A Quadratic Lower Bound for the Permanent and Determinant Problem over any Characteristic $\neq 2$

Jin-Yi Cai
Computer Sciences
Department, University of Wisconsin, Madison
and Radcliffe Institute
Harvard University, U.S.A.
jyc@cs.wisc.edu

Xi Chen
School of Mathematics
Institute for Advanced Study
U.S.A.
csxichen@gmail.com

Dong Li
School of Mathematics
Institute for Advanced Study
U.S.A.
dongli@math.ias.edu

ABSTRACT

In Valiant's theory of arithmetic complexity, the classes VP and VNP are analogs of P and NP. A fundamental problem concerning these classes is the Permanent and Determinant Problem: Given a field $\mathbb{F}$ of characteristic $\neq 2$, and an integer n, what is the minimum m such that the permanent of an $n \times n$ matrix $\mathbf{X} = (x_{ij})$ can be expressed as a determinant of an $m \times m$ matrix, where the entries of the determinant matrix are affine linear functions of x_{ij}'s, and the equality is in $\mathbb{F}[\mathbf{X}]$. Mignon and Ressayre (2004) [11] proved a quadratic lower bound $m = \Omega(n^2)$ for fields of characteristic 0. We extend the Mignon-Ressayre quadratic lower bound to all fields of characteristic $\neq 2$.

Categories and Subject Descriptors

F.2.1 [**Analysis of Algorithms and Problem Complexity**]: Numerical Algorithms and Problems—*Computations in finite fields, Computations on matrices, Computations on polynomials*

General Terms

Theory

Keywords

Permanent, determinant, arithmetic complexity, finite field

1. INTRODUCTION

Given a set of n^2 indeterminates $\mathbf{X} = (x_{i,j})_{i,j=1,\ldots,n}$ over a field $\mathbb{F}$, we can define

$$\det(\mathbf{X}) = \textstyle\sum_{\pi \in S_n} \operatorname{sign}(\pi) \prod_{i=1}^{n} x_{i,\pi(i)}, \quad \text{and}$$
$$\operatorname{per}(\mathbf{X}) = \textstyle\sum_{\pi \in S_n} \prod_{i=1}^{n} x_{i,\pi(i)}.$$

The determinant function is certainly one of the most well-studied functions in mathematics. The permanent function is also well-studied, especially in combinatorics [12]. For example, if $\mathbf{A}$ is a 0-1 matrix then $\operatorname{per}(\mathbf{A})$ counts the number of perfect matchings in a bipartite graph with adjacency matrix $\mathbf{A}$.

These well-known functions took on important new meanings when viewed from the computational complexity perspective. It is well known that the determinant can be computed in polynomial time. In fact it can be computed in the complexity class NC^2. By contrast, Valiant [22, 21] showed that computing the permanent is #P-complete.

In fact, Valiant [21] (see also [4, 5]) has developed a substantial theory. The complexity classes $\mathrm{VP}_{\mathbb{F}}$ and $\mathrm{VNP}_{\mathbb{F}}$ are the analogs of P and NP in this theory of arithmetic complexity, and det and per functions are the central objects in the two classes, respectively. It was shown that the complexity of computing the permanent characterizes the class $\mathrm{VNP}_{\mathbb{F}}$ and the complexity of computing the determinant (almost) characterizes the class $\mathrm{VP}_{\mathbb{F}}$.

More precisely, a family of polynomials $\{f_n\}$ is in $\mathrm{VP}_{\mathbb{F}}$ if $\deg(f_n) = n^{O(1)}$ and there is a family of arithmetic circuits of size $n^{O(1)}$ computing $\{f_n\}$. A family of polynomials $\{g_n\}$ is in $\mathrm{VNP}_{\mathbb{F}}$ if $\deg(g_n) = n^{O(1)}$, and there exists a family of polynomials $\{f_n\} \in \mathrm{VP}_{\mathbb{F}}$ such that

$$g_n(x_1, ..., x_n) = \sum_{y_1,\ldots,y_m \in \{0,1\}} f_{n+m}(x_1, ..., x_n, y_1, ..., y_m),$$

where $m = n^{O(1)}$. We say that $\{f_n\}$ is a projection of $\{g_m\}$ if there are some $\alpha_1, \alpha_2, \ldots, \alpha_m \in \mathbb{F} \cup \{x_1, \ldots, x_n\}$, such that $f_n(x_1, \ldots, x_n) = g_m(\alpha_1, \ldots, \alpha_m)$. It is a p-projection if $m = n^{O(1)}$. A projection is a particularly simple reduction. It is a special case of an affine linear reduction, where each α_i is an affine linear function of x_i's. Valiant proved that

THEOREM 1 (VALIANT). *For any field $\mathbb{F}$,* $\operatorname{per} \in \mathrm{VNP}_{\mathbb{F}}$. *Moreover, for any $\mathbb{F}$ with* char $\mathbb{F} \neq 2$, *any $\{f_n\} \in \mathrm{VNP}_{\mathbb{F}}$ is a p-projection of* per.

It is also known that det is in $\mathrm{VP}_{\mathbb{F}}$ [23]. More exact characterizations of det were given in terms of polynomial-sized arithmetic branching programs [7, 19, 24].

THEOREM 2 (VALIANT). *Any polynomial f_n is a projection of* $\det_m$ *of an $m \times m$ matrix, where m is linear in the formula size of f_n. In particular, if $\{f_n\}$ has polynomial formula size, then $\{f_n\}$ is a p-projection of* det. *Also if $\{f_n\} \in \mathrm{VP}_{\mathbb{F}}$, then f_n is the projection of* $\det_m$ *for some $m = n^{O(\log n)}$.*

By Ryser's formula [12], per_n has formula size $O(n^2 2^n)$. Thus by Valiant's theorem it is the projection of $\det_m$, where $m = O(n^2 2^n)$. Furthermore if we view Ryser's formula as on the truncated linear row sums directly (instead of on the variables), then Valiant's theorem implies that

THEOREM 3. *For every n, there exists a collection $\mathbf{A}$ of affine linear functions $A_{k,l}(\mathbf{X})$ over n^2 variables, where $1 \le k, l \le m = O(2^n)$, such that $\mathrm{per}_n(\mathbf{X}) = \det_m(\mathbf{A}(\mathbf{X}))$.*

It is remarkable that this is the best general upper bound known for this.

DEFINITION 1. *The determinantal complexity dc of f_n is the minimum integer m, such that there exist affine linear functions $A_{k,l}(\mathbf{X})$, where $1 \le k, l \le m$, such that $f_n(\mathbf{X}) = \det_m(\mathbf{A}(\mathbf{X}))$.*

The question addressed in this paper is about $\mathsf{dc}(\mathrm{per}_n)$. Valiant's analog of P $\neq$ NP will follow if one can show a lower bound $\mathsf{dc}(\mathrm{per}_n) = n^{\omega(\log n)}$.

