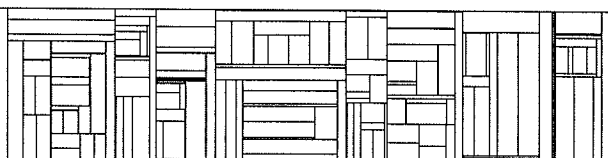


Are There Elimination Algorithms for the Permanent?

Carl Sturdivant

DAIMI PB – 306
March 1990

COMPUTER SCIENCE DEPARTMENT
AARHUS UNIVERSITY
Ny Munkegade, Building 540
DK-8000 Aarhus C, Denmark



Abstract

We define the class of elimination algorithms. These are algebraic algorithms for evaluating multivariate polynomials, and include as a special case Gaussian elimination for evaluating the determinant. We show how to find the linear symmetries of a polynomial, defined appropriately, and use these methods to find the linear symmetries of the permanent and determinant. We show that in contrast to Gaussian elimination for the determinant, there is no elimination algorithm for the permanent.

1 Introduction

Throughout this paper, when we refer to the permanent, we mean the permanent of an $n \times n$ matrix.

There is considerable interest in the computational properties of the permanent. The permanent has long been known to be of great expressive power in encoding combinatorial enumeration problems [Minc, 78]. An efficient algorithm for evaluating permanents would thus be of substantial interest.

Valiant's result that evaluating a 0-1-permanent is $\#P$ complete, [Valiant, 79 (i)], formalises the expressive power of the permanent, showing it to be sufficiently powerful to resolve any combinatorial enumeration problem in a computationally efficient manner, provided the corresponding existence problem is in NP . This is not a restrictive condition, and merely asserts that the structures to be counted should not be hard to recognize. (For definitions, see [Garey & Johnson, 79].)

However, this result may be a double-edged sword, since it suggests that the permanent is difficult to evaluate. Indeed, if the well-known conjecture $P \neq NP$ is proven, then it will follow that there does not exist an efficient algorithm to evaluate the permanent.

However, progress towards negative results of much weaker kinds in computational complexity theory has been almost negligible as of the time of writing. And the basis of the conjecture $P \neq NP$ is simply that since no one has been able to invent an efficient algorithm for any of a wide class of natural problems, the existence of such algorithms is held to be

improbable. In this paper, we prove the evaluation of the permanent by any of a wide class of algorithms to be impossible.

Early attempts to understand the computational properties of the permanent mainly fall into two categories. The first was the invention of various methods of evaluating the permanent, all requiring more than about 2^n arithmetic operations (many of these are given in [Minc, 78]). Of interest in this relation is the result that if only addition and multiplication operations are used, then more than about 2^n operations are necessary [Jerrum & Snir, 82]. Furthermore, it can be shown that subtraction is the important additional arithmetic operation, and that division is unimportant ([Jerrum & Snir, 82] and [Strassen, 73]).

The second category was various attempts to relate the computational properties of the permanent to those of the much more tractable determinant, usually giving negative results. This all began when in 1913 Pólya showed that for $n \geq 3$, the permanent could not be obtained from the $n \times n$ determinant by affixing minus signs to an arbitrary sub-set of the entries. Further to this, in 1961 Marcus and Minc showed that there exists no linear transformation on $n \times n$ matrices for $n \geq 3$ that converts the determinant of each matrix into its permanent [Marcus & Minc, 61].

A related result has been proved in 1988 due to Cai; this shows that if each entry of a $\lceil \sqrt{2}n \rceil \times \lceil \sqrt{2}n \rceil$ matrix is taken to be either a variable x_{ij} or a constant for $1 \leq i, j \leq n$, then the determinant of the resulting matrix is not equal to the permanent of the $n \times n$ matrix $[x_{ij}]$, [Cai, 88].

Such a transformation is called a projection of the determinant to the permanent, and if $k(n)$ is the size of the smallest determinant that projects to the $n \times n$ permanent, then $k(n)$ is closely related to the size of the smallest formula for the $n \times n$ permanent [Valiant, 79 (ii)].

When taken in this spirit the result of Cai that $k(n) \geq \lceil \sqrt{2}n \rceil$ is very weak, especially in view of the result that the formula size of the permanent is at least about n^3 [Kalorkoti, 82].

The results of this paper fall into the second category. We explore the possibility of more general computational analogies between the permanent and the determinant.

2 Elimination Algorithms

Let $f \in \mathbf{C}[\mathbf{X}]$ where $\mathbf{X} = (X_1, \dots, X_n)^t$ is a tuple of indeterminates. Informally, an elimination algorithm for evaluating f works as follows: Given $\mathbf{a} = (a_1, \dots, a_n)^t \in \mathbf{C}^n$, the values to be substituted for \mathbf{X} , the algorithm selects in some fashion a linear transformation $T : \mathbf{C}^n \rightarrow \mathbf{C}^n$ that has two properties: First, that $T\mathbf{a}$ is a tuple containing a number of zero values that enables the evaluation of $f(T\mathbf{a})$ to proceed in some simple manner. Second, that the use of T in general preserves f , i.e. $f(T\mathbf{X}) = f(\mathbf{X})$. We call such a transformation T , a *linear symmetry* of f . Thus the evaluation of $f(T\mathbf{a})$ yields the desired result $f(\mathbf{a})$.

