Electronic Colloquium on Computational Complexity, Report No. 125 (2024)

On read-k projections of the determinant

Pavel Hrubeš* Pushkar S. Joglekar†

Abstract

We consider read-k determinantal representations of polynomials and prove some non-expressibility results. A square matrix M whose entries are variables or field elements will be called *read-k*, if every variable occurs at most k times in M. It will be called a *determinantal representation* of a polynomial f if $f = \det(M)$. We show that

- the $n \times n$ permanent polynomial does not have a read-k determinantal representation for $k \in o(\sqrt{n}/\log n)$ (over a field of characteristic different from two).

We also obtain a quantitative strengthening of this result by giving a similar non-expressibility for $k \in o(\sqrt{n}/\log n)$ for an explicit *n-variate* multilinear polynomial (as opposed to the permanent which is n^2-variate).

1 Introduction

In algebraic complexity theory, two polynomials are of central interest: the determinant and the permanent of a square matrix. If X is an $n \times n$ matrix with indeterminates $x_{i,j}$ as entries, the polynomials are defined as

$$\det_n(X) = \sum_\sigma \text{sgn}(\sigma) \prod_{i=1}^n x_{i,\sigma(i)}\,,\ \text{perm}_n(X) = \sum_\sigma \prod_{i=1}^n x_{i,\sigma(i)}\,,$$

where σ ranges over permutations of $\{1, \dots, n\}$ and $\text{sgn}(\sigma) \in \{1, -1\}$ is the sign of σ. Motivated by similarity of these expressions, Pólya [9] asked whether there exists a simple expression of the permanent in terms of the determinant. This question, which may look like a mere mathematical curiosity, was placed into a deeper context by Valiant. In the seminal paper [10], he defined algebraic analogues of complexity classes P and NP, which we now call as VP and VNP. He showed that the permanent polynomial is complete for the class VNP (if the underlying field is of characteristic different from two). Since the determinant lies in VP, a "simple expression" of perm in terms of det would entail that the two complexity classes coincide.

*Institute of Mathematics of ASCR, Czechia, email: pahrubes@gmail.com. This work was supported by Czech Science Foundation GAČR grant 19-27871X.

†Vishwakarma Institute of Technology, Pune, India, email: joglekar.pushkar@gmail.com. The author would like to thank Pavel Hrubeš for hosting him at the Institute of Mathematics of ASCR where a part of this work was done.

ISSN 1433-8092

The precise version of Pólya's problem arising in this context is the following: if $m = m(n)$ is the smallest m so that we can express

$$\mathrm{perm}_n(X) = \det_m(M)\,, \tag{1}$$

where M is a matrix with variables or scalars as entries, can $m(n)$ be bounded by a polynomial in n or does it grow super-polynomially? This question is intimately related to the problem whether VP = VNP and is one of the major open problems in algebraic complexity theory. It is generally believed that m grows exponentially with n. However, the strongest lower bound known today – due to Mignon and Ressayre[1] [7], see also [4]– is quadratic in n. More on the fascinating story of the determinant and permanent can be found in [3, 1].

The problem can be refined in many ways. In this paper, we consider read-k representations. A matrix M whose entries are variables or field elements is *read-k*, if every variable occurs at most k times in M. It will be called a determinantal representation of a polynomial f if $f = \det(M)$. Read-k determinantal representations (or read-k projections of determinant) were defined in [2] where it was shown that for sufficiently large n, perm_n does not have a read-once determinantal representation. Note that in this setting, the question is not about the size of M but merely about its existence. A more general model of rank-k projections was considered in [5]. There it was shown that perm_n cannot be expressed as the determinant of a matrix of the form $A + \sum_{i,j} B_{i,j}x_{i,j}$ with $B_{i,j}$ matrices of rank at most 1.

Continuing this line of research, we will prove that perm_n does not have a read-k determinantal representation for $k \in o\left(\sqrt{n}/\log n\right)$. In fact, we will show that any M satisfying (1) must have $\Omega(n^{2.5}/\log n)$ entries containing a variable.

This result is incomparable with the quadratic lower bound on the size $m(n)$ of a determinantal representation. Denoting $s(n)$ the smallest number of entries containing a variable in a determinantal representation of perm_n, the two quantities are related by

$$m(n)/2 \le s(n) \le m(n)^2$$

(the first inequality follows from Lemma 1 below, the latter is obvious). This does not allow to deduce our lower bound $s(n) \ge \Omega(n^{2.5}/\log n)$ from the bound $m(n) \ge \Omega(n^2)$ in [7], or vice versa. On the other hand, super-polynomial lower bounds on $s(n)$ and $m(n)$ are *equivalent*.