In some sense this problem has a longer history. Pólya [14] was the first to ask a question on when one can express a permanent as a modified determinant. He noticed that

$$\mathrm{per}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \det\begin{pmatrix} a & -b \\ c & d \end{pmatrix},$$

and asked if there are any similar equations, by affixing ± 1 to the variables, for $n \ge 3$. This was answered in the negative by Szegö [18]. This line of inquiry culminated in

THEOREM 4 (MARCUS, MINC). *If $\mathrm{char}\ \mathbb{F} = 0$ and $n \ge 3$, then there are no homogeneous linear functions $f_{k,\ell}$ in the indeterminates $x_{i,j}$ $(1 \le i, j, k, \ell \le n)$ such that $\mathrm{per}(x_{i,j}) = \det(f_{k,\ell})$.*

In terms of $\mathsf{dc}(\mathrm{per}_n)$, this celebrated theorem is equivalent to $\mathsf{dc}(\mathrm{per}_n) \ge n+1$, over fields of $\mathrm{char}\ \mathbb{F} = 0$ (note that if the permanental matrix is also $n \times n$, then clearly constant terms in affine linear equations do not help, as seen by the homogeneous part.).

The first non-trivial lower bound for $\mathsf{dc}(\mathrm{per}_n)$ is by von zur Gathen [25], who showed that $\mathsf{dc}(\mathrm{per}_n) \ge \sqrt{8/7}n$. (This was proved for p-projections.) Von zur Gathen's result was then improved independently by Babai and Seress (as reported in [26]), by Cai [6], and by Meshulam [10]. Their results were (ignoring lower order terms) $\mathsf{dc}(\mathrm{per}_n) \ge \sqrt{2}n$.

This rather weak lower bound stood as the best bound until 2004, when Mignon and Ressayre [11] proved that $\mathsf{dc}(\mathrm{per}_n) \ge n^2/2$, over any field of $\mathrm{char}\ \mathbb{F} = 0$. Over a field of $\mathrm{char}\ \mathbb{F} = p \neq 2$, the best bound is a very recent unpublished result by Valiant [20], which is $\Omega(n^{5/4})$ for projections.

More important than the bound $\sqrt{8/7}n$, von zur Gathen [25] introduced a method of taking derivatives and then comparing appropriate dimensions/ranks. The follow-up improvements to $\sqrt{2}n$ all use this approach.

The Mignon-Ressayre breakthrough [11] uses a new idea: Take second-order derivatives.

The key step in their proof [11] is to lower bound the rank of the second derivative matrix $\mathbf{H}$ of the permanent at a certain matrix $\mathbf{X}_0$. However, their proof encounters a major difficulty when $\mathrm{char}\ \mathbb{F} \neq 0$. The matrix $\mathbf{H}$ has various non-zero entries, which is a necessary condition to being of high rank. But these non-zero entries are all divisible by large factorials. Thus when $\mathrm{char}\ \mathbb{F} = p$, these entries are all zero, and the matrix $\mathbf{H}$ becomes $\mathbf{0}$. In this paper we overcome this difficulty by considering another explicit construction of matrix $\mathbf{X}_0$.

We mention some other related results. In [9], Jerrum and Snir showed that any monotone arithmetic circuit family that computes permanent must have exponential size. For depth-three arithmetic circuits over fields of characteristic 0, Shpilka and Wigderson [17] proved that the permanent (and determinant) requires circuit size $\Omega(n^2)$. For depth-three arithmetic circuits over finite characteristic, Grigoriev and Razborov [8] showed an exponential lower bound for both determinant and permanent. Raz [15] proved a lower bound of $n^{O(\log n)}$ on the size of families of multilinear formulas computing permanent and determinant. For syntactically multilinear arithmetic circuits, Raz, Shpilka and Yehudayoff [16] proved a $\Omega(n^{4/3}/\log^2 n)$ lower bound for an explicit multilinear function. A survey of some work on the Permanent and Determinant Problem can be found in [1], where it also discusses an algebraic geometry approach by Mulmuley and Sohoni [13] and connections to the pseudorandom generator used in the AKS proof for primality [2, 3].

This paper is organized as follows. In Section 2, we discuss the general approach by Mignon and Ressayre, and state our result. In Section 3, we prove an $\Omega(n^2)$ lower bound valid for all characteristic $\neq 2$. In Section 4 we indicate how to improve the leading constant in $\Omega(n^2)$ to match the Mignon-Ressayre bound.

2. THE APPROACH AND THE THEOREM

2.1 The Proof by Mignon and Ressayre

Given an $n \times n$ matrix $\mathbf{X} = (x_{i,j})_{i,j=1,2,\ldots,n}$ over a field $\mathbb{F}$, the determinant $\det(\mathbf{X})$ and the permanent $\mathrm{per}(\mathbf{X})$ are both polynomials of degree n over n^2 variables. Their partial derivatives of all orders are defined formally.

We use $\mathbf{H}(\mathbf{X}) = (H_{ij,kl})_{i,j,k,l=1,2,\ldots,n}$ to denote the *Hessian* matrix of $\mathrm{per}(\mathbf{X})$:

$$H_{ij,kl} = \frac{\partial^2 \mathrm{per}(\mathbf{X})}{\partial x_{i,j}\ \partial x_{k,l}} \in \mathbb{F}[\mathbf{X}], \quad \text{for all } 1 \le i, j, k, l \le n.$$

Similarly, we can define the Hessian matrix of $\det(\mathbf{X})$, and denote it by $\mathbf{H}_{\det}(\mathbf{X})$.

Now suppose that there exists a collection $\mathbf{A}$ of m^2 affine linear functions, where $\mathbf{A} = \{A_{k,l}(x_{1,1}, x_{1,2}, \ldots, x_{n,n}),\ k, l : 1 \le k, l \le m\}$, such that in the polynomial ring $\mathbb{F}[\mathbf{X}]$,

$$\mathrm{per}_n(\mathbf{X}) = \det_m\left((A_{k,l}(\mathbf{X}))_{1\le k,l\le m}\right). \qquad (1)$$

The first step in the proof by Mignon and Ressayre [11] is to transform $\mathbf{A}$ to a normal form. Consider a fixed matrix $\mathbf{X}_0 \in \mathbb{F}^{n\times n}$ such that $\mathrm{per}(\mathbf{X}_0) = 0$. We expand the affine linear functions $A_{k,l}(\mathbf{X})$ at $\mathbf{X}_0$, and write $(A_{k,l}(\mathbf{X})) = (L_{k,l}(\mathbf{X} - \mathbf{X}_0)) + \mathbf{Y}_0$ for some homogeneous linear functions $L_{k,l}$ and some matrix $\mathbf{Y}_0 \in \mathbb{F}^{m\times m}$. It follows from (1) that $\det(\mathbf{Y}_0) = \mathrm{per}(\mathbf{X}_0) = 0$. Let $\mathbf{C}$ and $\mathbf{D}$ be two non-singular matrices such that $\mathbf{C}\mathbf{Y}_0\mathbf{D}$ is a diagonal matrix

$$\begin{pmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_s \end{pmatrix}, \quad \text{where } s < m.$$

It follows from previous work [26, 6, 10] that if (1) holds then this s must be $m-1$. (But it will also follow easily from the Mignon-Ressayre proof.) Since the first row and column of $\mathbf{CY}_0\mathbf{D}$ are both zero, we may multiply diagonal matrices $\mathrm{diag}(\det(\mathbf{C})^{-1}, 1, \ldots, 1)$ and $\mathrm{diag}(\det(\mathbf{D})^{-1}, 1, \ldots, 1)$ to the left and right, so we may just assume $\det(\mathbf{C}) = \det(\mathbf{D}) = 1$. It follows that, by (multiplying matrices $\mathbf{C}$ and $\mathbf{D}$ to the left and right, and) renaming $L_{k,l}$ and $\mathbf{Y}_0$, we may assume (1) takes the form

$$\mathrm{per}(\mathbf{X}) = \det\Big(\big(L_{k,l}\,(\mathbf{X} - \mathbf{X}_0)\big) + \mathbf{Y}_0\Big),$$

where $\mathbf{Y}_0 = \mathrm{diag}(0, 1, \ldots, 1)$.