Gaussian elimination for evaluating the determinant can be interpreted as an elimination algorithm in this sense as follows: The linear symmetries of the determinant that are used are those that correspond to multiplying the indeterminates arranged in a square matrix on the left and right by matrices of determinant one. Given a particular matrix whose determinant is to be computed, a linear transformation is selected that when applied to these particular inputs, produces a new input with many zeros (in fact, an upper triangular matrix) whose determinant may easily be computed. The utility of introducing zeros by means of a linear transformation may now readily be seen: a formula for the polynomial in question may be much reduced in size, in this case to a single term.

Clearly if the set of linear symmetries of f is very restricted, then f cannot have any elimination algorithms. Conversely, if f has a substantial set of linear symmetries, it seems likely that these could be exploited for computational purposes. Thus in the next section, we investigate linear symmetries in general: their properties and how to find them.

3 Linear Symmetries

We generalize the previous section slightly to include more than one polynomial.

Let $\mathbf{f} = (f_1, \dots, f_n)^t \in (\mathbf{C}[\mathbf{X}])^m$ and let $\nabla = (\frac{\partial}{\partial X_1}, \dots, \frac{\partial}{\partial X_n})^t$ be a formal differentiation operator. Let $M_n(\mathbf{C})$ be the set of all $n \times n$ matrices over \mathbf{C} .

Definition 1 The Linear Symmetries of \mathbf{f} ,

$$G_{\mathbf{f}} = \left\{ \left(\begin{array}{c|c} U & 0 \\ \hline 0 & W \end{array} \right) \mid U \in M_n(\mathbf{C}), W \in M_m(\mathbf{C}) \right. \\ \left. \forall \mathbf{x} \in \mathbf{C}^n \quad \mathbf{f}^t(U\mathbf{x})W = \mathbf{f}^t(\mathbf{x}) \right\}$$

$G_{\mathbf{f}}$ is therefore an affine closed set in $\mathbf{C}^{(n+m)^2}$. Clearly, $G_{\mathbf{f}}$ is a semi-group under matrix multiplication. It is natural to inquire under what conditions it is a group.

There are two kinds of redundancy that \mathbf{f} could have that would prevent $G_{\mathbf{f}}$ from being a group. The first is if \mathbf{f} , regarded as a function, does not vary in all directions in \mathbf{C}^n . In this case a linear symmetry may safely kill vectors in the “bad” directions, and thus be singular.

Definition 2 The Translational Symmetries of \mathbf{f} ,

$$T_{\mathbf{f}} = \{\mathbf{a} \in \mathbf{C}^n \mid \forall \mathbf{X} \in \mathbf{C}^n \quad \mathbf{f}(\mathbf{X} + \mathbf{a}) = \mathbf{f}(\mathbf{X})\}$$

Proposition 1 $T_{\mathbf{f}}$ is a vector space.

Proof

Clearly $\mathbf{0} \in T_{\mathbf{f}}$ and $\mathbf{a}, \mathbf{b} \in T_{\mathbf{f}}$ implies $\mathbf{f}((\mathbf{X} + \mathbf{a}) + \mathbf{b}) = \mathbf{f}(\mathbf{X} + \mathbf{a}) = \mathbf{f}(\mathbf{X})$, i.e. $\mathbf{a} + \mathbf{b} \in T_{\mathbf{f}}$. Thus it remains to show that $T_{\mathbf{f}}$ is closed under scalar multiplication.

Suppose $\mathbf{a} \in T_{\mathbf{f}}$. We show $\lambda \mathbf{a} \in T_{\mathbf{f}}$ for $\lambda \in \mathbf{C}$ as follows: choose a non-singular matrix $S \in M_n(\mathbf{C})$ satisfying $\mathbf{a} = S\mathbf{e}^{(n)}$ where

$$e_i^{(n)} = \begin{cases} 1 & \text{if } i = n \\ 0 & \text{otherwise} \end{cases}$$

Define $\mathbf{g}(\mathbf{X}) = \mathbf{f}(S\mathbf{X})$ then $\mathbf{e}^{(n)} \in T_{\mathbf{g}}$.

Define $D = \mathbf{C}[X_1, \dots, X_n]$ then for $1 \leq i \leq m$, $g_i \in D[X_n]$ so write g_i as $g_i(X_n)$. Now $g_i(0) = g_i(1) = g_i(2) = \dots = g_i(N)$ for any $N \in \mathbf{N}$. Thus $g_i(X_n) - g_i(0)$ has roots including \mathbf{N} over D . However, D is an integral domain, and so all $h \in D[X_n] \setminus \{0\}$ have only finitely many roots. Thus $g_i(X_n) = g_i(0)$ for $1 \leq i \leq m$, i.e. $g_i \in D$ (g_i does not depend upon X_n at all). Thus $\lambda \mathbf{e}^{(n)} \in T_{\mathbf{g}}$ for any $\lambda \in \mathbf{C}$, since \mathbf{g} is independent of X_n .

$$\begin{aligned} & \forall \mathbf{x} \quad \mathbf{g}(\mathbf{x} + \lambda \mathbf{e}^{(n)}) = \mathbf{g}(\mathbf{x}) \text{ and } \mathbf{g} \text{ is } \mathbf{f} \text{ composed with } S, \\ \Rightarrow & \forall \mathbf{x} \quad \mathbf{f}(S(\mathbf{x} + \lambda \mathbf{e}^{(n)})) = \mathbf{f}(S\mathbf{x}) \\ \Rightarrow & \forall S\mathbf{x} \quad \mathbf{f}(S\mathbf{x} + \lambda \mathbf{a}) = \mathbf{f}(S\mathbf{x}) \\ \Rightarrow & \forall \mathbf{x} \quad \mathbf{f}(\mathbf{x} + \lambda \mathbf{a}) = \mathbf{f}(\mathbf{x}) \\ \Rightarrow & \lambda \mathbf{a} \in T_{\mathbf{f}} \end{aligned}$$

■

Thus informally, if $\dim(T_{\mathbf{f}}) > 0$ then $G_{\mathbf{f}}$ may contain some singular matrices.