On a high level, our proof follows ideas of Nechiporuk [8] which were later adapted to the algebraic setting by Kalorkoti [6]. As a technical component, which may be of an independent interest, we identify a specific property differentiating the determinant and the permanent. We will show that every multilinear polynomial f in n variables can be expressed as the permanent of a *read-once* matrix (of an exponential size). This follows by inspecting Valiant's VNP-completeness proof in [10]. An analogous statement is false in the case of the determinant: there exists such an f which requires read-k determinantal representations with k exponential in n. This is proved by a non-constructive counting argument.

[1] In fact, the lower bound holds even if M is allowed to have affine functions as entries.

Notation and definitions $\mathbb{F}$ will denote an underlying field. Unless stated otherwise, the field is arbitrary. X will denote a set of variables.

Given a matrix M with entries from $\mathbb{F} \cup X$, its *variable size* is the number of entries containing a variable. It will be called *read-k* if every variable appears at most k times in M. For a polynomial $f \in \mathbb{F}[X]$, M will be called a *determinantal representation of f* if $f = \det(M)$.

As usual, $[n] = \{1, \ldots, n\}$.

2 Some properties of determinantal representations

We first show that the size of a determinantal representation can be bounded in terms of its variable size.

Lemma 1. *Let M be a square matrix with entries from $\mathbb{F} \cup X$ of variable size $s \geq 1$. Then there exists a $2s \times 2s$ matrix H of variable size s with entries from $\mathbb{F} \cup X$ such that $\det(H) = \det(M)$. Moreover, each variable occurs in H the same number of times as in M and the variables appear on the main diagonal of H only.*

Proof. The lemma is proved in two steps. In the first step, we transform M to a matrix M^* with the same determinant such that every row and column of M^* contains at most one variable. In the second step, we reduce the dimension of M^*.

Assume that M is an $m \times m$ matrix. For the first step, suppose that M contains a variable x in the (i, j)-th position. Let M' be the $(m+2) \times (m+2)$ matrix

$$M' := \begin{pmatrix} M_0 & e_i & \\ & 1 & x \\ e_j^t & 0 & 1 \end{pmatrix},$$

where M_0 is obtained by setting the (i, j)-th entry to zero in M, e_i is the i-th unit column vector, e_j^t is the j-th unit row vector, and the unspecified entries are zero. Using cofactor expansion on the last column, we obtain $\det(M) = \det(M')$. The number of occurrences of variables has not changed while the displayed variable does not share a row or column with another variable. Repeating this construction s times for each variable in M, we indeed obtain an $(m + 2s) \times (m + 2s)$ matrix M^* with $f = \det(M^*)$ whose rows and columns contain at most one variable each.

We now proceed with the second step. Permuting rows and columns of M^*, we can write $\det(M) = \pm \det(N)$ with

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

where A, B, C, D are of dimensions $s \times s$, $s \times (s+m)$, $(s+m) \times s$, $(s+m) \times (s+m)$, respectively, and variables appear on the main diagonal of A only.

Since B has s rows, it has rank at most s. We can also assume that every column of B is a linear combination of its first s columns. Applying suitable column operations to the last $m+s$ columns of N, we can further convert N to the form

$$\begin{pmatrix} A & B_1 & 0 \\ C & D_1 & D_2 \end{pmatrix},$$

with B_1 being an $s \times s$ matrix. D_2 is of dimension $(m+s) \times m$ and hence has rank at most m. Assuming that every row of D_2 is a linear combination of its last m rows, we can apply row-operations to write

$$\det(M) = \pm \det \begin{pmatrix} A & B_1 & 0 \\ C_1 & D_1' & 0 \\ C_2 & D_1'' & D_2' \end{pmatrix} = \pm \det(D_2') \det \begin{pmatrix} A & B_1 \\ C_1 & D_1' \end{pmatrix},$$

where D_2' is an $m \times m$ scalar matrix. The matrix $H = \begin{pmatrix} A & B_1 \\ C_1 & D_1' \end{pmatrix}$ is a $2s \times 2s$ matrix consisting of scalars except for the s variables on the diagonal of A. Since the last column of H contains field elements only, the factor $\pm\det(D_2')$ can be moved inside H by multiplying the last column. $\square$

This leads to the following non-constructive lower bound on variable size of determinantal representations.

