NEW PERMANENT ESTIMATORS VIA NON-COMMUTATIVE DETERMINANTS

Alexander Barvinok

July 2000

Abstract. We introduce a new notion of the determinant, called symmetrized determinant, for a square matrix with the entries in an associative algebra $\mathcal{A}$. The monomial expansion of the symmetrized determinant is obtained from the standard expansion of the commutative determinant by averaging the products of entries of the matrix in all possible orders. We show that for any fixed finite-dimensional associative algebra $\mathcal{A}$, the symmetrized determinant of an $n \times n$ matrix with the entries in $\mathcal{A}$ can be computed in polynomial in n time (the degree of the polynomial is linear in the dimension of $\mathcal{A}$). Then, for every associative algebra $\mathcal{A}$ endowed with a scalar product and unbiased probability measure, we construct a randomized polynomial time algorithm to estimate the permanent of non-negative matrices. We conjecture that if $\mathcal{A} = \mathrm{Mat}(d, \mathbb{R})$ is the algebra of $d \times d$ real matrices endowed with the standard scalar product and Gaussian measure, the algorithm approximates the permanent of a non-negative $n \times n$ matrix within $O(\gamma_d^n)$ factor, where $\lim_{d \longrightarrow +\infty} \gamma_d = 1$. Finally, we provide some informal arguments why the conjecture might be true.

1. Introduction

(1.1) Permanent and determinant. Let $A = (a_{ij})$ be an $n \times n$ real matrix and let S_n denote the symmetric group of all permutations σ of the set $\{1, \dots, n\}$. The number

$$\mathrm{per}\, A = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i\sigma(i)}$$

is called the *permanent* of A. We will be interested in the case when A is non-negative: $a_{ij} \geq 0$ for $i, j = 1, \dots, n$.

To compute or to approximate the permanent efficiently is one of the most intriguing problems, see, for example, [Jerrum and Sinclair 89], [Karmarkar *et al.* 93], Chapter 18 of [Papadimitriou 94], [Linial *et al.* 98], [Barvinok 97] and [Barvinok 99].

Key words and phrases. non-commutative determinant, permanent, polynomial time algorithms, randomized algorithms, mixed discriminant, measure concentration.

This research was partially supported by NSF Grant DMS 9734138.

On the other hand, the determinant

$$\det A = \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma) \prod_{i=1}^{n} a_{i\sigma(i)}$$

can be computed using $O(n^3)$ arithmetic operations (even when A is a matrix over a commutative ring), see, for example, Sections 11.1 and 15.1 of [Papadimitriou 94].

Hence it seems natural to try to use determinants to approximate the permanent.

(1.2) Permanent estimators. The following approach is due to Godsil and Gutman and independently to Girko (see, for example, Chapter 8 of [Lovász and Plummer 86] and Section 3 of Chapter 2 of [Girko 90]. Let us choose a probability distribution μ on $\mathbb{R}$ with the properties that

$$\mathbf{E}\ x = \int_{\mathbb{R}} x\ d\mu(x) = 0 \quad \text{and} \quad \mathbf{E}\ x^2 = \int_{\mathbb{R}} x^2\ d\mu(x) = 1.$$

Let us sample n^2 numbers $u_{ij} : i, j = 1, \ldots, n$ independently and at random from μ. Let $B = (b_{ij})$ be the matrix defined by

$$b_{ij} = u_{ij} \sqrt{a_{ij}}$$

and let

$$\alpha = (\det B)^2.$$

Then α is a random variable and it turns out that $\mathbf{E}\ \alpha = \operatorname{per} A$. Hence, in principle, $\operatorname{per} A$ can be approximated by averaging sufficiently many determinants. It turns out that by extending the ground field, one can ensure a better concentration of α around its expectation and hence a better computational complexity of the approximation.

In [Karmarkar *et al.* 93] it was shown that if one allows u_{ij} to be complex numbers (we must define then $\alpha = |\det B|^2$), one can make the variance of α smaller. More precisely, the variance of α for the distribution μ that chooses the cubic roots of unity with the probability 1/3 each is exponentially smaller in the worst case than that for μ that chooses -1 and 1 with the probability 1/2 each. In [Barvinok 99], it was shown that if μ is a Gaussian distribution in $\mathbb{R}$ then with high probability a random value of α approximates its expectation within a c^n factor for $c \approx 0.28$; similar behavior is observed when μ is a complex Gaussian distribution, but in the complex case the constant c gets better: $c \approx 0.56$. Moreover, if μ is a quaternionic Gaussian distribution (in which case α should be the *Study determinant* of B, that is the determinant of the complexification of B, see, for example, [Aslaksen 96]), the constant c gets even better: $c \approx 0.76$.