The second kind of redundancy is that \mathbf{f} may be linearly dependent over \mathbf{C} . In this case a linear symmetry may also be singular.

Definition 3 The Linear Dependencies of \mathbf{f} ,

$$D_{\mathbf{f}} = \{\mathbf{a} \in \mathbf{C}^n \mid \mathbf{a} \cdot \mathbf{f} = 0\}$$

$D_{\mathbf{f}}$ is clearly a vector space.

Proposition 2 $G_{\mathbf{f}}$ is a group iff $\dim(T_{\mathbf{f}}) = \dim(D_{\mathbf{f}}) = 0$.

Proof

(\Leftarrow) It is sufficient to show that each element of $G_{\mathbf{f}}$ has an inverse as a matrix, since it is obvious that such an inverse will then certainly be a member of $G_{\mathbf{f}}$. Let $(\begin{smallmatrix} U & | & 0 \\ 0 & | & W \end{smallmatrix})$ be a member of $G_{\mathbf{f}}$, assumed singular by contradiction. Thus there are two cases: either U or W is singular. If U is singular then there exists an \mathbf{a} with $U\mathbf{a} = \mathbf{0}$. Thus, $\mathbf{f}^t(\mathbf{X}) = \mathbf{f}^t(U\mathbf{X})W = \mathbf{f}^t(U(\mathbf{X} + \mathbf{a}))W = \mathbf{f}^t(\mathbf{X} + \mathbf{a})$. Thus, $\dim(T_{\mathbf{f}}) > 0$, a contradiction.

If W is singular, then there exists a \mathbf{b} with $W\mathbf{b} = \mathbf{0}$. Thus $\mathbf{f}^t(\mathbf{X})\mathbf{b} = \mathbf{f}^t(U\mathbf{X})W\mathbf{b} = \mathbf{0}$. Thus $\dim(D_{\mathbf{f}}) > 0$, a contradiction.

(\Rightarrow) If $\dim(T_{\mathbf{f}}) > 0$, then there exists $\mathbf{a} \neq \mathbf{0}$, such that $\mathbf{f}(\mathbf{X} + \mathbf{a}) = \mathbf{f}(\mathbf{X})$. Now choose a basis for \mathbf{C}^n where \mathbf{a} is one of the base vectors. We may now choose a matrix U satisfying $U\mathbf{a} = \mathbf{0}$ and also satisfying $U\mathbf{b} = \mathbf{b}$ for any other base vector \mathbf{b} in the basis. Now write any vector $\mathbf{X} = \lambda\mathbf{a} + \mathbf{c}$ where \mathbf{c} is a linear combination of the other base vectors, and therefore satisfies $U\mathbf{c} = \mathbf{c}$. Then

$$\mathbf{f}(U\mathbf{X}) = \mathbf{f}(U(\lambda\mathbf{a} + \mathbf{c})) = \mathbf{f}(\mathbf{c}) = \mathbf{f}(\lambda\mathbf{a} + \mathbf{c}) = \mathbf{f}(\mathbf{X}),$$

the last step following because \mathbf{a} is a translational symmetry of \mathbf{f} . Thus, $(\begin{smallmatrix} U & | & 0 \\ 0 & | & I_m \end{smallmatrix}) \in G_{\mathbf{f}}$ and therefore $G_{\mathbf{f}}$ is not a group, since U is singular.

Alternatively, if $\dim(D_{\mathbf{f}}) > 0$, then there exists $\mathbf{b} \neq \mathbf{0}$ satisfying $\mathbf{f}^t\mathbf{b} = \mathbf{0}$. Now choose a basis for \mathbf{C}^n including \mathbf{b} and choose a matrix W satisfying $W\mathbf{b} = \mathbf{0}$ and $W\mathbf{c} = \mathbf{c}$ for any other base vector. Thus, for any vector $\mathbf{y} = \lambda\mathbf{b} + \mathbf{a}$ where \mathbf{a} is a linear combination of the other base vectors, we have $\mathbf{f}^tW\mathbf{y} = \mathbf{f}^tW(\lambda\mathbf{b} + \mathbf{a}) = \mathbf{f}^t\mathbf{a} = \mathbf{f}^t(\lambda\mathbf{b} + \mathbf{a}) = \mathbf{f}^t\mathbf{y}$, the last step following because \mathbf{b} is a linear dependency of \mathbf{f} .

