Yale University
Department of Computer Science

On Projections of Determinant to Permanent

Jin-yi Cai

YALEU/DCS/TR-606
April 1988

Research spported by NSF grant CCR-8709818.

On Projections of Determinant to Permanent

Jin-yi Cai[*]
Department of Computer Science
Yale University
New Haven, CT 06520

Abstract

In Valiant's theory of arithmetic complexity, the following question occupies a central position: Given an integer n, what is the minimal m such that the permanent of an $n \times n$ matrix is the projection of the determinant of an $m \times m$ matrix.

The lower bound of $m > n$ is easy to see. The only nontrivial lower bound known previously is due to von zur Gathen: $m \geq \lfloor \sqrt{8/7} \cdot n \rfloor$. In this paper we give two proofs of the following lower bound $m \geq \lfloor \sqrt{2} \cdot n \rfloor$. The first proof is purely combinatorial, and the second one is algebro-geometric. As a consequence of the second proof we obtain a generalization of a classic theorem due to Marcus and Minc.

1 Introduction

It is notorious that in computational complexity theory, lower bounds are hard to prove. We have very few hard-core separation results of complexity classes other than the classic space and time hierarchy theorems [HLS] and $AC^0 \neq NC^1$ [FFS]. In the vast terrain between NC^1 and $P^{\#\mathrm{P}}$, there is convincing evidence but no hard proof that any of the complexity classes are distinct.

It is into this atmosphere, came the refreshing algebraic formulation by Valiant [V1, V2, V3] of analogues of many famous Boolean conjectures such as $P \neq NP$.

In particular, the ***determinant and permanent problem*** embodies the central question of separation of complexity classes in Valiant's theory. It was hoped that these algebraic formulations might help to place the hard complexity problems in a more structured setting

[*] Research supported by NSF grant CCR-8709818.

with powerful algebraic tools available to tackle them.

Let F be any field and $X = (x_{ij})$ be an $n \times n$ matrix, where $x_{ij}, 1 \leq i, j \leq n$, are algebraically independent indeterminates over the field F.

Definition 1.1

$$\begin{aligned} detX &= \sum_{\sigma}(-1)^{sign(\sigma)} x_{1\sigma 1} x_{2\sigma 2} \ldots x_{n\sigma n}, & (1) \\ perX &= \sum_{\sigma} x_{1\sigma 1} x_{2\sigma 2} \ldots x_{n\sigma n} & (2) \end{aligned}$$

where σ runs through all permutations on n letters, and $sign(\sigma)$ denotes the sign of the permutation σ.

Despite the similarity in their definition, the determinant and the permanent are exceedingly different in their apparent computational complexity. For the determinant Gaussian elimination affords a fast algorithm, while no sub-exponential time algorithm is known (nor is it expected to exist) to compute the permanent. Moreover, Valiant proved that the permanent function is #P-complete for any field F of characteristic not equal to 2.

Definition 1.2 *A polynomial $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ is called the projection of a polynomial $g(y_1, \ldots, y_m)$ if there exists a mapping $\phi : \{y_j | 1 \leq j \leq m\} \longrightarrow \{x_i | 1 \leq i \leq n\} \cup F$, such that $f(x_1, \ldots, x_n) = g(\phi(y_1), \ldots, \phi(y_m))$.* [1]

Projection as a reducibility among low level complexity classes is discussed extensively in [V2][V3]. Valiant proved that determinant is "universal" with respect to formula size under projection, i.e., every function, given by a formula, is the projection of a determinant of size polynomial in the size of the given formula. Let $p(n)$ be the minimal m such that an $n \times n$ permanent is the projection of an $m \times m$ determinant. The *determinant and permanent problem* is to determine $p(n)$. Valiant's anologue of $P \neq NP$ will follow if one can show a super exponential-polylog lower bound for $p(n)$. A super polynomial lower bound will separate NC^1 from $P^{\#P}$. On the other hand, a polynomial upper bound on $p(n)$ will collapse (non-uniform)NC^2 and $P^{\#P}$.