Now we can take second-order derivatives, and evaluate them at $\mathbf{X}_0$. By the chain rule,

$$\mathbf{H}(\mathbf{X}_0) = \mathbf{L} \cdot \mathbf{H}_{\det}(\mathbf{Y}_0) \cdot \mathbf{L}^T,$$

where $\mathbf{L}$ is an $n^2 \times m^2$ matrix over $\mathbb{F}$. It follows immediately that $\mathrm{rank}(\mathbf{H}(\mathbf{X}_0)) \leq \mathrm{rank}(\mathbf{H}_{\det}(\mathbf{Y}_0))$.

It is relatively easy to derive a $O(m)$ upper bound for the rank of $\mathbf{H}_{\det}(\mathbf{Y}_0)$. Notice that when one takes a partial derivative $\partial/\partial x_{ij}$ on the determinant (as well as on the permanent), one simply gets the minor after striking out row i and column j. Second order derivative $\partial^2/\partial x_{ij}\partial x_{kl}$ simply strikes out rows $\{i,k\}$ and columns $\{j,l\}$. By the form of $\mathbf{Y}_0$, to get a non-zero value for an entry (ij,kl) in $\mathbf{H}_{\det}(\mathbf{Y}_0)$, it must be that $1 \in \{i,k\}$ and $1 \in \{j,l\}$. In fact the only non-zero entries are

$$(ij,kl) = (11,tt), (tt,11), (1t,t1) \text{ or } (t1,1t),$$

for all $t > 1$. This immediately gives a $2m$ upper bound for $\mathrm{rank}(\mathbf{H}_{\det}(\mathbf{Y}_0))$. (If we did not assume $s = m-1$, then it would have been even more difficult to get a non-zero entry in $\mathbf{H}_{\det}(\mathbf{Y}_0)$. If $s = m-2$, there could be at most $O(1)$ many non-zero entries. If $s < m-2$, there are no non-zero entries.)

The real work of their proof is to find an explicit $\mathbf{X}_0$ such that $\mathrm{per}(\mathbf{X}_0) = 0$ and yet $\mathrm{rank}(\mathbf{H}(\mathbf{X}_0))$ is high. For the case when char $\mathbb{F} = 0$, they constructed an infinite sequence of $n \times n$ matrices $\mathbf{X}_0$ such that $\mathrm{per}_n(\mathbf{X}_0) = 0$ and the rank of the $n^2 \times n^2$ matrix $\mathbf{H}(\mathbf{X}_0)$ is full. This gives their quadratic lower bound $m = \Omega(n^2)$.

Theorem 5 (Mignon and Ressayre). *For any field of characteristic* 0, $\mathsf{dc}(\mathrm{per}_n) \geq n^2/2$.

However, their matrices $\mathbf{X}_0$ do not work for fields $\mathbb{F}$ with small characteristics, e.g., 3. All entries of $\mathbf{H}(\mathbf{X}_0)$ are divisible by large factorials, and thus, divisible by char $\mathbb{F}$. As a result, $\mathbf{H}(\mathbf{X}_0)$ becomes the zero matrix of rank 0. In a way, to get non-zero values for entries in $\mathbf{H}(\mathbf{X}_0)$, which are permanental minors of $\mathbf{X}_0$, and yet to be able to analyze the rank, the most natural approach is to assign pretty uniform values for $\mathbf{X}_0$. This is what was done. But these entries are non-zero by virtue of the fact that they are sums of constant terms with a large factorial number of terms. Thus the appearance of large factorials in $\mathbf{H}(\mathbf{X}_0)$ is not surprising. To avoid these factorials, we have to be more judicious in our choice of $\mathbf{X}_0$. We need it to be not terribly uniform, and yet sufficiently structured so that we can still calculate the rank for $\mathbf{H}(\mathbf{X}_0)$.

2.2 Our Main Result

Our main result is a new construction of matrix $\mathbf{X}_0$ such that $\mathbf{H}(\mathbf{X}_0)$ has almost full rank over any field of char $\mathbb{F} \neq 2$. More exactly, we will prove the following theorem in Section 4:

Theorem 6. *Let $p > 2$ be a prime, then*

1. *If $p \neq 23$, then for any $n > 2$ that satisfies $p \,|\, (n+1)$, there exists an $(n+1) \times (n+1)$ matrix $\mathbf{X}_0$ over finite field $\mathbb{F}_p$, such that $\mathrm{per}(\mathbf{X}_0) \equiv 0 \pmod p$ and*
$$\mathrm{rank}\,(\mathbf{H}(\mathbf{X}_0)) \geq (n-2)(n-3);$$
2. *If $p \neq 3, 5$, then for any $n > 1$ that satisfies $p \,|\, (n+2)$, there exists an $(n+1) \times (n+1)$ matrix $\mathbf{X}_0$ over finite field $\mathbb{F}_p$, such that $\mathrm{per}(\mathbf{X}_0) \equiv 0 \pmod p$ and*
$$\mathrm{rank}\,(\mathbf{H}(\mathbf{X}_0)) \geq (n-2)(n-3).$$

This implies the lower bound for $\mathsf{dc}(\mathrm{per}_n)$ over field $\mathbb{F}_p$. (We remark that a lower bound for $\mathbb{F}_p$ is also valid over $\mathbb{Q}$.)

Corollary 1. *For any prime $p \neq 2$, $\mathsf{dc}(\mathrm{per}_n) \geq (n-2)(n-3)/2$ over a field of char $\mathbb{F} = p$.*

To prove the theorem, we introduce, for any $v \in \mathbb{F}_p$, and integer $n \geq 1$, the following $(n+1) \times (n+1)$ matrix $\mathbf{M}_v^n = (M_{i,j})$: $M_{(n+1),(n+1)} = v$, $M_{i,i} = M_{(n+1),i} = M_{i,(n+1)} = 1$ for all $i : 1 \leq i \leq n$, and $M_{i,j} = 0$ otherwise. For example, $\mathbf{M}_2^3$ is given by

$$\mathbf{M}_2^3 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 2 \end{pmatrix}.$$

We will prove the two cases of Theorem 6 using $\mathbf{M}_1^n$ and $\mathbf{M}_2^n$ respectively. Given v and n, the following lemma essentially defines the Hessian matrix $\mathbf{H}(\mathbf{M}_v^n)$ of $\mathbf{M}_v^n$.

Lemma 1. *Let $\mathbf{H}(\mathbf{M}_v^n) = (H_{ij,kl}) \in \mathbb{F}_p^{(n+1)^2 \times (n+1)^2}$, then for all $i,j : 1 \leq i \neq j \leq n$ and $k,l : 1 \leq k \neq l \leq n$, we have*

$$H_{ij,kl} \equiv \begin{cases} v+n-2 & \textit{if } k = j \textit{ and } l = i; \\ 1 & \textit{if } k = j \textit{ and } l \neq i,j; \\ 1 & \textit{if } l = i \textit{ and } k \neq i,j; \\ 0 & \textit{otherwise.} \end{cases}$$

Given $v \in \mathbb{F}_p$ and $n \geq 1$, for i and $j : 1 \leq i \neq j \leq n$, we use $\mathbf{H}_{ij}$ to denote the (n^2-n)-dimensional vector truncated from the $(ij)^{th}$ row of $\mathbf{H}(\mathbf{M}_v^n)$: here we only keep its $(kl)^{th}$ entry if $1 \leq k \neq l \leq n$. For all i,j,k,l satisfying $1 \leq i \neq j \leq n$ and $1 \leq k \neq l \leq n$, the following lemma shows the possible values of the inner product $\mathbf{H}_{ij} \cdot \mathbf{H}_{kl}$.