Theorem 2. *For every n, there exists a multilinear polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$ such that every determinantal representation of f requires variable size $\Omega(2^{n/2})$.*

Proof. Let s_n be the smallest $s \geq 1$ such that every multilinear polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$ has a determinantal representation of variable size s. Lemma 1 implies that every such f can be expressed as $f = \det(C + x_1 D_1 + \cdots + x_n D_n)$ where C is a scalar matrix and $D_1, \ldots, D_n$ are diagonal matrices in $\mathbb{F}^{2s_n \times 2s_n}$. Viewing entries of C and diagonal entries of $D_1, \ldots, D_n$ as parameters, every coefficient of f is a polynomial function of these parameters. Since f has 2^n coefficients and there are $k = (2s_n)^2 + 2s_n n$ parameters, this gives a polynomial map $G : \mathbb{F}^k \to \mathbb{F}^{2^n}$ whose image contains all of $\mathbb{F}^{2^n}$. This implies $k \geq 2^n$. For if $\mathbb{F}$ is finite of size q, we must have $q^k \geq q^{2^n}$. If $\mathbb{F}$ is infinite and $k < 2^n$, there would exist a non-trivial polynomial vanishing on $\mathbb{F}^{2^n}$, which is impossible. Finally, $k \geq 2^n$ implies $s_n \geq (1-\epsilon)2^{n/2-1}$ for every $\epsilon > 0$ and n sufficiently large. $\square$

3 A property of the permanent

We now show that Lemma 1 and Theorem 2 fail when the determinant is replaced with the permanent polynomial. It follows from Valiant's completeness results that every multilinear polynomial in $\mathbb{F}[X]$ can be expressed both as $\mathrm{perm}_m(M)$ and $\det_m(M')$ where M, M' are matrices over $\mathbb{F} \cup X$ of an exponential size. Hence, from the perspective of matrix size, the two polynomials are indistinguishable. However, we show that in the case of the permanent, the matrix M can be assumed to be *read-once*:

Theorem 3. *Let $\mathbb{F}$ be a field of characteristic different from two. Let $f \in \mathbb{F}[x_1, \ldots, x_n]$ be a multilinear polynomial. Then there exists $m \leq O(2^n)$ and a matrix M with entries in $\mathbb{F} \cup \{x_1, \ldots, x_n\}$ such that $f = \mathrm{perm}_m(M)$ and each variable x_i appears in M* exactly once*. Moreover, every row and column of M contains at most one variable.*

We outline the proof of Theorem 3 in the rest of this section. It follows by inspection of Valiant's proof of VNP completeness of the permanent. We refer to [11], [3] for a detailed exposition of Valiant's work.

Recall that an *arithmetic formula* over a field $\mathbb{F}$ is a rooted binary tree whose leaves are labelled with variables or field elements and other vertices are labelled with one of the operation $+$ or $\times$. As the *size* of a formula, we take the number of $+, \times$ operations. Every vertex in a formula computes a polynomial in the obvious way.

The following two lemmas are paraphrased versions of Theorem 21.27 and 21.29 from [3].

Lemma 4 ([3])**.** *Let F be an arithmetic formula of size m computing a polynomial $f \in \mathbb{F}[X]$. Then there exists an $(2m+2) \times (2m+2)$ matrix M with entries from $\mathbb{F} \cup X$ such that $f = \mathrm{perm}_{2m+2}(M)$ and every variable occurs in M the same number of times it occurs in F. Moreover, every column and row of M contains at most one variable.*

Lemma 5 ([3])**.** *Let $\mathbb{F}$ be a field of characteristic different from two. Let M be an $m \times m$ matrix with entries from $\mathbb{F} \cup \{x_1, \ldots, x_n, y_1, \ldots, y_k\}$ having in each row and column at most one variable. Then there exists $m' \leq 10m$ and an $m' \times m'$ matrix M' with entries from $\mathbb{F} \cup \{x_1, \ldots, x_n\}$ such that $\mathrm{perm}_{m'}(M') = \sum_{y_1,\ldots,y_k \in \{0,1\}} \mathrm{perm}_m(M)$ and every variable x_i occurs in M' the same number of times it occurs in M . Moreover, every row and column of M' contains at most one variable.*

We also need the following simple fact:

Lemma 6. *Every n-variate multilinear polynomial can be computed by an arithmetic formula of size $O(2^n)$.*

Proof. If f is a multilinear polynomial with $n > 0$ variables, we can write it as

$$f(x_1, \ldots, x_n) = x_n f_1(x_1, \ldots, x_{n-1}) + f_0(x_1, \ldots, x_{n-1}),$$

where f_1, f_0 are multilinear polynomials in $n-1$ variables. Given formulas for f_0, f_1 of size at most s, we obtain a formula for f of size $\leq 2s+2$. By induction, this gives a formula of size $O(2^n)$. □

Now we are ready to prove Theorem 3.