Valiant proved an exponential upper bound for $p(n)$. The only trivial lower bound is $p(n) > n$. In pursuit of non-trivial lower bound, von zur Gathen [G] has made a first step. He proved

Theorem 1.3 $p(n) \geq \lfloor \sqrt{8/7} \cdot n \rfloor \approx 1.069n$.

[1] We view the equality as that of the ring $F[x_1, \ldots, x_n]$. If the field F is infinite, then this is the same as functional equality.

Furthermore he initiated an algebraic geometry approach that potentially may yield much more. What relationship exists between the twin-looking determinant and permanent functions has been pursued by many people from Pólya [P] on. Aside from the von zur Gathen result cited above, there is a classic result due to Marcus and Minc [MM].

Theorem 1.4 *If $ch.F = 0$, then there are no linear forms f_{kl} in the indeterminates x_{ij} $(1 \leq i, j, k, l \leq n)$ such that $per(x_{ij}) = det(f_{kl})$.*

In this paper, we prove the following generalization of the Marcus-Minc Theorem.

Theorem 1.5 *For any infinite field of characteristic not equal to 2, there are no affine linear functions [2] f_{kl} in the indeterminates x_{ij} $(1 \leq i, j \leq n$ and $1 \leq k, l \leq m)$ such that $per(x_{ij}) = det(f_{kl})$, provided $m < \lfloor \sqrt{2}n \rfloor$.*

As an immediate corollary we have the lower bound on projections of determinant to permanent.

Corollary 1.6

$$p(n) \geq \lfloor \sqrt{2}n \rfloor.$$

In the next section we give a purely combinatorial proof of a result which is asymptotically as strong as the one stated in the corollary. Readers may find it interesting as it reveals certain properties of the problem not exposed in the later sections with the algebraic geometry approach.

Starting from section 3 the treatment takes an algebraic flavor. We use argument from algebraic geometry to establish the claimed lower bound.

A general reference on permanents can be found in [M].

2 A Combinatorial Proof

Suppose $X = (x_{ij})$ is an $n \times n$ matrix, where $x_{ij}, 1 \leq i, j \leq n$, are indeterminates, over any field F of characteristic not equal to 2. We denote by X_i (X^j) the ith (jth) row (column) of X. In this section we prove the following

Theorem 2.1

$$p(n) > \sqrt{2}n - O(n^{3/4})$$

[2] Linear forms are homogeneous linear polynomials and affine linear functions are linear polynomials not neccessarily homogeneous.

Proof Let $m \leq \sqrt{2}n - C \cdot n^{3/4}$ for some constant C, and let Y be any $m \times m$ matrix whose entries are elements from F or indeterminates x_{ij}. Suppose $perX = detY$.

Let n_0 be the number of entries in Y that are from F, n_1 be the number of indeterminates x_{ij} that appear exactly once in Y, and n_2 be the number of x_{ij} that appear at least twice in Y.

Clearly, every x_{ij} must appear at least once in Y, since as a polynomial in this x_{ij} over the ring $R = F[X - \{x_{ij}\}]$ the permanent $perX$ has degree 1, and hence not in R.

It follows that

$$\begin{aligned} n_0, n_1, n_2 &\geq 0, & (3)\\ n_1 + n_2 &= n^2, & (4)\\ n_0 + n_1 + 2n_2 &\leq m^2 < 2n^2 - 2Cn^{7/4}. & (5) \end{aligned}$$

Thus $n_0 + n_2 \leq m^2 - n^2$ and $n_1 \geq n_1 - n_0 \geq 2n^2 - m^2 \geq 2Cn^{7/4}$.

The n_1 indeterminates x_{ij} that appear exactly once in Y will be called *singles*. Our proof will focus on these singles. We first prove a simple lemma.