Lemma 2. *Assume i and j satisfy $1 \leq i \neq j \leq n$, then*

1. $\mathbf{H}_{ij} \cdot \mathbf{H}_{ij} = (v+n-2)^2 + 2(n-2)$;
2. $\mathbf{H}_{ij} \cdot \mathbf{H}_{ji} = 0$;
3. *when $1 \leq k \leq n$ and $k \neq i,j$,* $\mathbf{H}_{ij} \cdot \mathbf{H}_{ik} = \mathbf{H}_{ij} \cdot \mathbf{H}_{kj} = 2(v+n-2) + (n-3)$;
4. *when $1 \leq k \leq n$ and $k \neq i,j$,* $\mathbf{H}_{ij} \cdot \mathbf{H}_{ki} = \mathbf{H}_{ij} \cdot \mathbf{H}_{jk} = 1$;
5. *when $1 \leq k \neq l \leq n$ and $\{k,l\} \cap \{i,j\} = \emptyset$,* $\mathbf{H}_{ij} \cdot \mathbf{H}_{kl} = 2$.

Proof. We only prove the first and third cases here. The other cases can be proved similarly.

For the first case, we run all possibilities (kl) where $1 \leq k \neq l \leq n$, and the only non-zero entries in $\mathbf{H}_{ij} \cdot \mathbf{H}_{ij}$ are $(v+n-2)^2$ for the index (ji), and 1 for indices (jt) and

(ti), where $1 \le t \le n$ and $t \neq i, j$. As a result, $\mathbf{H}_{ij} \cdot \mathbf{H}_{ij} = (v+n-2)^2 + 2(n-2)$. For the third case, the only non-zero entries in $\mathbf{H}_{ij} \cdot \mathbf{H}_{ik}$ are $(v+n-2)$ for indices (ji) and (ki), and 1 for indices (ti), where $1 \le t \le n$ and $t \neq i, j, k$, thus $\mathbf{H}_{ij} \cdot \mathbf{H}_{ik} = 2(v+n-2) + (n-3)$. $\square$

We also need the following lemma concerning the det of matrices of a specific form.

LEMMA 3. *Let $\mathbf{A} = (A_{i,j})_{i,j=1,\dots,n}$ be an $n \times n$ matrix over $\mathbb{F}_p$ satisfying $A_{i,i} = \alpha$ for all $1 \le i \le n$ and $A_{i,j} = \beta$ otherwise. Then,*

$$\det(\mathbf{A}) = \big(\alpha + (n-1)\beta\big)(\alpha - \beta)^{n-1}.$$

3. A WEAKER THEOREM

In this section, we prove the following weaker version of Theorem 6.

LEMMA 4. *Let $p > 2$ be a prime, then for any sufficiently large n satisfying $p \,|(n+1)$, we have $\mathrm{per}(\mathbf{M}_1^n) \equiv 0 \pmod p$ and rank$(\mathbf{H}(\mathbf{M}_1^n)) = \Omega(n^2)$.*

PROOF. In the proof, we denote matrix $\mathbf{M}_1^n$ by $\mathbf{M}$. Clearly $\mathrm{per}(\mathbf{M}) = n+1 \equiv 0 \pmod p$, so we only need to prove the second part.

Let S be a maximal subset of integers $\{i : 1 \le i < n/2\}$ with $|S| \equiv 2 \pmod p$, and T be a maximal subset of $\{j : n/2 \le j \le n\}$ with $|T| \equiv 2 \pmod p$. Both $|S|$ and $|T|$ are $\Omega(n)$.

We will show that there exists a sub-matrix $\mathbf{R}$ of $\mathbf{H}(\mathbf{M})$ with $|S| \cdot |T|$ rows, such that, $\det(\mathbf{R}\mathbf{R}^T)$ is non-zero. As a result, we have

$$\begin{aligned} \mathrm{rank}\big(\mathbf{H}(\mathbf{M})\big) &\ge \mathrm{rank}(\mathbf{R}) \\ &\ge \mathrm{rank}(\mathbf{R}\mathbf{R}^T) = |S| \cdot |T| = \Omega(n^2), \end{aligned}$$

and the lemma follows.

To get the matrix $\mathbf{R}$, we choose the following subset of rows and columns of $\mathbf{H}(\mathbf{M})$: rows (ij), where $i \in S$ and $j \in T$; and columns (kl), where $1 \le k \neq l \le n$. So $\mathbf{R}$ is an $(|S| \cdot |T|) \times (n^2 - n)$ matrix. Let $S = \{i_1, i_2, \dots, i_{|S|}\}$ and $T = \{j_1, j_2, \dots, j_{|T|}\}$, then we can write $\mathbf{R}$ as

$$\mathbf{R} = \begin{pmatrix} \mathbf{H}_{i_1 j_1} \\ \mathbf{H}_{i_1 j_2} \\ \vdots \\ \mathbf{H}_{i_1 j_{|T|}} \\ \mathbf{H}_{i_2 j_1} \\ \vdots \\ \mathbf{H}_{i_{|S|} j_{|T|}} \end{pmatrix},$$

where $\mathbf{H}_{ij}$ is the (n^2-n)-dimensional vector truncated from the $(ij)^{th}$ row of $\mathbf{H}(\mathbf{M})$.

Consider the inner products of arbitrary two rows of $\mathbf{R}$. By Lemma 2, we have for $i \in S$ and $j \in T$,

1. $\mathbf{H}_{ij} \cdot \mathbf{H}_{ij} = (v+n-2)^2 + 2(n-2) \equiv -2 \pmod p$, since $v = 1$, $n \equiv -1 \pmod p$;
2. when $j' \neq j$ and $j' \in T$, $\mathbf{H}_{ij} \cdot \mathbf{H}_{ij'} = 2(v+n-2) + (n-3) \equiv -8 \not\equiv 0 \pmod p$;
3. when $i' \neq i$ and $i' \in S$, $\mathbf{H}_{ij} \cdot \mathbf{H}_{i'j} \equiv -8 \not\equiv 0 \pmod p$;
4. when $i' \neq i$, $j' \neq j$, $i' \in S$ and $j' \in T$, $\mathbf{H}_{ij} \cdot \mathbf{H}_{i'j'} \equiv 2 \pmod p$.

Now we can write $\mathbf{R}\mathbf{R}^T$ as an $|S| \times |S|$ block matrix:

$$\mathbf{R}\mathbf{R}^T = \begin{pmatrix} \mathbf{A} & \mathbf{B} & \mathbf{B} & \cdots & \mathbf{B} \\ \mathbf{B} & \mathbf{A} & \mathbf{B} & \cdots & \mathbf{B} \\ \mathbf{B} & \mathbf{B} & \mathbf{A} & \cdots & \mathbf{B} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{B} & \mathbf{B} & \mathbf{B} & \cdots & \mathbf{A} \end{pmatrix}, \text{ where}$$

$$\mathbf{A} = \begin{pmatrix} a & b & b & \cdots & b \\ b & a & b & \cdots & b \\ b & b & a & \cdots & b \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b & b & b & \cdots & a \end{pmatrix}, \ \mathbf{B} = \begin{pmatrix} b & c & c & \cdots & c \\ c & b & c & \cdots & c \\ c & c & b & \cdots & c \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c & c & c & \cdots & b \end{pmatrix},$$

are both $|T| \times |T|$ matrices with $a = -2$, $b = -8$ and $c = 2$.