Proof of Theorem 3. Let X be the set of variables $\{x_1, \ldots, x_n\}$. Let $f \in \mathbb{F}[X]$ be a multilinear polynomial

$$f = \sum_{S \subseteq [n]} a_S \prod_{i \in S} x_i.$$

Introduce new variables $Y = \{y_1, \dots, y_n\}$. Let $\hat{f}$ be the polynomial

$$\hat{f}(y_1, \dots, y_n) = \sum_{S \subseteq [n]} a_S \prod_{i \in S} y_i \prod_{i \in [n] \setminus S} (1 - y_i) \, .$$

This guarantees that for any boolean substitution $y_1, \dots, y_n \in \{0, 1\}$, $\hat{f}(y_1, \dots, y_n) = a_S$ where $S = \{i \mid y_i = 1\}$. We can therefore write

$$f = \sum_{y_1, \dots, y_n \in \{0,1\}} \hat{f}(y_1, \dots, y_n) \prod_{i=1}^{n} (x_i y_i + (1 - y_i)) \, .$$

Note that in this expression, each x_i appears exactly once. Let g be the polynomial $\hat{f}(y_1, \dots, y_n) \prod_{i=1}^{n}(x_i y_i + (1 - y_i))$. As $\hat{f}$ is multilinear, it has a formula of size $O(2^n)$ by Lemma 6. It follows that g has a formula of size $O(2^n)$ in which each variable from X appears exactly once. Lemma 4 gives an $m' \times m'$ matrix M' with $m' \leq O(2^n)$ with entries from $\mathbb{F} \cup X \cup Y$ such that $g = \mathrm{perm}_{m'}(M')$, each variable from X appears exactly once in M' and every row or column of M' contains at most one variable. Since $f = \sum_{y_1, y_2, \dots, y_n \in \{0,1\}} g(X, Y)$ we can apply Lemma 5 to obtain the desired matrix M. □

4 Permanent versus determinant

We now prove our main result on variable size of determinantal representations of permanent.

Theorem 7. *Over a field of characteristic different from two, every determinantal representation of* perm_n *requires variable size* $\Omega(n^{5/2}/\log n)$.

Proof. Let X be the set of variables $\{x_{i,j} | 1 \leq i, j \leq n\}$ and let $\bar{X}$ be the $n \times n$ matrix with $x_{i,j}$ in (i, j)-th entry. Assume that $\mathrm{perm}_n(\bar{X}) = \det(M)$ where M is a matrix with entries from $\mathbb{F} \cup X$.

Let $Z \subseteq X$ be a set of k variables $x_{i_1,j_1}, \dots, x_{i_k,j_k}$ where $i_1, \dots, i_k$ are distinct and $j_1, \dots, j_k$ are also distinct. If $k = \lfloor \log_2 n - c \rfloor$, where c is a suitable absolute constant, Theorem 3 implies[2] the following:

for every multilinear polynomial $f \in \mathbb{F}[Z]$, there exists a matrix $\bar{X}_f$ obtained by setting variables outside of Z to constants in $\bar{X}$ such that $f = \mathrm{perm}_n(\bar{X}_f)$.

Since $\mathrm{perm}_n(\bar{X}) = \det(M)$, this means that also $f = \det(M_f)$ where M_f is obtained by setting variables outside of Z to constants in M. On the other hand, Theorem 2 shows that there exists a multilinear polynomial in $\mathbb{F}[Z]$ which requires determinantal representation of variable size $\Omega(2^{k/2})$. Hence M must contain $\Omega(2^{k/2})$ entries from Z. Inside X, we can find $t = n\lfloor \frac{n}{k} \rfloor$ such disjoint sets $Z_1, \dots, Z_t$. For every Z_i, M contains $\Omega(2^{k/2})$ entries from Z_i. Since the sets are disjoint, M contains $\Omega(t2^{k/2})$ entries from X altogether. This gives an $\Omega(n^{5/2}/\log n)$ lower bound on variable size of M. □

[2] Note that perm_n is invariant under permutations of rows and columns.