Lemma 2.2 *Let V be a row or a column of Y and $S(V)$ be the set of all singles on V. Then either there exists an $i, 1 \leq i \leq n$, such that $S(V) \subseteq X_i$ or there exists a $j, 1 \leq j \leq n$, such that $S(V) \subseteq X^j$.*

Proof Suppose x_{ij} and x_{kl} are 2 singles on a same row of Y. If $i \neq k$ and $j \neq l$, then the coefficient of the term $x_{ij}x_{kl}$ of $perX$ (as a polynomial over the ring $R = F[X - \{x_{ij}, x_{kl}\}]$) is non zero. However, since they occur as singles in Y on a same row, the coefficient of $x_{ij}x_{kl}$ in $detY$ is zero. This contradiction shows that either $i = k$ or $j = l$.

Now suppose x_{st} is another single on the same row of Y. Then we claim either $i = k = s$ or $j = l = t$. Othewise, say $i = k$ and $l = t$, then $j \neq l$ and $k \neq s$, thus $j \neq t$ and $i \neq s$, a contradiction. Therefore it follows by induction that all the singles on a single row of Y must belong to a single row or a single column of X.

The other case is completely symmetric. **QED**

For any row or column V of Y with at least 2 singles, we may associate a unique row X_i or a unique column X^j (but not both) such that $S(V) \subseteq X_i$ or $S(V) \subseteq X^j$. We say that the row X_i or column X^j *claims* V.

Certain singles may be *isolated* in the sense that on the row and the column of Y in which the single appears there are no other singles. We wish to exclude these singles, as they do not help in the proof. Fortunately the number of these isolated singles is no more than m, and thus the number of *non-isolated* singles is at least $1.5Cn^{7/4}$.

We now define the notion of a *single's club*.

For a non-isolated single x, i.e., there is at least one other single either on the the row V_x of Y where x appears, or on the column V^x of Y where x appears, we associate x with a unique row or a unique column of X as follows: In the first case, the row V_x is claimed by a unique row or column V of X ($S(V_x) \subseteq V$), we associate x with V; if the first case does not apply, then V^x is claimed by a unique row or a unique column V' of X ($S(V_x) \subseteq V'$), and we associate x with V'. We emphasize that in either cases, x is associated either to a row X_i or to a column X^j in X, but not both; furthermore, x belongs to the associated row or column in X.

Define the *single's club* of X_i to be

$$M_i = \{x \in X_i | x \text{ is a single associated with } X_i\}.$$

The *single's club* of X_j is defined analogously. Clearly

$$M_i \subseteq \bigcup_{V \text{ claimed by } X_i} V, \tag{6}$$

and similarly for M^j.

Furthermore $\Sigma_{i=1}^{n}|M_i| + \Sigma_{j=1}^{n}|M^j|$ is exactly the number of non-isolated singles, which is at least $1.5Cn^{7/4}$.

We claim that "quite many" M_i, M^j's are relatively "big" in size. More specifically,

Proposition 1:

$$|\{X_i, X^j : |M_i| \geq C/2 \cdot n^{3/4}, |M^j| \geq C/2 \cdot n^{3/4}\}| \geq C/2 \cdot n^{3/4}. \tag{7}$$

Suppose otherwise. Since each $|M_i|, |M^j|$ is at most n,

$$\Sigma_i|M_i| + \Sigma_j|M^j| < C/2 \cdot n^{3/4} \cdot n + 2n \cdot C/2 \cdot n^{3/4} = 1.5Cn^{7/4}.$$

A contradiction.

We next show that "quite a few" rows and columns of X, whose single's clubs have been included above, claim "very few" rows and columns in Y.

Proposition 2:

$$\begin{aligned} |\{X_i, X^j \ &: \ |M_i| \geq C/2n^{3/4}, |M^j| \geq C/2n^{3/4}, \\ &X_i, X^j \text{ claim at most } n^{1/4} \text{ rows and columns each } \}| \geq 4\sqrt{n}. \end{aligned} \tag{8}$$

For the proof, suppose this is not the case. Then at least $C/2 \cdot n^{3/4} - 4\sqrt{n}$ many X_i, X^j's, whose singles's club having at least $C/2 \cdot n^{3/4}$ members, each claim more than $n^{1/4}$ rows and columns in Y. Hence the total number of rows and columns in Y claimed is more than

$$(C/2 \cdot n^{3/4} - 4\sqrt{n}) \cdot n^{1/4} = C/2 \cdot n - o(n) > 2m,$$

If $j = s$, then since they are all singles, $s \neq t$ and $j \neq t$, thus $v = i$ by Lemma 2.2. But then x_{is} cannot be a single. Hence $j \neq s$, and therefore by Lemma 2.2 again, $u = i$. Thus $v \neq i$ and $j = t$. But then x_{it} cannot be a single.