Thus $\mathbf{f}^tW = \mathbf{f}^t$ and $(\begin{smallmatrix} I_n & | & 0 \\ 0 & | & W \end{smallmatrix}) \in G_{\mathbf{f}}$ and therefore $G_{\mathbf{f}}$ is not a group, since W is singular. ■

If $\dim(D_{\mathbf{f}}) = \dim(T_{\mathbf{f}}) = 0$ then we say that \mathbf{f} is *irredundant*.

From a practical point of view $D_{\mathbf{f}}$ can be obtained simply by solving linear equations. $T_{\mathbf{f}}$ can also be found by solving linear equations by using the following:

Proposition 3 $T_{\mathbf{f}} = \{\mathbf{a} \in \mathbf{C}^n \mid (\mathbf{a} \cdot \nabla)\mathbf{f} = 0\}$.

Proof

$$\mathbf{a} \in T_{\mathbf{f}} \Rightarrow \lambda \mathbf{a} \in T_{\mathbf{f}} \Rightarrow \mathbf{f}(\mathbf{x} + \lambda \mathbf{a}) - \mathbf{f}(\mathbf{x}) = 0$$

$$\Rightarrow \lim_{\lambda \rightarrow 0} \frac{\mathbf{f}(\mathbf{x} + \lambda \mathbf{a}) - \mathbf{f}(\mathbf{x})}{\lambda} = 0$$

$$\Rightarrow (\mathbf{a} \cdot \nabla)\mathbf{f} = 0$$

Conversely $(\mathbf{a} \cdot \nabla)\mathbf{f} = 0$ implies $\forall k \in \mathbf{N}^+ \quad \frac{1}{k!}(\mathbf{a} \cdot \nabla)^k \mathbf{f} = 0$. Thus

$$\sum_{k=1}^{\deg f} \frac{1}{k!} (\mathbf{a} \cdot \nabla)^k \mathbf{f} = 0.$$

But this is just the (finite) Taylor expansion of $\mathbf{f}(\mathbf{x} + \mathbf{a}) - \mathbf{f}(\mathbf{x})$. Thus $\mathbf{a} \in T_{\mathbf{f}}$. ■

Thus if \mathbf{f} is irredundant then $G_{\mathbf{f}}$ is a Zariski-closed linear algebraic subgroup of $GL(n+m, \mathbf{C})$. As a consequence of this, $G_{\mathbf{f}} = G_{\mathbf{f}}^0 \cup G_{\mathbf{f}}^1 \cup \dots \cup G_{\mathbf{f}}^k$ is a non-intersecting union of irreducible affine closed sets (the components of $G_{\mathbf{f}}$) where k is finite and may be zero. All of the $G_{\mathbf{f}}^l$ are smooth (indeed are analytic manifolds), and $G_{\mathbf{f}}^0$ contains the identity, and is a normal subgroup of $G_{\mathbf{f}}$, the $G_{\mathbf{f}}^l$ being cosets of $G_{\mathbf{f}}^0$ in $G_{\mathbf{f}}$. $G_{\mathbf{f}}^0$ consists of all elements of $G_{\mathbf{f}}$ connected by a path to the identity matrix within $G_{\mathbf{f}}$, see [Shafareyevič, 77] and [Borel, 69]. Therefore $G_{\mathbf{f}}$ is generated by $G_{\mathbf{f}}^0$ and a finite number of additional matrices. We will show how to obtain $G_{\mathbf{f}}^0$ explicitly.

As is usual with Lie groups, this is obtained by applying the exponential function to the vector space of “infinitesimal transformations” associated with $G_{\mathbf{f}}^0$ [Miller, 73].

Definition 4 The tangent space to the $G_{\mathbf{f}}$ identity is

$$V_{\mathbf{f}} = \left\{ \left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array} \right) \mid \mathbf{f}^t((I + \epsilon A)\mathbf{X})(I + \epsilon B) = \mathbf{f}^t(\mathbf{X}) + O(\epsilon^2) \right\}$$

This is precisely the external definition of tangent space used in algebraic geometry or differential geometry (see e.g. [Mumford, 76]) i.e. perturbation vectors of $O(\epsilon)$ about I which give only $O(\epsilon^2)$ deviation from the surface.

Clearly $V_{\mathbf{f}}$ is a vector space, and since $G_{\mathbf{f}}^0$ is smooth, $\dim(V_{\mathbf{f}}) = \dim(G_{\mathbf{f}}^0)$.

Proposition 4 Let $\exp: M_{n+m}(\mathbf{C}) \rightarrow M_{n+m}(\mathbf{C})$ be the exponential map, (defined by power series that converges everywhere), and let angle brackets denote closure under matrix multiplication (group multiplication). Then $\langle \exp(V_{\mathbf{f}}) \rangle = G_{\mathbf{f}}^0$.

Proof

Routine. ■

It follows that if we can find $V_{\mathbf{f}}$, then we can find $G_{\mathbf{f}}^0$; however, $V_{\mathbf{f}}$ can be found by simple linear algebra using the following:

Proposition 5 $\left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array} \right) \in V_{\mathbf{f}}$ iff $(A\mathbf{x}) \cdot \nabla \mathbf{f} + B^t \mathbf{f} = \mathbf{0}$.