This suggests that it may be of interest to construct more determinant-type estimators, as they could provide still better concentration properties of α.

Let us summarize some useful properties of the estimator. The estimator $\alpha = \alpha(u_{ij}) : i,j = 1,\dots,n$ is a function of n^2 independent and identically distributed random variables u_{ij}, such that:

(1.2.1) For each choice of u_{ij}, the value of $\alpha(u_{ij})$ can be computed using a polynomial in n number of arithmetic operations;

(1.2.2) The expected value of α is per A;

(1.2.3) For any choice of (u_{ij}), the value of $\alpha(u_{ij})$ is a non-negative real number;

(1.2.4) Let us fix all u_{ij} except those in one row i_0 (resp. in one column j_0). Then α is a quadratic form in $\{u_{i_0 j} : j = 1,\dots,n\}$ (resp. in $\{u_{ij_0} : i = 1,\dots,n\}$).

In this paper, for every associative finite-dimensional algebra $\mathcal{A}$ we construct an estimator with the properties (1.2.1)–(1.2.4).

(1.3) Non-commutative determinants. Exploring analogues of determinants over non-commutative rings and algebras is a very old topic, see, for example, [Aslaksen 96] for a survey and [Gelfand and Retakh 97] for new developments. Interestingly, most important non-commutative determinants, such as the Dieudonné determinant, quasideterminants of Gelfand and Retakh and the Moore determinant of a Hermitian quaternionic matrix turn out to be computationally efficient. However, with the notable exception of the Moore determinant, they are not close enough to the monomial expansion of the commutative determinant to produce a permanent estimator. On the other hand, as was noticed by S. Friedland [Friedland 00], the most straightforward version due to Cayley

$$\operatorname{Cdet} A = \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}$$

for an $n \times n$ matrix $A = (a_{ij})$ with the entries a_{ij} in an associative algebra $\mathcal{A}$ would have suited our purpose perfectly well had there been any reason to believe that this expression can be efficiently (in polynomial in n time) computed, see also Section 5.2.

The ambiguity that prevents the straightforward extension of the determinant to non-commutative algebras is that there is no natural choice for the order of the factors in the product $\prod_{i=1}^n a_{i\sigma(i)}$. We resolve this ambiguity by taking the average of the products in all possible $n!$ orders. Hence for an $n \times n$ matrix $A = (a_{ij})$ with the entries in an associative algebra $\mathcal{A}$ over a field $\mathbb{F}$ of characteristic 0, we write

$$\operatorname{sdet} A = \frac{1}{n!} \sum_{(\sigma,\tau) \in S_n \times S_n} (\operatorname{sgn} \sigma)(\operatorname{sgn} \tau) a_{\sigma(1)\tau(1)} \cdots a_{\sigma(n)\tau(n)}$$

("sdet" stands for the "symmetrized determinant"). It is easy to see that if $\mathcal{A}$ is commutative, we get the standard determinant. We prove that for any fixed finite-dimensional algebra $\mathcal{A}$, the value of sdet A for an $n \times n$ matrix over $\mathcal{A}$ can be computed in a polynomial in n time. More precisely, if the dimension of $\mathcal{A}$ as an $\mathbb{F}$-vector space is r, sdet A can be computed in $O(n^{r+3})$ time.

The paper is organized as follows. In Section 2, we discuss mixed discriminants, which are crucial for our proof in Section 3 of the polynomial time computability of the symmetrized determinant. In Section 4, for every finite-dimensional associative algebra $\mathcal{A}$ over $\mathbb{R}$ endowed with a scalar product and an unbiased probability distribution μ, we construct a permanent estimator which satisfies (1.2.1)–(1.2.4). In Section 4, we conjecture that if $\mathcal{A} = \operatorname{Mat}(d, \mathbb{R})$ is the algebra of $d \times d$ matrices endowed with the standard scalar product and Gaussian probability measure, then the algorithm approximates the permanent of an $n \times n$ matrix within a $O(\gamma_d^n)$ factor, where $\lim_{d \longrightarrow +\infty} \gamma_d = 1$. We also provide some intuitive argument supporting the conjecture.