This completes the proof of Theorem 2.1.

We note the following combinatorial fact:

Theorem 2.3 *If A is an $n \times n$ 0-1 matrix with no 2×2 submatrix $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$, then the number of 1's in A is $O(n^{3/2})$.*

For its proof, we view the matrix A as a representation of a certain graph on n nodes as follows: An edge exists between node i and j *iff* on some row there are 1's at position i and j. Thus, the condition on the forbidden configuration implies that the graph is a subgraph of K_n which is an edge disjoint union of cliques; and the number of 1's in A is the sum of the number of nodes of these cliques. It follows that number of 1's in A is at most $O(n^{3/2})$.

Using the above result (with some care), one can establish the following theorem along the above proof of Theorem 2.1:

Theorem 2.4 *If $perX = detY$, where X is $n \times n$ and Y is $m \times m$, and assume there are $\Omega(n^2)$ singles in Y, then $m = \Omega(n^{3/2})$.*

3 An Algebraic Geometry Approach

In this section we prove:

Theorem 3.1 *For any infinite field of characteristic not equal to 2, there are no affine linear functions f_{kl} in the indeterminates x_{ij} ($1 \leq i,j \leq n$ and $1 \leq k,l \leq m$) such that $per(x_{ij}) = det(f_{kl})$, provided $m < \lfloor \sqrt{2}n \rfloor$.*

The proof consists of two steps. First a general condition in terms of intersection of algebraic varieties is established which implies $perX \neq detY$, where Y is any matrix with linear functions as entries. This condition was first discovered by von zur Gathen. Then we show that if $m < \lfloor \sqrt{2}n \rfloor$, the condition is satisfied.

3.1 Intersection of Algebraic Varieties

We assume some familiarity with basic notions from algebra and algebraic geometry [AM] [H]. Without loss of generality, we will assume our ground field F is algebraically closed. We will be concerned with permanental and determinantal varieties. Let X be an $n \times n$ matrix (x_{ij}).

Definition 3.2

$$\begin{aligned} P_n &= \{P \in F^{n^2} | perX = 0\}, & (11) \\ D_n &= \{P \in F^{n^2} | detX = 0\} \\ &= \{P \in F^{n^2} | rank\ of\ X \leq n-1\}. & (12) \end{aligned}$$

Definition 3.3

$$\begin{aligned} SP_n &= \{P \in P_n | \frac{\partial}{\partial x_{ij}} perX = 0, \forall i,j\}, & (13) \\ SD_n &= \{P \in D_n | \frac{\partial}{\partial x_{ij}} detX = 0, \forall i,j\} \\ &= \{P \in D_n | rank\ of\ X \leq n-2\}. & (14) \end{aligned}$$

Given an $n \times n$ matrix $X = (x_{ij})$, and an $m \times m$ matrix $Y = (f_{kl})$, where f_{kl} are affine linear functions, the following criterion is stated in [G] by von zur Gathen:

Theorem 3.4 *Let Π be the image of F^{n^2} under the affine linear map defined by f_{kl}, which is an affine subspace in F^{m^2}. If $\Pi \cap SD_m \neq \emptyset$, then $perX \neq detY$.*

We give a proof outline.

- P_n and D_n are algebraic varieties of $dimP_n = dimD_n = n^2 - 1$.

This is due to the fact that both permanent and determinant are irreducible polynomials (Gaussian Lemma).

- (Due to von zur Gathen) Assume $n \geq 3$. SP_n and SD_n are algebraic sets with dimensions $dimSP_n \leq n^2 - 5$ and $dimSD_n = n^2 - 4$, respectively. Furthermore, SD_n is an algebraic (irreducible) variety.