Proof

The $O(\epsilon)$ part of $(\mathbf{f}^t((I + \epsilon A)\mathbf{x})(I + \epsilon B) - \mathbf{f}^t(\mathbf{X}))^t$ is $((A\mathbf{x}) \cdot \nabla \mathbf{f} + B^t \mathbf{f})\epsilon$. ■

We conclude that to find the computationally useful linear symmetries of \mathbf{f} , we first find $T_{\mathbf{f}}$ and $D_{\mathbf{f}}$ by solving linear equations, and check thereby that the linear symmetries form a group. We then find $V_{\mathbf{f}}$ by solving linear equations and apply the exponential map.

4 Applications to the permanent and the determinant

4.1 Notation

The permanent and determinant are usually written as polynomial functions of a matrix. Since the previous theory was developed to deal with functions of a column vector, we must provide a means of so encoding the permanent and determinant.

Let X be an $n \times n$ matrix with entries x_{ij} . Let $X_{.j}$ denote the j 'th column of X . Define $\mathbf{vec}(X) = (X^{t \cdot 1} | X^{t \cdot 2} | \dots | X^{t \cdot n})^t = \mathbf{x}$, i.e. \mathbf{x} consists of the columns of X stacked one on top of another in order. We now define $\text{per}(\mathbf{x}) = \text{per}(X)$ and similarly for the determinant.

Finally we introduce the Kronecker product \otimes : If A and B are $n \times n$ matrices then $A \otimes B$ is the $n^2 \times n^2$ matrix consisting of the $n \times n$ blocks $a_{ij}B$ arranged in the natural order, where the a_{ij} s are the entries of the matrix A . Under this regime, we have the usual identity $\mathbf{vec}(AXB) = (B^t \otimes A)\mathbf{x}$.

4.2 Results

Theorem 1 Provided $n > 2$, the $n \times n$ permanent has

$$G_{\text{per}}^0 = \left\{ \left(\frac{U}{0} \middle| \frac{0}{W} \right) \mid U = \Lambda \otimes \bar{\Lambda}, W = \det(\Lambda \bar{\Lambda})^{-1}, \right. \\ \left. \Lambda, \bar{\Lambda} \text{ } n \times n \text{ non singular diagonal matrices} \right\}$$

and furthermore, $\dim(G_{\text{per}}^0) = 2n - 1$.

Theorem 2 The $n \times n$ determinant has

$$G_{\text{det}}^0 = \left\{ \left(\frac{U}{0} \middle| \frac{0}{W} \right) \mid U = A \otimes B, W = \det(AB)^{-1}, \right. \\ \left. A, B \text{ } n \times n \text{ non singular matrices} \right\}$$

and furthermore, $\dim(G_{\text{det}}^0) = 2n^2 - 1$.

Note: These are simply the well-known symmetries of the permanent and determinant (apart from those that arise from permuting the variables, some of which are not in G^0). The interest of the theorems are that these are the only symmetries in G^0 . Clearly the paucity of symmetries of the permanent shows that it can have no elimination algorithms.

Proof of Theorems 1 and 2

We first note that both $\text{per}(\mathbf{x})$ and $\text{det}(\mathbf{x})$ are irredundant. This follows because a single non-zero polynomial cannot be linearly dependent, thus $\dim(D_{\text{per}}) = \dim(D_{\text{det}}) = 0$. Furthermore, per and det have no translational symmetries because by proposition 3 these are linear dependencies among all the partial derivatives. The partial derivatives are merely all the $(n-1) \times (n-1)$ sub-permanents and sub-determinants respectively. These cannot be linearly dependent over \mathbf{C} since no two of them have any terms in common. Thus $\dim(T_{\text{per}}) = \dim(T_{\text{det}}) = 0$. Thus by proposition 4, G_{per} and G_{det} are groups.

We now use proposition 7 to determine V_{det} and V_{per} .

$$\left(\begin{array}{c|c} M & 0 \\ \hline 0 & m \end{array} \right) \in V_{\text{per}}$$

where M is $n^2 \times n^2$ and m is 1×1 iff

$$\sum_{i,j=1}^n \left(\sum_{k,l=1}^n M_{ij\,kl} x_{kl} \frac{\partial}{\partial x_{ij}} \text{per}(\mathbf{x}) \right) + m \cdot \text{per}(\mathbf{x}) = 0 \quad (\star)$$

(The subscripts are doubled because the x_{ij} that are the entries of \mathbf{x} have two subscripts.) An analogous condition goes for V_{det} .

The condition (\star) implies a set of linear constraints that the $M_{ij\,kl}$ and m must satisfy: namely, that the coefficient of each monomial in the x_{ij} in the expansion of (\star) , must vanish. We now solve these linear equations explicitly.

There are essentially three kinds of monomials in (\star) . The first kind are those monomials that occur in the permanent itself. These originate from

two sources: first, from the term $m \cdot \text{per}(\mathbf{x})$ and second, from the various expressions of the form $M_{ij\ ij} x_{ij} \frac{\partial}{\partial x_{ij}} \text{per}(\mathbf{x})$. This is because the effect of the operator $x_{kl} \frac{\partial}{\partial x_{ij}}$ on a monomial in the permanent is either to yield zero if the monomial does not include x_{ij} or to “delete” x_{ij} “replacing” it with x_{kl} , since the monomials are all multilinear. Thus the only way that a permanent monomial may be obtained is if $(k, l) = (i, j)$, since each such monomial contains exactly one entry in each row and column of X .