Next we apply the following operations to $\mathbf{R}\mathbf{R}^T$: subtract the second last column from the last column of $\mathbf{R}\mathbf{R}^T$ (here what we mean by "a column" is a whole block column of $\mathbf{R}\mathbf{R}^T$). Then subtract the third last column from the second last column … till subtract the first column from the second column. We end up with

$$\begin{pmatrix} \mathbf{A} & \mathbf{B}-\mathbf{A} & 0 & \cdots & 0 \\ \mathbf{B} & \mathbf{A}-\mathbf{B} & \mathbf{B}-\mathbf{A} & \cdots & 0 \\ \mathbf{B} & 0 & \mathbf{A}-\mathbf{B} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{B} & 0 & 0 & \cdots & \mathbf{B}-\mathbf{A} \\ \mathbf{B} & 0 & 0 & \cdots & \mathbf{A}-\mathbf{B} \end{pmatrix}.$$

Then we add the first row to the second row. Add the second row to the third row, etc. Finally, we get

$$\begin{pmatrix} \mathbf{A} & \mathbf{B}-\mathbf{A} & 0 & 0 & \cdots & 0 \\ \mathbf{A}+\mathbf{B} & 0 & \mathbf{B}-\mathbf{A} & 0 & \cdots & 0 \\ \mathbf{A}+2\mathbf{B} & 0 & 0 & \mathbf{B}-\mathbf{A} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}+(|S|-2)\mathbf{B} & 0 & 0 & 0 & \cdots & \mathbf{B}-\mathbf{A} \\ \mathbf{A}+(|S|-1)\mathbf{B} & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Clearly, all these operations do not change its determinant. By using Lemma 3, we have (here we use s and t to denote $|S|-1$ and $|T|-1$, respectively)

$$\begin{aligned} \det(\mathbf{R}\mathbf{R}^T) &= \pm \det(\mathbf{A}+s\mathbf{B}) \cdot (\det(\mathbf{B}-\mathbf{A}))^s \\ &= \pm \left(a + sb + t\,(b+sc)\right)\left(a+sb-(b+sc)\right)^t \\ &\quad \big((b-a+t\,(c-b))\,(b-a-(c-b))^t\big)^s \\ &\equiv \pm(-16)(-4)^t\big((4)(-16)^t\big)^s \not\equiv 0 \pmod p, \end{aligned}$$

since $p > 2$. Therefore, we have $\mathrm{rank}(\mathbf{R}\mathbf{R}^T) = |S| \cdot |T|$, and the lemma is proven. $\square$

4. PROOF OF THE MAIN THEOREM

In this section, we prove Theorem 6. As already mentioned in Section 2.2, we will use $\mathbf{M}_1^n$ and $\mathbf{M}_2^n$ to prove the two cases, respectively. The idea behind the proof is similar to the previous one. However, the sub-matrix $\mathbf{R}$ we pick this time is a square matrix with $n^2 - n$ rows. By showing that the rank of $\mathbf{R}\mathbf{R}^T$ is almost full, the theorem follows.

PROOF OF THEOREM 6. Let $v = 1$ in the first case and $v = 2$ in the second case. Note that in both cases, we have $n \equiv -v \pmod p$.

Let $S = \{(i,j) : 1 \le i \neq j \le n\}$, then we use $\mathbf{R}_v$ to denote the following sub-matrix of $\mathbf{H}(\mathbf{M}_v^n)$: Row (or column) (ij)

of $\mathbf{H}(\mathbf{M}_v)$ is selected if and only if $(i,j) \in S$. Thus, $\mathbf{R}_v$ is an $(n^2-n) \times (n^2-n)$ matrix. Again, we write $\mathbf{R}_v$ as

$$\mathbf{R}_v = \begin{pmatrix} \mathbf{H}_{12} \\ \mathbf{H}_{13} \\ \vdots \\ \mathbf{H}_{1n} \\ \mathbf{H}_{21} \\ \mathbf{H}_{23} \\ \vdots \\ \mathbf{H}_{n(n-1)} \end{pmatrix},$$

where $\mathbf{H}_{ij}$ is the (n^2-n)-dimensional vector truncated from the $(ij)^{th}$ row of the original matrix $\mathbf{H}(\mathbf{M}_v^n)$.

Again use Lemma 2 we have the following cases (under the assumption that $n \equiv -v \pmod p$): For $(i,j) \in S$,

1. $\mathbf{H}_{ij} \cdot \mathbf{H}_{ij} = (v+n-2)^2 + 2(n-2) \equiv -2v \pmod p$. We denote $-2v$ by a.
2. $\mathbf{H}_{ij} \cdot \mathbf{H}_{ji} = 0$.
3. when $1 \le k \le n$ and $k \ne i,j$, $\mathbf{H}_{ij} \cdot \mathbf{H}_{ik} = \mathbf{H}_{ij} \cdot \mathbf{H}_{kj} = 2(v+n-2)+(n-3) \equiv -(v+7) \pmod p$. We denote $-(v+7)$ by b.
4. when $1 \le k \le n$ and $k \ne i,j$, $\mathbf{H}_{ij} \cdot \mathbf{H}_{ki} = \mathbf{H}_{ij} \cdot \mathbf{H}_{jk} = 1$.
5. when $1 \le k \ne l \le n$ and $\{k,l\} \cap \{i,j\} = \emptyset$, $\mathbf{H}_{ij} \cdot \mathbf{H}_{kl} = 2$.

As a result, $\mathbf{R}_v\mathbf{R}_v^T$ is an $n \times n$-block matrix and each block is an $(n-1) \times (n-1)$ matrix. An example, when $n = 6$, is shown in Fig.1.

In Fig.1, notice that the $(1,2)^{th}$ block can be transformed into the $(1,6)^{th}$ block with the following operations: Move the 1^{st} row to the 5^{th} row and then move the $2^{nd} - 5^{th}$ rows up by one row. One can also transform the $(1,6)^{th}$ block into the $(5,6)^{th}$ block by moving the 1^{st} column to the 5^{th} column and moving the $2^{nd} - 5^{th}$ columns one column left. Let $\mathbf{A}$ and $\mathbf{B}$ be the following $(n-1) \times (n-1)$ matrices,

$$\mathbf{A} = \begin{pmatrix} a & b & b & b & \cdots & b \\ b & a & b & b & \cdots & b \\ b & b & a & b & \cdots & b \\ b & b & b & a & \cdots & b \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ b & b & b & b & \cdots & a \end{pmatrix}, \mathbf{B} = \begin{pmatrix} 0 & 1 & 1 & 1 & \cdots & 1 \\ 1 & b & 2 & 2 & \cdots & 2 \\ 1 & 2 & b & 2 & \cdots & 2 \\ 1 & 2 & 2 & b & \cdots & 2 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 2 & 2 & 2 & \cdots & b \end{pmatrix}$$

then we formally state the property observed above in the following lemma.