The exact dimension of SP_n is unknown. Intuitively, the dimension of SD_n can be proved by considering a *generic* instance of a matrix of rank deficient by 2, thus some two rows are linear combinations of the rest. The upper bound of $n^2 - 4$ on SP_n can be obtained easily. One improves the bound to $n^2 - 5$ by exhibiting a nontrivial polynomial that vanishes on SP_n.

- In an n dimensional affine space, if two algebraic varieties V_1 and V_2 intersect, then $dim(V_1 \cap V_2) \geq dimV_1 + dimV_2 - m$.
- If $perX = detY$, then the dimension of the affine space Π is n^2. This is equivalent to saying that the affine linear map defined by f_{kl} from F^{n^2} to F^{m^2} is of full rank.

To see this, suppose otherwise. Then there is an invertible linear transformation T from F^{n^2} to F^{n^2}, such that $per\ T(X) = det(g_{kl})$, where g_{kl} are some new affine linear functions on x_{ij} and, say, x_{11} never occurs in the g_{kl}'s. Now differentiate both sides with respect to x_{11}, and set the matrix on the left hand side to be

$$\begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 1 & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 1 & \dots & 1 \end{pmatrix}.$$

We may do so since T is invertible. Now the derivative is zero on the right hand side, this implies that the coefficient of x_{11} in the (1,1) position of TX is zero. Similarly one can show that all entries in TX have a zero coefficient for x_{11}. This contradicts T being invertible.

- Finally one realizes that if $perX = det(f_{kl})$, and $\Pi \cap SD_m \neq \emptyset$, then SP_n contains a subvariety isomorphic to $\Pi \cap SD_m$, which has dimension at least $n^2 + (m^2 - 4) - m^2 = n^2 - 4$. A contradiction.

This follows from the chain-rule of differentiation.

3.2 Rank Deficiency

We finish the proof of Theorem 3.1. The intuitive idea is that when the size of the "determinantal matrix" Y is not too large relative to the number of variables, then there should be enough freedom to assign the variables in X so that the matrix $Y = (f_{kl}(x_{ij}))$ is rank deficient by two.

From now on we will view X both as a matrix and as a column vector $\mathbf{x} = (x_k)_{k=1}^{n^2}$. Let $Y = (f_{ij}(\mathbf{x}))_{i,j=1}^{m}$, where $f_{ij}(\mathbf{x}) = \sum_{k=1}^{n^2} c_{ij}^k x_k - b_{ij}$, and $c_{ij}^k, b_{ij} \in F$. When convenient, we will also view Y as an m^2 dimensional vector $\mathbf{y}$. We assume $perX = detY$.

For any $\mathbf{x_0}$, $Y(\mathbf{x_0})$ determines a linear transformation from F^m to F^m. We wish to find an $\mathbf{x_0} \in F^{n^2}$ such that the rank of $Y(\mathbf{x_0})$ is no more than $m-2$. Equivalently, we can show that the kernel of $Y(\mathbf{x_0})$ has dimension at least 2.

More generally, pick some s rows of Y, $s \geq 2$, and the submatrix determines a linear transformation from F^m to F^s, for any point $\mathbf{x_0} \in F^{n^2}$. We wish to find some s rows and an $\mathbf{x_0}$ such that the kernel of the linear transformation has dimension at least $m - s + 2$. If so, by the rank-nullity theorem, we are done.

Define

$$C_i = \begin{pmatrix} c_{i1}^1 & c_{i1}^2 & \dots & c_{i1}^{n^2} \\ c_{i2}^1 & c_{i2}^2 & \dots & c_{i2}^{n^2} \\ \vdots & \vdots & \ddots & \vdots \\ c_{im}^1 & c_{im}^2 & \dots & c_{im}^{n^2} \end{pmatrix}, B_i = \begin{pmatrix} b_{i1} \\ b_{i2} \\ \vdots \\ b_{im} \end{pmatrix}, 1 \leq i \leq m,$$

and $C = \begin{pmatrix} C_1 \\ C_2 \\ \vdots \\ C_m \end{pmatrix}$, $B = \begin{pmatrix} B_1 \\ B_2 \\ \vdots \\ B_m \end{pmatrix}$. We have $\mathbf{y} = C \cdot \mathbf{x} - B$.

