3.2], the latter of which also cites several other references with additional proofs.

These references all assume that the polynomials are multi-homogeneous and hence count the solutions in the multi-projective variety $\mathbb{P}_{n_1} \times \mathbb{P}_{n_2} \times \cdots \times \mathbb{P}_{n_k}$ (and therefore $|\mathbf{x}_i| = n_i + 1$). One can reduce the affine case to the homogeneous case by homogenization. These arguments are rather standard in algebraic geometry.

We directly cite the affine version which is the most convenient for us:

Theorem 3.11 (Multi-homogeneous Bézout's theorem)**.** *Let $\mathbf{x}_1, \ldots, \mathbf{x}_k$ be k disjoint sets of variables such that $|\mathbf{x}_i| = n_i$. Let $P_1, \ldots, P_N$ be a set of polynomials, where P_i is of multi-degree $d_{i,1}, \ldots, d_{i,k}$, where $d_{i,j}$ is the degree of P_i in the variables $\mathbf{x}_j$, and $N = n_1 + n_2 + \cdots + n_k$.*

For every $i \in [N]$, define the linear form (in variables $y_1, \ldots, y_k$)

$$\mathbf{d}_i = d_{i,1}y_1 + d_{i,2}y_2 + \cdots + d_{i,k}y_k.$$

Then, the number of solutions to the system $\{P_i(\mathbf{x}_1, \ldots, \mathbf{x}_k) = 0 : i \in [N]\}$ is either infinite, or has size at most B, where B is the coefficient of the monomial

$$y_1^{n_1} y_2^{n_2} \cdots y_k^{n_k}$$

in the polynomial

$$\mathbf{d}_1 \mathbf{d}_2 \cdots \mathbf{d}_N.$$

The version stated here is from [MS87] (see also [Abe18], Theorem 2.45). The bound B is called the *Bézout number* of the system, and the original statement concerns the number of *isolated* solutions, but clearly if the number of solutions is finite, every solution is isolated.

We would like to invoke Theorem 3.11 for the polynomial system in Definition 3.7. However, for this theorem to make sense, the number of equations needs to be equal to the number of variables $n_1 + n_2 + \cdots + n_k$ since $\mathbf{d}_1 \mathbf{d}_2 \cdots \mathbf{d}_N$ is a homogeneous polynomial of degree N.

Fortunately, we can amend the system in Definition 3.7 slightly to obtain this.

Definition 3.12. *Pick a vector $\mathbf{q} \in \mathbb{C}^m$ such that $\mathbf{b}^T\mathbf{q} \neq 0$ for every $\mathbf{b} \in \mathbb{C}^m$ for which there exists $\mathbf{a}, \mathbf{c}$ such that $(\mathbf{a}, \mathbf{b}, \mathbf{c}) \in \mathcal{T}$. This is possible since $\mathcal{T}$ is finite, by Corollary 3.10, using an argument identical to that in Claim 3.6.*

Let $\Gamma \in \mathbb{C}^{m-1 \times m}$ be a matrix such that $\ker \Gamma = \operatorname{span}\{\mathbf{q}\}$.

Replace the m equations in item 2 of Definition 3.7 by the $m - 1$ equations $\Gamma M(\mathbf{x})\mathbf{v} = 0$ in variables $\mathbf{x}$ and $\mathbf{v}$.

Finally, add another variable z, and add the equation $z\mathbf{u}^T\mathbf{q} = 1$.

Let $\mathcal{T}' \subseteq \mathbb{C}^{2m+n+1}$ denote the set of solutions to this system.

Claim 3.13. $|\mathcal{T}| = |\mathcal{T}'|$

Proof. Recall that we changed the equations in item 2, and added the equation $z\mathbf{u}^T q = 1$.

We show a bijection between the two sets.

Every solution of $\mathcal{T}$ corresponds to a unique solution in $\mathcal{T}'$: if $(\mathbf{a}, \mathbf{b}, \mathbf{c}) \in \mathcal{T}$ then $M(\mathbf{a})\mathbf{c} = 0$ and thus $\Gamma M(\mathbf{a})\mathbf{c} = 0$. Further, $\mathbf{b}^T\mathbf{q} \neq 0$ by the choice of $\mathbf{q}$, so there is a unique choice $z = \frac{1}{\mathbf{b}^T\mathbf{q}}$ such that $(\mathbf{a}, \mathbf{b}, \mathbf{c}, \frac{1}{\mathbf{b}^T\mathbf{q}}) \in \mathcal{T}'$.