LEMMA 5. *The $(1,2)^{th}$ block of matrix $\mathbf{R}_v\mathbf{R}_v^T$ is $\mathbf{B}$. For any $i : 1 \le i \le n-1$, let $\mathbf{C}_i$ denote the following $(n-1) \times (n-1)$ matrix:*

$$\mathbf{C}_i = \begin{pmatrix} \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}_{i \times i} & \\ & \mathbf{I}_{n-1-i} \end{pmatrix}.$$

Then for all i,j such that $1 \le i < j \le n$, the $(i,j)^{th}$ block of matrix $\mathbf{R}_v\mathbf{R}_v^T$ is $\mathbf{C}_{j-1}^T\mathbf{B}\mathbf{C}_i$.

PROOF. To prove the lemma it suffices to show that, for all $1 \le i < j < n$, the $(i,j+1)^{th}$ block of $\mathbf{R}_v\mathbf{R}_v^T$ can be obtained from its $(i,j)^{th}$ block by exchanging the $(j-1)^{th}$ and j^{th} rows; and for all $1 \le i < j-1 < n$, the $(i+1,j)^{th}$ block of $\mathbf{R}_v\mathbf{R}_v^T$ can be obtained from its $(i,j)^{th}$ block by exchanging the i^{th} and $(i+1)^{th}$ columns. We only prove the first statement here. Assume i and j satisfy $1 \le i < j < n$. We define the following mappings:

$$\gamma(l) = \begin{cases} l & l \ne j, j+1; \\ j+1 & l = j; \\ j & l = j+1, \end{cases} \quad \text{and} \quad \sigma_r(l) = \begin{cases} l & l \le r-1; \\ l+1 & l \ge r, \end{cases}$$

for all $r \in \mathbb{Z}$. One can easily check that for any $l \in \mathbb{Z}$, we have $\gamma(\sigma_j(l)) = \sigma_{j+1}(l)$.

First, our analysis of $\mathbf{H}_{ij} \cdot \mathbf{H}_{kl}$ implies that

$$\mathbf{H}_{ij} \cdot \mathbf{H}_{kl} = \mathbf{H}_{\gamma(i)\gamma(j)} \cdot \mathbf{H}_{\gamma(k)\gamma(l)}.$$

This is because the value of $\mathbf{H}_{ij} \cdot \mathbf{H}_{kl}$ only depends on the equality relations between indices i,j and k,l (e.g., whether i is equal to k). As a result, exchanging j and $j+1$ does not change the inner product.

Second, for all $k,k' : 1 \le k,k' \le n-1$, we observe that the $(k,k')^{th}$ entry of the $(i,j)^{th}$ block of $\mathbf{R}_v\mathbf{R}_v^T$ is $\mathbf{H}_{i,\sigma_i(k)} \cdot \mathbf{H}_{j,\sigma_j(k')}$, while the $(k,k')^{th}$ entry of its $(i,j+1)^{th}$ block is $\mathbf{H}_{i,\sigma_i(k)} \cdot \mathbf{H}_{j+1,\sigma_{j+1}(k')}$. To compare the two blocks, we need to consider the following cases about k:

1. $k < j-1$. Then $\sigma_i(k) \le k+1 < j$, and thus, $\gamma(\sigma_i(k)) = \sigma_i(k)$. As a result,

$$\begin{aligned} \mathbf{H}_{i,\sigma_i(k)} \cdot \mathbf{H}_{j,\sigma_j(k')} &= \mathbf{H}_{\gamma(i),\gamma(\sigma_i(k))} \cdot \mathbf{H}_{\gamma(j),\gamma(\sigma_j(k'))} \\ &= \mathbf{H}_{i,\sigma_i(k)} \cdot \mathbf{H}_{j+1,\sigma_{j+1}(k')}. \end{aligned}$$

2. $k > j$. Similarly, one can show that

$$\mathbf{H}_{i,\sigma_i(k)} \cdot \mathbf{H}_{j,\sigma_j(k')} = \mathbf{H}_{i,\sigma_i(k)} \cdot \mathbf{H}_{j+1,\sigma_{j+1}(k')}.$$

3. $k = j-1$, then $\gamma(\sigma_i(k)) = j+1 = \sigma_i(j)$. So,

$$\begin{aligned} \mathbf{H}_{i,\sigma_i(k)} \cdot \mathbf{H}_{j,\sigma_j(k')} &= \mathbf{H}_{\gamma(i),\gamma(\sigma_i(k))} \cdot \mathbf{H}_{\gamma(j),\gamma(\sigma_j(k'))} \\ &= \mathbf{H}_{i,\sigma_i(j)} \cdot \mathbf{H}_{j+1,\sigma_{j+1}(k')}. \end{aligned}$$

4. $k = j$, then $\gamma(\sigma_i(k)) = j = \sigma_i(j-1)$. Similarly,

$$\begin{aligned} \mathbf{H}_{i,\sigma_i(k)} \cdot \mathbf{H}_{j,\sigma_j(k')} &= \mathbf{H}_{\gamma(i),\gamma(\sigma_i(k))} \cdot \mathbf{H}_{\gamma(j),\gamma(\sigma_j(k'))} \\ &= \mathbf{H}_{i,\sigma_i(j-1)} \cdot \mathbf{H}_{j+1,\sigma_{j+1}(k')}. \end{aligned}$$

As a result, the lemma is proven. □

Now we know $\mathbf{R}_v\mathbf{R}_v^T$ has the following form (here we let $*$ denote the blocks we don't care, although we know exactly what they are, since $\mathbf{R}_v\mathbf{R}_v^T$ is symmetric):

$$\begin{pmatrix} \mathbf{A} & \mathbf{C}_1^T\mathbf{B}\mathbf{C}_1 & \mathbf{C}_2^T\mathbf{B}\mathbf{C}_1 & \cdots & \mathbf{C}_{n-2}^T\mathbf{B}\mathbf{C}_1 & \mathbf{C}_{n-1}^T\mathbf{B}\mathbf{C}_1 \\ * & \mathbf{A} & \mathbf{C}_2^T\mathbf{B}\mathbf{C}_2 & \cdots & \mathbf{C}_{n-2}^T\mathbf{B}\mathbf{C}_2 & \mathbf{C}_{n-1}^T\mathbf{B}\mathbf{C}_2 \\ * & * & \mathbf{A} & \cdots & \mathbf{C}_{n-2}^T\mathbf{B}\mathbf{C}_3 & \mathbf{C}_{n-1}^T\mathbf{B}\mathbf{C}_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ * & * & * & \cdots & \mathbf{A} & \mathbf{C}_{n-1}^T\mathbf{B}\mathbf{C}_{n-1} \\ * & * & * & \cdots & * & \mathbf{A} \end{pmatrix}.$$

Again, we will apply matrix operations to $\mathbf{R}_v\mathbf{R}_v^T$. But before that, we need to prove the following key property about the block matrices in $\mathbf{R}_v\mathbf{R}_v^T$: The difference between the $(i+1,j+1)^{th}$ and $(i+1,j)^{th}$ blocks is exactly the same as the difference between the $(i,j+1)^{th}$ and $(i,j)^{th}$ blocks.