The linear constraints imposed originate therefore from the equation

$$\sum_{ij} (M_{ij\ ij} + \frac{m}{n}) x_{ij} X_{ij} = 0$$

where $X_{ij} = \frac{\partial}{\partial x_{ij}} \text{per}(\mathbf{x})$ and we use the identity $\text{per}(\mathbf{x}) = \frac{1}{n} \sum_{ij} x_{ij} X_{ij}$. Equating the coefficient of the generic monomial $\prod_i x_{i\sigma(i)}$ to zero gives

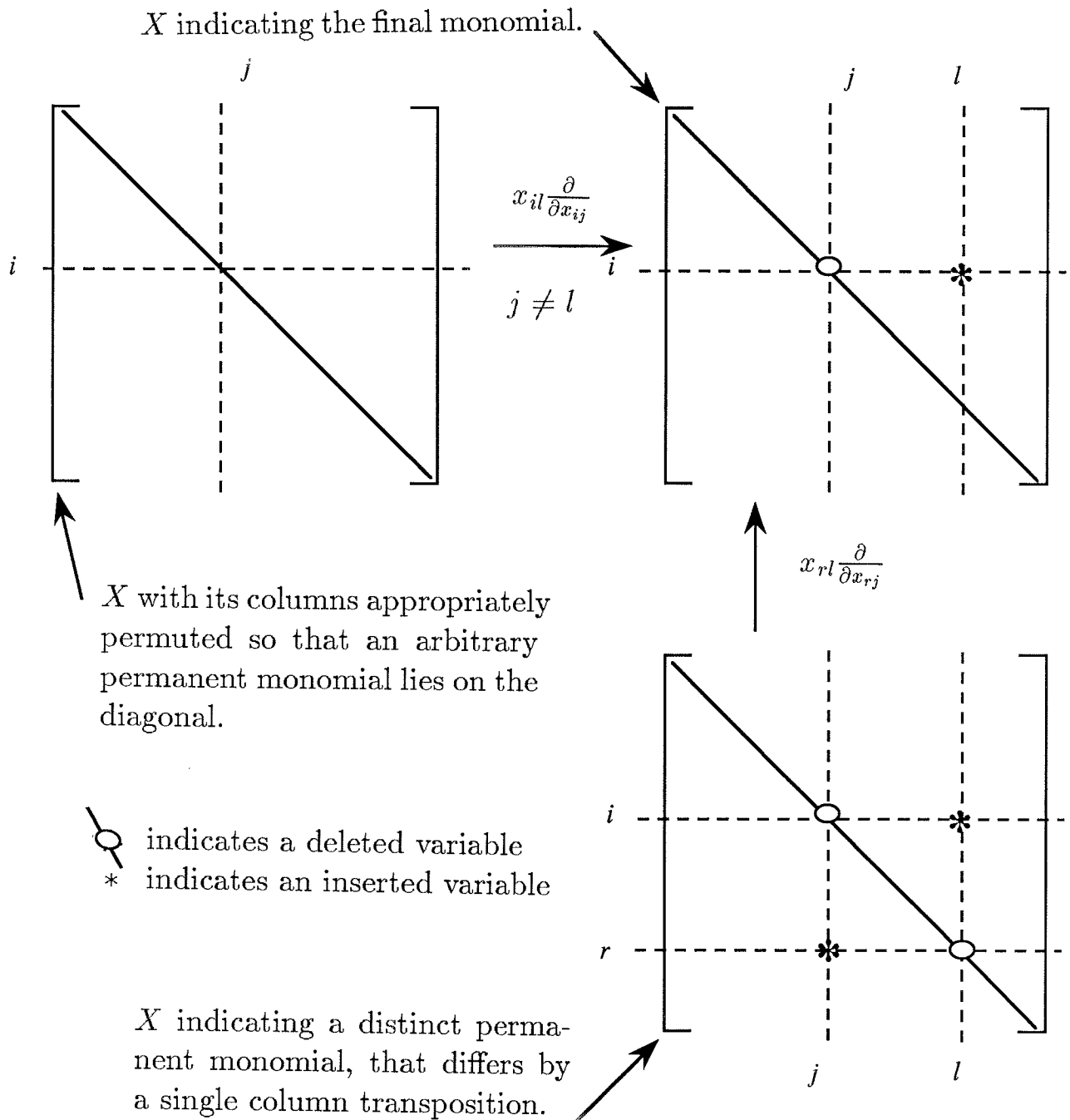
$$\sum_i (M_{i\sigma(i)\ i\sigma(i)} + \frac{m}{n}) = 0$$

The general solution to these constraints is $M_{ij\ ij} = a_i + b_j$ and $m = -\sum_i (a_i + b_i)$ where a_i and b_j are $2n$ arbitrary parameters although only $2n - 1$ are independent, since if c is any constant $(a_i + c)$ and $(b_j - c)$ yield the same values for $M_{ij\ ij}$ and m . A similar argument goes for the determinant.

The second kind of monomial occurs in the various expressions of the form $M_{ij\ kl} x_{kl} \frac{\partial}{\partial x_{ij}} \text{per}(\mathbf{x})$ where $i \neq k$ and $j \neq l$. These monomials have the form of a permanent monomial where a variable x_{ij} has been deleted and a variable x_{kl} , that is neither in the same row nor column of X as x_{ij} , has been inserted. Clearly, such a monomial arises from a unique permanent monomial by the action of a unique $x_{kl} \frac{\partial}{\partial x_{ij}}$. Thus condition (\star) implies that all $M_{ij\ kl}$ with $i \neq k$ and $j \neq l$ must be zero. Note that a similar argument goes for the determinant.