If perm_n has a read-k determinantal representation M then M has variable size at most n^2k. This implies:

Corollary 8. *Over a field of characteristic different from two, every read-k determinantal representation of* perm_n *requires* $k \geq \Omega(\sqrt{n}/\log n)$.

5 A harder multilinear polynomial

We now present an explicit multilinear polynomial U_n for which we can prove a quantitatively stronger lower bound than the one presented in Theorem 7. Another improvement is that the lower bound holds over any field. Furthermore, U_n has a polynomial-size arithmetic formula and hence also a polynomial determinantal representation (whereas for perm_n this is not known).

For an integer $n \geq 2$, let $r := \lfloor \log_2 n \rfloor - 1$ and $\ell := \lfloor n/2r \rfloor$. U_n has variables $x_{i,j}$, $i \in [\ell], j \in [r]$, and y_S, $S \subseteq [r]$, indexed by subsets of $[r]$. The number of variables is therefore $r\ell + 2^r \leq n$. U_n is defined as

$$\mathrm{U}_n := y_\emptyset + \sum_{i\in[\ell]} \sum_{\emptyset \neq S \subseteq [r]} y_S \prod_{j \in S} x_{i,j} \,.$$

Theorem 9. *Over any field, every determinantal representation of* U_n *requires variable size* $\Omega(n^{1.5}/\log n)$.

Proof sketch. U_n is defined to have the following property: given $i \in [\ell]$ and a multilinear polynomial $f \in \mathbb{F}[x_{i,1}, \ldots, x_{i,r}]$ of the form $\sum_{S\subseteq[r]} a_S \prod_{j\in S} x_{i,j}$, we can set $x_{i',j}$ to zero for every $i' \neq i$ and y_S to a_S for every S to obtain the polynomial f from U_n. This is precisely the property we used in the proof of Theorem 7, except that U_n has fewer variables. The same argument as in Theorem 7 gives that every determinantal representation of U_n contains $\Omega(\ell 2^{r/2})$ variables which gives the bound $\Omega(n^{1.5}/\log n)$. ☐

Let us make some comments:

(i) Every read-k determinantal representation of U_n requires $k \geq \Omega(\sqrt{n}/\log n)$.

(ii) On the other hand, U_n has a read-$O(n)$ determinantal representation of variable size $O(n^2)$.

(i) is an immediate consequence of Theorem 9. (ii) follows by, first, observing that U_n has an arithmetic formula in which every variable appears $O(n)$ times and, second, that Lemma 4 holds also when perm_{2m+2} is replaced with $\det_{2m+2}$.

References

[1] Manindra Agrawal. Determinant versus permanent. *Proceedings of the International Congress of Mathematicians*, 3:985–998, 07 2008.

[2] N. R. Aravind and P. S. Joglekar. On the expressive power of read-once determinants. In *Fundamentals of Computation Theory - 20th International Symposium*, volume 9210 of *Lecture Notes in Computer Science*, pages 95–105. Springer, 2015.

[3] P. Bürgisser, M. Clausen, and M. A. Shokrollahi. *Algebraic complexity theory*, volume 315 of *Grundlehren der mathematischen Wissenschaften*. Springer, 1997.

[4] J. Cai, X. Chen, and D. Li. A quadratic lower bound for the permanent and determinant problem over any characteristic $\neq 2$. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing*, pages 491–498, 2008.

[5] Ch. Ikenmeyer and J. M. Landsberg. On the complexity of the permanent in various computational models. *CoRR*, abs/1610.00159, 2016.

[6] K. Kalorkoti. A lower bound for the formula size of rational functions. *SIAM J. Comput.*, 14(3):678–687, 1985.

[7] T. Mignon and N. Ressayre. A quadratic bound for the determinant and permanent problem. *International Mathematics Research Notices*, pages 4241–4253, 2004.

[8] E. I. Nechiporuk. On a boolean function. *Soviet Math. Dokl.*, 7(4):999–1000, 1966.

[9] G. Pólya. Aufgabe 424. *Arch. Math. Phys.*, 20(271), 1913.

[10] Leslie G. Valiant. Completeness classes in algebra. In *Proceedings of the 11h Annual ACM Symposium on Theory of Computing,*, pages 249–261. ACM, 1979.

[11] Joachim von zur Gathen. Feasible arithmetic computations: Valiant's hypothesis. *J. Symb. Comput.*, 4(2):137–172, 1987.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il