The above discussion on dimensions of kernel translates to the following:

- Find a point $\mathbf{x}_0 \in F^{n^2}$, s blocks $(s \geq 2)$ $C_{i_1}, C_{i_2}, \ldots, C_{i_s}$, and an $sr \times sm$ matrix $\mathcal{A} = diag\{A, A, \ldots, A\}$, where $r = m - s + 2$ and

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1m} \\ a_{21} & a_{22} & \ldots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{r1} & a_{r2} & \ldots & a_{rm} \end{pmatrix}$$

is an $r \times m$ matrix of rank r, such that

$$\mathcal{A} \cdot \begin{pmatrix} C_{i_1} \\ C_{i_2} \\ \vdots \\ C_{i_s} \end{pmatrix} \cdot \mathbf{x}_0 = \mathcal{A} \cdot \begin{pmatrix} B_{i_1} \\ B_{i_2} \\ \vdots \\ B_{i_s} \end{pmatrix}. \tag{15}$$

Among all block permutations $\tilde{C} = \begin{pmatrix} C_{i_1} \\ C_{i_2} \\ \vdots \\ C_{i_m} \end{pmatrix}$ of C, we choose one with a lexicographically maximum "rank sequence":

$$(\text{rank}(C_{i_1}), \text{rank} \begin{pmatrix} C_{i_1} \\ C_{i_2} \end{pmatrix}, \ldots, \text{rank}(\tilde{C})).$$

Let r_l be the difference of lth and $(l-1)$ st entries in this rank sequence (i.e., the increment in rank by the lth block in $\tilde{C}$). We proved in Section 3.1 that the matrix C is of full rank, thus $\sum_{l=1}^{m} r_l = n^2$. By the choice of our $\tilde{C}$, $r_1 \geq r_2 \geq \ldots \geq r_m$. If for all $l, 1 \leq l \leq m$, $r_l \leq m - l + 1$, then $n^2 = \sum_{l=1}^{m} r_l \leq \sum_{l=1}^{m} l = \frac{m(m+1)}{2}$. Hence we have $m > \sqrt{2} \cdot n - 1$ as promised.

Therefore, let's assume for some s, $s \geq 2$, $r_s \geq m - s + 2$. We denote $r = m - s + 2$.

We will consider non-singular linear transformations of $\mathbf{x}$, which in turn effects column transformations on C. For the chosen $\tilde{C}$, there is a cononical "lower triangular" form under this linear transformations: For $1 \leq j \leq n^2$, if t_j is minimal index such that $\tilde{c}_{t_j,j} \neq 0$, then the t_j's form a strictly monotonic increasing sequence $t_1 < t_2 < \ldots < t_{n^2}$. Note that since the matrix C is of rank n^2, all t_j's exist. We choose the first s blocks of $\tilde{C}$, $(\tilde{c}_{ij})_{sm \times n^2}$.

Now we take a slightly different view. We take the conditon (15) as a linear equation system to be solved for $\mathbf{x}$, and we wish to find an A of rank r such that $A \cdot (\tilde{c}_{ij})$ is of full rank sr. And if so, surely there must be a solution $\mathbf{x_0}$ satisfying (15).

More specifically, we will consider (15) as a linear equation system on

$$x_1, \ldots, x_r, x_{r_1+1}, \ldots, x_{r_1+r}, \ldots, x_{r_1+\ldots+r_{s-1}+1}, \ldots, x_{r_1+\ldots+r_{s-1}+r},$$

(setting all other variables $x_i = 0$). The determinant of this linear system is $\prod_{l=1}^{s} det_l$, where $det_l = det(A \cdot D_l)$, and D_l is the lth "diagonal" block in the canonical form $(\tilde{c}_{ij})$, i.e., the submatrix of the canonical form consisting of rows $(l-1)m+1$ to lm and columns $R+1$ to $R+r$, where $R = r_1 + \ldots + r_{l-1}$.