	12	13	14	15	16	21	23	24	25	26	31	32	34	35	36	41	42	43	45	46	51	52	53	54	56	61	62	63	64	65
12	a	b	b	b	b	0	1	1	1	1	1	b	2	2	2	1	b	2	2	2	1	b	2	2	2	1	b	2	2	2
13	b	a	b	b	b	1	b	2	2	2	0	1	1	1	1	1	2	b	2	2	1	2	b	2	2	1	2	b	2	2
14	b	b	a	b	b	1	2	b	2	2	1	2	b	2	2	0	1	1	1	1	1	2	2	b	2	1	2	2	b	2
15	b	b	b	a	b	1	2	2	b	2	1	2	2	b	2	1	2	2	b	2	0	1	1	1	1	1	2	2	2	b
16	b	b	b	b	a	1	2	2	2	b	1	2	2	2	b	1	2	2	2	b	1	2	2	2	b	0	1	1	1	1
21	0	1	1	1	1	a	b	b	b	b	b	1	2	2	2	b	1	2	2	2	b	1	2	2	2	b	1	2	2	2
23	1	b	2	2	2	b	a	b	b	b	1	0	1	1	1	2	1	b	2	2	2	1	b	2	2	2	1	b	2	2
24	1	2	b	2	2	b	b	a	b	b	2	1	b	2	2	1	0	1	1	1	2	1	2	b	2	2	1	2	b	2
25	1	2	2	b	2	b	b	b	a	b	2	1	2	b	2	2	1	2	b	2	1	0	1	1	1	2	1	2	2	b
26	1	2	2	2	b	b	b	b	b	a	2	1	2	2	b	2	1	2	2	b	2	1	2	2	b	1	0	1	1	1
31	1	0	1	1	1	b	1	2	2	2	a	b	b	b	b	b	2	1	2	2	b	2	1	2	2	b	2	1	2	2
32	b	1	2	2	2	1	0	1	1	1	b	a	b	b	b	2	b	1	2	2	2	b	1	2	2	2	b	1	2	2
34	2	1	b	2	2	2	1	b	2	2	b	b	a	b	b	1	1	0	1	1	2	2	1	b	2	2	2	1	b	2
35	2	1	2	b	2	2	1	2	b	2	b	b	b	a	b	2	2	1	b	2	1	1	0	1	1	2	2	1	2	b
36	2	1	2	2	b	2	1	2	2	b	b	b	b	b	a	2	2	1	2	b	2	2	1	2	b	1	1	0	1	1
41	1	1	0	1	1	b	2	1	2	2	b	2	1	2	2	a	b	b	b	b	b	2	2	1	2	b	2	2	1	2
42	b	2	1	2	2	1	1	0	1	1	2	b	1	2	2	b	a	b	b	b	2	b	2	1	2	2	b	2	1	2
43	2	b	1	2	2	2	b	1	2	2	1	1	0	1	1	b	b	a	b	b	2	2	b	1	2	2	2	b	1	2
45	2	2	1	b	2	2	2	1	b	2	2	2	1	b	2	b	b	b	a	b	1	1	1	0	1	2	2	2	1	b
46	2	2	1	2	b	2	2	1	2	b	2	2	1	2	b	b	b	b	b	a	2	2	2	1	b	1	1	1	0	1
51	1	1	1	0	1	b	2	2	1	2	b	2	2	1	2	b	2	2	1	2	a	b	b	b	b	b	2	2	2	1
52	b	2	2	1	2	1	1	1	0	1	2	b	2	1	2	2	b	2	1	2	b	a	b	b	b	2	b	2	2	1
53	2	b	2	1	2	2	b	2	1	2	1	1	1	0	1	2	2	b	1	2	b	b	a	b	b	2	2	b	2	1
54	2	2	b	1	2	2	2	b	1	2	2	2	b	1	2	1	1	1	0	1	b	b	b	a	b	2	2	2	b	1
56	2	2	2	1	b	2	2	2	1	b	2	2	2	1	b	2	2	2	1	b	b	b	b	b	a	1	1	1	1	0
61	1	1	1	1	0	b	2	2	2	1	b	2	2	2	1	b	2	2	2	1	b	2	2	2	1	a	b	b	b	b
62	b	2	2	2	1	1	1	1	1	0	2	b	2	2	1	2	b	2	2	1	2	b	2	2	1	b	a	b	b	b
63	2	b	2	2	1	2	b	2	2	1	1	1	1	1	0	2	2	b	2	1	2	2	b	2	1	b	b	a	b	b
64	2	2	b	2	1	2	2	b	2	1	2	2	b	2	1	1	1	1	1	0	2	2	2	b	1	b	b	b	a	b
65	2	2	2	b	1	2	2	2	b	1	2	2	2	b	1	2	2	2	b	1	1	1	1	1	0	b	b	b	b	a

Figure 1: An example of matrix $\mathbf{R}_v\mathbf{R}_v^T$ when $n = 6$

LEMMA 6. *For all $1 \le i < j \le n$ such that $i+1 < j$ and $j+1 \le n$, we have*

$$(\mathbf{C}_j^T - \mathbf{C}_{j-1}^T)\mathbf{B}\mathbf{C}_{i+1} = (\mathbf{C}_j^T - \mathbf{C}_{j-1}^T)\mathbf{B}\mathbf{C}_i.$$

PROOF. For $1 \le k \le n-1$, we use $\mathbf{B}_k$ to denote the k^{th} row vector of $\mathbf{B}$. We also use $\mathbf{B}'$ to denote $(\mathbf{C}_j^T - \mathbf{C}_{j-1}^T)\mathbf{B}$, and $\mathbf{B}'_k$ to denote the k^{th} row of $\mathbf{B}'$. It is not hard to check that $\mathbf{B}'_{j-1} = \mathbf{B}_j - \mathbf{B}_1$, $\mathbf{B}'_j = \mathbf{B}_1 - \mathbf{B}_j$, and $\mathbf{B}'_k = \mathbf{0}$ for all $k \ne j-1, j$.

On the other hand, all the entries of $\mathbf{B}_j - \mathbf{B}_1$ are equal to 1 except the j^{th} entry which is equal to $b-1$. As we assumed that $i+1 < j$, we have $\mathbf{B}'\mathbf{C}_{i+1} = \mathbf{B}'\mathbf{C}_i = \mathbf{B}'$, and the lemma is proven. □

We apply the following operations to $\mathbf{R}_v\mathbf{R}_v^T$: subtract the second last column from the last column of $\mathbf{R}_v\mathbf{R}_v^T$, then subtract the third last column from the second last column ... till subtract the first column from the second column. Let $\mathbf{P}$ denote the upper right sub-matrix, after the operations, of $\mathbf{R}_v\mathbf{R}_v^T$ containing $(n-1) \times (n-1)$ blocks (see Fig.2).