The third type of monomial occurs in the various expressions of the form $M_{ij\ il} x_{il} \frac{\partial}{\partial x_{ij}} \text{per}(\mathbf{x})$ where $j \neq l$ and of the form $M_{ij\ kj} x_{kj} \frac{\partial}{\partial x_{ij}} \text{per}(\mathbf{x})$ where $i \neq k$. The latter expressions are related to the former expressions by transposition of X , under which per and det are invariant, thus we will investigate only the former. The monomials obtained by the action of $x_{il} \frac{\partial}{\partial x_{ij}}$ are of the form of a permanent monomial in which x_{ij} has been

deleted and a variable in the same row of X has been inserted, namely x_{il} . Such a monomial could have been obtained from precisely two distinct permanent monomials as illustrated by the following diagrams.



Thus, in the case of the permanent we have the equations

$$M_{ij\,il} + M_{rj\,rl} = 0$$

for any i, j, l and r where $j \neq l$, since the above holds for an *arbitrary* monomial.

In the case of the determinant we have $M_{ij\,il} - M_{rj\,rl} = 0$ for any i, j, l and r where $j \neq l$. The sign difference arises from the fact that the two monomials in the diagram are of opposite parity and therefore have opposite sign in the determinant. It is here that the major difference between the permanent and the determinant becomes apparent.

The constraints for the determinant merely provide that given any $j \neq l$, $M_{ij\,il} = M_{rj\,rl}$ for any i and r ; i.e. $M_{ij\,il} = a_{jl}$ where a_{jl} for $j \neq l$ are $n^2 - n$ arbitrary parameters. (It is natural in this case to take the n arbitrary parameters a_i from the analyses of the first kind of monomial to be a_{ii} . We also have $M_{ij\,kj} = b_{ik}$ from the analogous “transposed” constraints, and we take b_{ii} to be b_i .)

Thus the general solution for the determinant involves $2n^2$ arbitrary parameters (although only $2n^2 - 1$ are independent) and is $M_{ij\,kl} = \delta_{ik}a_{jl} + \delta_{jl}b_{ik}$ and $m = -\sum_i(a_{ii} + b_{ii})$.

The situation for the permanent is very different. Instead of all the $M_{ij\,il}$ for a given $j \neq l$ being equal, they are all negations of each other. Clearly, if there are more than two of them, then this implies they are all identically zero. Thus for $n > 2$ the general solution for the permanent is $M_{ij\,ij} = a_i + b_j$ and all other $M_{ij\,kl}$ are identically zero; i.e. $M_{ij\,kl} = \delta_{ik}\delta_{jl}(a_i + b_j)$ and $m = -\sum_i(a_i + b_i)$. We have now found V_{per} and V_{det} , and they are of dimensions $2n - 1$ and $2n^2 - 1$ respectively.

Now, by proposition 6, we merely have to apply the exponential map to obtain G_{per}^0 and G_{det}^0 . For the determinant we have $M = I \otimes A + B \otimes I$ where I is the $n \times n$ identity matrix and A and B are $n \times n$ matrices of arbitrary parameters. We also have $m = -\text{Tr}(A) - \text{Tr}(B)$. Thus $\exp(M) = \exp(A) \otimes \exp(B)$ which is the Kronecker product of two arbitrary non-singular matrices, since \exp is onto $GL(n, \mathbf{C})$, and $\exp(m) = \det(\exp(A)\exp(B))^{-1}$. Thus since $C \otimes D (\text{vec}(X)) = D^t X C$, we have theorem 2. Theorem 1 follows analogously except that only the diagonals of the arbitrary matrices are non-zero. ■

5 A Miscellany of Further Results

Having found G^0 for the permanent and the determinant, a number of other observations are now easy to prove.

The next theorem is a formalization of the now intuitively obvious fact that since G_{per}^0 and G_{det}^0 are not isomorphic, then the permanent cannot be obtained from the determinant by the substitution of non-singular linear forms. This fact was first proved in [Marcus & Minc, 61].

Definition 5 Similarity of \mathbf{f} and \mathbf{g} : \mathbf{f} is similar to \mathbf{g} ($\mathbf{f} \equiv \mathbf{g}$) iff there exist non-singular matrices S, T (i.e. $\det(\begin{smallmatrix} S & 0 \\ 0 & T \end{smallmatrix}) \neq 0$) such that $\mathbf{f}^t(S\mathbf{X})T = \mathbf{g}^t(\mathbf{X})$.

Proposition 6 The relation \equiv is an equivalence relation on $(\mathbf{C}[\mathbf{X}])^m$, and $\mathbf{f} \equiv \mathbf{g}$ (for irredundant \mathbf{f}, \mathbf{g}) implies $G_{\mathbf{f}} \cong G_{\mathbf{g}}$ (isomorphism as groups and affine closed sets). In fact, $G_{\mathbf{f}}$ and $G_{\mathbf{g}}$ are conjugate subgroups of $GL(n+m, \mathbf{C})$ and $V_{\mathbf{f}} \cong V_{\mathbf{g}}$ (conjugate Lie algebras).