If we view det_l as a polynomial in the indeterminates a_{ij}, it is a non-zero element in the ring $F[a_{ij}]$. This is easily seen by applying a homomorphism $h : a_{ij} \mapsto 0$, where $1 \leq i \leq r$ and $j \neq t_\alpha$ for $1 \leq \alpha \leq r$, and thus,

$$h(det_l) = c \cdot \det \begin{pmatrix} a_{1t_1} & a_{1t_2} & \cdots & a_{1t_r} \\ a_{2t_1} & a_{2t_2} & \cdots & a_{2t_r} \\ \vdots & \vdots & \ddots & \vdots \\ a_{rt_1} & a_{rt_2} & \cdots & a_{rt_r} \end{pmatrix}, \tag{16}$$

for some $c \neq 0$. Similarly all det_l, $1 \leq l \leq s$, are nontrivial polynomials. Hence, the product of (16) with $\prod_{l=1}^{s} det_l \in F[a_{ij}]$ is a nontrivial polynomial, and therefore does not vanish identically. (One can phrase this in geometric terms as follows: a higher dimensional variety can *not* be expressed as a finite union of lower dimensional varieties.) Hence we have a rank r matrix A (guarenteed by the extra determinant (16) in the product) such that the linear equation system on the chosen subset of $\mathbf{x}$ has a solution. **QED**

4 Conclusions

We discussed two proofs of lower bounds pertaining to a central question in Valiant's theory, the determinant and permanent problem. The second proof also establishes a strengthening of a classic theorem due to Marcus and Minc.

The lower bound established here is still far weaker than what we would like to see, namely superpolynomial.

As a negative note on improving the second proof, we observe that in section 3.2 we must use the presumed identity $perX = detY$ again in a major way. The following example shows the inadequacy of doing otherwise.

$$Y = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ x_{i_2 j_1} & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ x_{i_m j_1} & x_{i_m j_2} & \ldots & 1 \end{pmatrix}, \tag{17}$$

where $m \approx \sqrt{2}n$.

Acknowledgement

The author thanks Neil Immerman for first bringing up this problem in a discussion. He also thanks S. Bhatt, M. Furst, D. Kozen, D. J. Newman, D. Reich, V. Vazirani and A. Ranade for valuable discussions.

References

[AM] Atiyah, M. FRS, MacDonald, I., *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

[C] Cai, J., "With probability one, a random oracle separates PSPACE from the polynomial-time hierarchy," Proc. 18th ACM Sym. on Theory of Computation, 1986, pp 21-29.

[E] Egorychev, G., "The solution of van der Waerden's Problem for Permanent," Advances in Mathematics, 42, 1981, pp 299-305.

[FSS] Furst, M., Saxe, J., Sipser, M., "Parity, circuits and the polynomial-time hierarchy," Mathematical Systems Theory, 17, 1984, pp 13-27.

[G] von zur Gathen, J., "Permanent and Determinant" Proc. 27th IEEE Foundations of Computer Science, 1986, pp 398-401.

[HLS] Hartmanis, J., Lewis, P., Stearns, R., "Hierarchies of memory limited computations", Proc. 6th Symp. on Switching Circuit Theory and Logical Design, 1965, pp 179-190.

[H] Hartshorne, R., *Algebraic Geometry,* Springer-Verlag, 1977.

[HU] Hopcroft, J., Ullman, J., *Introduction to automata theory, languages, and computation,* Addison-Wesley, 1979.

[MM] Marcus, M., Minc, H., "On the relation between the determinant and the permanent," Illinois J. Math, 5, 1961, pp 376-381.

[M] Minc, H., Encyclopedia of Mathematics and its Applications, vol 6, Addison-Wesley, Reading, MA 1978.

[P] Pólya, G., Aufgabe 424. Arch. Math. Phys. 20, 1913, p 271.

[S] Szegö, G., Zu Aufgabe 424. Arch. Math. Phys. 21, 1913, pp 291-292.