Next, we transform $\mathbf{P}$ as follows: Subtract the second last row from the last row, then subtract the third last row from the second last row ... till subtract the first row from the second row. We only need to focus on the lower right part of $\mathbf{P}$ containing $(n-2) \times (n-2)$ blocks, which we denote by $\mathbf{P}^*$. It directly follows from Lemma 6 that $\mathbf{P}^*$ is a lower triangular block matrix, and the block matrices along the diagonal are:

$$\big(\mathbf{C}_i^T(\mathbf{B}-\mathbf{A})\mathbf{C}_i - (\mathbf{C}_i^T - \mathbf{C}_{i-1}^T)\mathbf{B}\mathbf{C}_{i-1}\big)\,,\ i = 2, ..., n-1.$$

On the other hand, as implied by the proof of Lemma 6, the rank of $(\mathbf{C}_i^T - \mathbf{C}_{i-1}^T)\mathbf{B}\mathbf{C}_{i-1}$ is exactly 1, so

$$\begin{aligned}
&\text{rank}(\mathbf{R}_v\mathbf{R}_v^T) \ge \text{rank}(\mathbf{P}^*)\\
&\ge \sum_{i=2}^{n-1} \text{rank}\big(\mathbf{C}_i^T(\mathbf{B}-\mathbf{A})\mathbf{C}_i - (\mathbf{C}_i^T - \mathbf{C}_{i-1}^T)\mathbf{B}\mathbf{C}_{i-1}\big)\\
&\ge (n-2)\big(\text{rank}(\mathbf{B}-\mathbf{A}) - 1\big).
\end{aligned}$$

Finally, by Lemma 3, the determinant of the lower right $(n-2)\times(n-2)$ sub-matrix of $\mathbf{B}-\mathbf{A}$ is

$$\begin{aligned}
&\big((b-a) + (n-3)(2-b)\big)\big((b-a) - (2-b)\big)^{n-3}\\
&\equiv \begin{cases} (-46)(-16)^{n-3} \pmod p & \text{when } v = 1;\\ (-60)(-16)^{n-3} \pmod p & \text{when } v = 2.\end{cases}
\end{aligned}$$

As a result, we have $\text{rank}(\mathbf{H}(\mathbf{M}_1^n)) \ge \text{rank}(\mathbf{R}_1\mathbf{R}_1^T) \ge (n-2)(n-3)$ when $p \ne 23$; and $\text{rank}(\mathbf{H}(\mathbf{M}_2^n)) \ge \text{rank}(\mathbf{R}_2\mathbf{R}_2^T) \ge (n-2)(n-3)$ when $p \ne 3, 5$.

$$\mathbf{P}=\begin{pmatrix}\mathbf{C}_1^T(\mathbf{B}-\mathbf{A})\mathbf{C}_1 & (\mathbf{C}_2^T-\mathbf{C}_1^T)\mathbf{B}\mathbf{C}_1 & (\mathbf{C}_3^T-\mathbf{C}_2^T)\mathbf{B}\mathbf{C}_1 & \cdots & (\mathbf{C}_{n-1}^T-\mathbf{C}_{n-2}^T)\mathbf{B}\mathbf{C}_1\\ * & \mathbf{C}_2^T(\mathbf{B}-\mathbf{A})\mathbf{C}_2 & (\mathbf{C}_3^T-\mathbf{C}_2^T)\mathbf{B}\mathbf{C}_2 & \cdots & (\mathbf{C}_{n-1}^T-\mathbf{C}_{n-2}^T)\mathbf{B}\mathbf{C}_2\\ * & * & \mathbf{C}_3^T(\mathbf{B}-\mathbf{A})\mathbf{C}_3 & \cdots & (\mathbf{C}_{n-1}^T-\mathbf{C}_{n-2}^T)\mathbf{B}\mathbf{C}_3\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ * & * & * & \cdots & \mathbf{C}_{n-1}^T(\mathbf{B}-\mathbf{A})\mathbf{C}_{n-1}\end{pmatrix}$$

Figure 2: Matrix P transformed from $\mathbf{R}_v\mathbf{R}_v^T$

A natural question is what makes this sequence of matrices works for the proof. We can only offer our take on this. We believe that probably most matrices $\mathbf{X}$, where $\text{per}(\mathbf{X})=0$, will work, i.e., its Hessian will have a quadratic rank. The problem is rather how to prove this. Over characteristic 0, Mignon and Ressayre gave a construction which is essentially the all 1 matrix (except the $(1,1)$ entry to make $\text{per}(\mathbf{X})=0$). This makes most second derivatives in the Hessian of the permanent a constant (but involving a large factorial). The key to our matrix is to choose it sufficiently uniform so that we can still prove its rank analytically, but not so uniform so as to involve large factorials.

Acknowledgement

We wish to thank Les Valiant for many interesting discussions on the topic. This work would not have been possible for us without the discussions and comments from Les.

Jin-Yi Cai's work was supported by NSF Grant NSF CCR-0511679. Xi Chen and Dong Li were both supported by NSF Grant DMS-0635607.

5. REFERENCES

[1] M. Agrawal. Determinant versus permanent. *manuscript*.

[2] M. Agrawal. Proving lower bounds via pesudo-random generators. In *Proceedings of the FST and TCS*, pages 96–105, 2005.

[3] M. Agrawal, N. Kayal, and N. Saxena. Primes is in P. *Annals of Mathematics*, 160(2):781–793, 2004.

[4] P. Bürgisser. *Completeness and Reduction in Algebraic Complexity Theory*. Springer-Verlag, 2000.

[5] P. Bürgisser, M. Clausen, and M. Shokrollahi. *Algebraic Complexity Theory*. Grundlehren der mathematischen Wissenschaften, Vol 315. Springer, 1997.

[6] J. Cai. A note on the determinant and permanent problem. *Inf. Comput.*, 84(1):119–127, 1990.

[7] C. Damm. DET = $L^{\#L}$. *Technical Report Informatik-preprint 8*, 1991. Fachbereich Informatik der Humboldt Universität zu Berlin.

[8] D. Grigoriev and A. Razborov. Exponential lower bounds for depth 3 arithmetic circuits in algebras of functions over finite fields. *Appl. Algebra Eng. Commun. Comput.*, 10(6):465–487, 2000.

[9] M. Jerrum and M. Snir. Some exact complexity results for straight-line computations over semirings. *J. ACM*, 29(3):874–897, 1982.

[10] R. Meshulam. Two extremal matrix problems. *Linear Alg. and its Applications*, 114/115:261–271, 1989.

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

[12] H. Minc. *Permanents*. Encyclopedia of Mathematics and its Applications, vol 6. Addison-Wesley, 1978.

[13] K. Mulmulay and M. Sohoni. Geometric complexity theory, P vs. NP, and explicit obstructions. *SIAM Journal on Computing*, 31(2):496–526, 2002.

[14] G. Pólya. Aufgabe 424. *Arch. Math. Phys.*, 20:271, 1913.

[15] R. Raz. Multi-linear formulas for permanent and determinant are of super-polynomial size. *J. ACM*, to appear.

[16] R. Raz, A. Shpilka, and A. Yehudayoff. A lower bound for the size of syntactically multilinear arithmetic circuits. In *Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science*, pages 438–448, 2007.

[17] A. Shpilka and A. Wigderson. Depth-3 arithmetic circuits over fields of characteristic zero. *Computational Complexity*, 10(1):1–27, 2001.

[18] G. Szegö. Zu aufgabe 424. *Arch. Math. Phys.*, 21:291–292, 1913.

[19] S. Toda. Counting problems computationally equivalent to the determinant. *manuscript*, 1991.

[20] L. Valiant. Private communication.

[21] L. Valiant. The complexity of computing the permanent. *Theor. Comput. Sci.*, 8(2):189–201, 1979.

[22] L. Valiant. The complexity of enumeration and reliability problems. *SIAM J. Comput.*, 8(3):410–421, 1979.

[23] L. Valiant, S. Skyum, S. Berkowitz, and C. Rackoff. Fast parallel computation of polynomials using few processors. *SIAM Journal on Computing*, 12:641–644, 1983.

[24] V. Vinay. Counting auxiliary pushdown automata and semi-unbounded arithmetic circuits. In *Proceedings of the Structure in Complexity Theory Conference*, pages 270–284, 1991.

[25] J. von zur Gathen. Permanent and determinant. In *Proceedings of the 27th IEEE Foundations of Computer Science*, pages 398–401, 1986.

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