Conversely, let $(\mathbf{a}, \mathbf{b}, \mathbf{c}, \beta) \in \mathcal{T}'$. We will show that $(\mathbf{a}, \mathbf{b}, \mathbf{c}) \in T$.

We need to show that $M(\mathbf{a})\mathbf{c} = 0$. It holds that $\Gamma M(\mathbf{a})\mathbf{c} = 0$, so $M(\mathbf{a})\mathbf{c} = \alpha\mathbf{q}$ for some $\alpha \in \mathbb{C}$ since it is in $\ker(\Gamma)$. But since $(\mathbf{a}, \mathbf{b}, \mathbf{c}, \beta)$ is a solution to the system in Definition 3.12, $\mathbf{b}$ satisfies the equation $\mathbf{b}^T M(\mathbf{a}) = 0$ (in item 1 of Definition 3.7) so

$$0 = \mathbf{b}^T M(\mathbf{a})\mathbf{c} = \alpha\mathbf{b}^T\mathbf{q}.$$

Since $\beta\mathbf{b}^T\mathbf{q} = 1$, $\mathbf{b}^T\mathbf{q} \neq 0$, and we must have $\alpha = 0$ and $M(\mathbf{a})\mathbf{c} = 0$. □

Lemma 3.14. *The size of $\mathcal{T}'$, that is, the number of solutions to the system in Definition 3.12, is at most $2^{n-2} \cdot \left(\frac{e(2m-1)}{n-1}\right)^{n-1}$.*

Proof. Our sets of variables are denoted $\mathbf{x}, \mathbf{u}, \mathbf{v}, z$, so that, in the notation of Theorem 3.11, we have $n_1 = n, n_2 = n_3 = m$ and $n_4 = 1$. We list the multi-degrees of the equations, in the order listed in Definition 3.7 (but recall we are working with the amended system in Definition 3.12), and deduce the corresponding linear form in the variables y_1, y_2, y_3, y_4, in the notation of Theorem 3.11.

1. $(1,1,0,0)$ (m equations), and for each the corresponding linear form is $y_1 + y_2$
2. $(1,0,1,0)$ ($m-1$ equations, with linear form $y_1 + y_3$)
   Here the number of equations is $m-1$, due to the amendment detailed in Definition 3.12.
3. $(0,1,1,0)$ ($n-2$ equations, with linear form $y_2 + y_3$)
4. $(1,0,0,0)$ (1 equation, with linear form y_1)
5. $(0,1,0,0)$ (1 equation, with linear form y_2)
6. $(0,0,1,0)$ (1 equation, with linear form y_3)
7. Finally, we added the equation $z\mathbf{u}^T\mathbf{q} = 1$, which has multi-degree $(0,1,0,1)$ with linear form $y_2 + y_4$.

The corresponding Bézout number is therefore the coefficient of $y_1^n y_2^m y_3^m y_4$ in the polynomial

$$(y_1 + y_2)^m \cdot (y_1 + y_3)^{m-1} \cdot (y_2 + y_3)^{n-2} \cdot y_1 \cdot y_2 \cdot y_3 \cdot (y_2 + y_4),$$

or the coefficient of $y_1^{n-1} y_2^{m-1} y_3^{m-1}$ in

$$(y_1 + y_2)^m \cdot (y_1 + y_3)^{m-1} \cdot (y_2 + y_3)^{n-2}.$$

Expanding the product, this polynomial equals

$$\left(\sum_{k_1=0}^{m} \binom{m}{k_1} y_1^{k_1} y_2^{m-k_1}\right) \cdot \left(\sum_{k_2=0}^{m-1} \binom{m-1}{k_2} y_1^{k_2} y_3^{m-1-k_2}\right) \cdot \left(\sum_{k_3=0}^{n-2} \binom{n-2}{k_3} y_2^{k_3} y_3^{n-2-k_3}\right)$$