Proof

Routine. ■

This provides a simple criterion for similarity of polynomials of non-trivial symmetry.

Theorem 3 [Marcus & Minc, 61]

There is no linear transformation S such that $\det(S\mathbf{x}) = \text{per}(\mathbf{x})$, for $n > 2$.

Proof

Such an S cannot be singular, since that would imply that $\text{per}(\mathbf{x})$ had a non-zero translational symmetry, which by proposition 3 is false.

However, the existence of a non-singular S satisfying $\det(S\mathbf{x}) = \text{per}(\mathbf{x})$ implies $\det \equiv \text{per}$ and thus, by proposition 6, $G_{\det}^0 \cong G_{\text{per}}^0$. This is impossible for $n > 2$ by theorems 1 and 2, since the groups have different dimensions. ■

Another useful property possessed by the determinant is the existence of a bilinear product of matrices (just ordinary matrix multiplication) that preserves the determinant, as expressed by the identity $\det(AB) = \det(A) \cdot \det(B)$. However, the permanent has inadequate symmetry to support such a product.

Theorem 4 For $n > 2$, there is no bilinear function

$$\Psi : M_n(\mathbf{C})^2 \rightarrow M_n(\mathbf{C})$$

satisfying $\text{per}(\Psi(A, B)) = \text{per}(A) \cdot \text{per}(B)$ for all $A, B \in M_n(\mathbf{C})$.

Proof

We assume, in contradiction, that there is such a bilinear function. We define a matrix U_A , parametrized by A as follows: $U_A \text{vec}(X) = \text{vec}(\Psi(A, X))$. Clearly, U_A is linear in A and furthermore, $\text{per}(U_A \mathbf{x}) = \text{per}(A) \cdot \text{per}(\mathbf{x})$, and thus if $\text{per}(A) \neq 0$ then $(\begin{array}{c|c} U_A & 0 \\ \hline 0 & \text{per}(A)^{-1} \end{array}) \in G_{\text{per}}$. Therefore U_A is non-singular for all A with $\text{per}(A) \neq 0$. We now show that U_A as a function of A is injective. Assume $U_A = U_{A'}$ then $\Psi(A, X) = \Psi(A', X)$ and since Ψ is bilinear this implies $\Psi(A - A', X) = 0$.

By a precisely similar argument to that used to establish that U_A is nonsingular when $\text{per}(A) \neq 0$, it follows that by choosing $X = B$ where $\text{per}(B) \neq 0$, that $\Psi(A - A', B) = 0$ implies $A - A' = 0$.

Since A may range over an n^2 dimensional space, it follows that U_A must do likewise. If A is sufficiently close to the identity, then $\text{per}(A) \neq 0$, and this implies that $\dim(G_{\text{per}}) \geq n^2$ since $(\begin{array}{c|c} U_A & 0 \\ \hline 0 & \text{per}(A)^{-1} \end{array})$ is in G_{per} .

This is in direct contradiction to Theorem 1, for $n > 2$. ■

6 Conclusion

We have shown that the continuous linear symmetries of the permanent and determinant are exactly and only those that have been known historically. The permanent is barren of interesting symmetries and has therefore been shown to lack a wide variety of properties that are possessed by the determinant. In particular, the permanent is not computed by any kind of elimination algorithm.

References

- [Borel, 69] Borel, A., *Linear Algebraic Groups*. Benjamin, 1969.
- [Cai, 88] Cai, Jin-Yi, A Note on the Determinant and Permanent Problem. *Information & Computation* **84**, p. 119-127 (1990).
- [Garey & Johnson, 79] Garey, Micheal R. and Johnson, David S., *Computers and Intractability*. W.H. Freeman, 1979.
- [Jerrum & Snir, 82] Jerrum, M. and Snir, M., Some Exact Complexity Results for Straight-Line Computations over Semirings. *Journal of the ACM*, vol. 29, pp. 874-897 (1982).
- [Kalorkoti, 82] Kalorkoti, K.A., A Lower Bound on the Formula Size of Rational Functions. *Lecture Notes in Computer Science*, Springer-Verlag, vol. 140, pp. 330-338, (1982).
- [Marcus & Minc, 61] Marcus, M. and Minc, H., On the Relation Between the Determinant and the Permanent. *Illinois Journal of Mathematics* **5**, pp. 376-381 (1961).
- [Miller, 73] Miller, W., *Symmetry Groups and Their Applications*. Academic Press, 1973.
- [Minc, 78] Minc, H., *Permanents*. Addison-Wesley, 1978.
- [Mumford, 76] Mumford, D., *Algebraic Geometry, I*. Springer-Verlag, 1976.
- [Shafareyevič, 77] Shafareyevič, I.R., *Basic Algebraic Geometry*. Springer-Verlag, 1977.

- [**Strassen, 73**] Strassen, V. Die Berechnungskomplexität von elementarsymmetrischen Funktionen und von Interpolationskoeffizienten. *Numerische Mathematik* vol. **20**, no. 3, (1973).
- [**Valiant, 79 (i)**] Valiant, L.G., The Complexity of Computing the Permanent. *Theoretical Computer Science* **8**, pp. 189-201, (1979).
- [**Valiant, 79 (ii)**] Valiant, L.G., Completeness Classes in Algebra. *Proc. 11th ACM Symp. on Theory of Computing*, pp. 249-261, (1979).