Suppose we pick from the first factor a summand $k_1 = k$, for some value of k, which gives us $y_1^k y_2^{m-k}$. Then in order to contribute to the coefficient of $y_1^{n-1} y_2^{m-1} y_3^{m-1}$ we must pick $k_2 = n-1-k$ from the second factor, and $k_3 = k-1$ from the third. The relevant coefficient is therefore

$$B := \sum_{k=0}^{m} \binom{m}{k} \cdot \binom{m-1}{n-1-k} \cdot \binom{n-2}{k-1}$$

For simplicity, we use the convention $\binom{i}{j} = 0$ whenever $j > i$ or $j < 0$. Since $\binom{n-2}{k-1} \leq 2^{n-2}$, we get

$$B \leq 2^{n-2} \cdot \sum_{k=0}^{n} \binom{m}{k} \cdot \binom{m-1}{n-1-k} = 2^{n-2} \binom{2m-1}{n-1} \leq 2^{n-2} \cdot \left(\frac{e(2m-1)}{n-1}\right)^{n-1}. \qquad \square$$

We can now finish the proof of Theorem 1.1.

Proof of Theorem 1.1. Let $M(\mathbf{x})$ be a determinantal representation of the polynomial $\sum_{i=1}^{n} x_i^n$. Let $\mathcal{S}, \mathcal{T}, \mathcal{T}'$ be the sets as defined above.

By Corollary 3.10, we have that $|\mathcal{T}|$ is finite and $|\mathcal{T}| \geq (n-1)^{(n-2)}$. By Lemma 3.14 and Claim 3.13, we have that $|\mathcal{T}| \leq 2^{n-2} \cdot \left(\frac{e(2m-1)}{n-1}\right)^{n-1}$.

Combining these bounds, we get that indeed $m = \Omega(n^2)$. $\square$

References

[Abe18] Simon Abelard. *Comptage de points de courbes hyperelliptiques en grande caractéristique : algorithmes et complexité*. PhD thesis, Université de Lorraine, 2018.

[BS83] Walter Baur and Volker Strassen. The Complexity of Partial Derivatives. *Theoretical Computer Science*, 22:317–330, 1983.

[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.

[CKSV22] Prerona Chatterjee, Mrinal Kumar, Adrian She, and Ben Lee Volk. Quadratic Lower Bounds for Algebraic Branching Programs and Formulas. *Comput. Complex.*, 31(2):8, 2022.

[CKV24] Abhranil Chatterjee, Mrinal Kumar, and Ben Lee Volk. Determinants vs. Algebraic Branching Programs. *Comput. Complex.*, 33(2):11, 2024.

[JS07] Gabriela Jeronimo and Juan Sabia. Computing multihomogeneous resultants using straight-line programs. *Journal of Symbolic Computation*, 42(1):218–235, 2007. Effective Methods in Algebraic Geometry (MEGA 2005).

[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.

[KV22] Mrinal Kumar and Ben Lee Volk. A Lower Bound on Determinantal Complexity. *Comput. Complex.*, 31(2):12, 2022.

[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`.

[MS87] Alexander Morgan and Andrew Sommese. A homotopy for solving general polynomial systems that respects m-homogeneous structures. *Applied Mathematics and Computation*, 24(2):101–113, 1987.

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

[Sha13] Igor R. Shafarevich. *Basic Algebraic Geometry 1: Varieties in Projective Space*. Springer, Berlin, Heidelberg, 3 edition, 2013.

[She26] Karthik Sheshadri. A near-quadratic lower bound on the border determinantal complexity of $\sum_i x_i^n$ via conormal specialization, 2026. Pre-print available at `arXiv:2606.13628`.

[Str73a] Volker Strassen. Die Berechnungskomplexität Von Elementarsymmetrischen Funktionen Und Von Interpolationskoeffizienten. *Numerische Mathematik*, 20(3):238–251, June 1973.

[Str73b] Volker Strassen. Vermeidung von Divisionen. *Journal für die reine und angewandte Mathematik*, 264:184–202, 1973.

[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*, pages 249–261. ACM, 1979.

[Wik26] Wikipedia contributors. Multi-homogeneous Bézout theorem, 2026. Accessed: 2026-09-24.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il