2. Preliminaries: Mixed Discriminants

(2.1) Definition. Let $A_1, \ldots, A_n$ be $n \times n$ matrices over a field $\mathbb{F}$ of characteristic 0. We write $A_k = (a_{ij}^k)$, where $a_{ij}^k \in \mathbb{F}$ for $i, j = 1, \ldots, n$ and $k = 1, \ldots, n$ (k is the index, not the power). Let $t_1, \ldots, t_n \in \mathbb{F}$ be variables. The expression $\det\big(t_1 A_1 + \ldots + t_n A_n\big)$ is a homogeneous polynomial in $t_1, \ldots, t_n$ of degree n and its normalized coefficient

$$D(A_1, \ldots, A_n) = \frac{1}{n!} \frac{\partial^n}{\partial t_1 \ldots \partial t_n} \det\big(t_1 A_1 + \ldots + t_n A_n\big)$$

is called the *mixed discriminant* of $A_1, \ldots, A_n$. In terms of the entries (a_{ij}^k) of the matrices $A_1, \ldots, A_n$, the mixed discriminant can be written as

$$D(A_1, \ldots, A_n) = \frac{1}{n!} \sum_{(\sigma, \tau) \in S_n \times S_n} (\operatorname{sgn} \sigma)(\operatorname{sgn} \tau) \prod_{k=1}^{n} a_{\sigma(k)\tau(k)}^k. \tag{2.1.1}$$

Mixed discriminants are symmetric, that is,

$$D(A_1, \ldots, A_n) = D(A_{\phi(1)}, \ldots, A_{\phi(n)}) \tag{2.2}$$

for any permutation $\phi : \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\}$. For various properties of mixed discriminants, see, for example, Section 5.2 of [Bapat and Raghavan 97].

We are particularly interested in the situation when the number of different matrices among $A_1, \ldots, A_n$ is small. The following result is Lemma 9.3 from [Barvinok 97]. For the sake of completeness, we present its proof here.

(2.3) Lemma. *Let $k_1, \ldots, k_r$ be non-negative integers such that $k_1 + \ldots + k_r = n$ and let $A_1, \ldots, A_r$ be $n \times n$ matrices. Then*

$$D\big(\underbrace{A_1, \ldots, A_1}_{k_1 \text{ copies}}, \ldots, \underbrace{A_r, \ldots, A_r}_{k_r \text{ copies}}\big)$$
$$= \frac{(-1)^n}{n!} \sum_{\substack{0 \leq m_1 \leq k_1 \\ \ldots \\ 0 \leq m_r \leq k_r}} (-1)^{m_1 + \ldots + m_r} \binom{k_1}{m_1} \cdots \binom{k_r}{m_r} \det\big(m_1 A_1 + \ldots + m_r A_r\big).$$

Proof. For a subset $\omega \subset \{1, \ldots, n\}$, let

$$t_i(\omega) = \begin{cases} 1 & \text{if } i \in \omega \\ 0 & \text{if } \ i \notin \omega \end{cases}$$

and let $\mathbf{t}_\omega = \big(t_1(\omega), \ldots, t_n(\omega)\big)$ be the indicator of ω. One can observe that if p is a homogeneous polynomial of degree $n > 0$ in n variables $t_1, \ldots, t_n$, then

$$\frac{\partial^n}{\partial t_1 \cdots \partial t_n} p = (-1)^n \sum_{\omega \subset \{1, \ldots, n\}} (-1)^{|\omega|} p(\mathbf{t}_\omega).$$

Indeed, it suffices to check the identity for monomials $t_1^{\alpha_1} \cdots t_n^{\alpha_n}$. If some $\alpha_i = 0$ then the right hand side is 0 since the terms corresponding to $\omega \cup \{i\}$ and $\omega \setminus \{i\}$ annihilate each other. For the monomial $t_1 \cdots t_n$ the right hand side is 1 since the only non-zero term is for $\omega = \{1, \ldots, n\}$.

Given $n \times n$ matrices $A_1, \ldots, A_n$, let us apply the above identity to

$$p(t_1, \ldots, t_n) = \det(t_1 A_1 + \ldots + t_n A_n).$$

Suppose that the set $\{A_1, \ldots, A_n\}$ consists of k_1 copies of A_1, …, k_r copies of A_r, where $A_1, \ldots, A_r$ are distinct, and let $S_i = \big\{j : A_j \text{ is a copy of } A_i\big\}$ for $i = 1, \ldots, r$. Then $|S_i| = k_i$, $S_1 \cup \ldots \cup S_r$ is a partition of the set $\{1, \ldots, n\}$ and

$$p(\mathbf{t}_\omega) = \det(m_1 A_1 + \ldots + m_r A_r), \quad \text{where} \quad m_i = |\omega \cap S_i|.$$

Moreover, for given $m_1, \ldots, m_r$, there are exactly $\binom{k_1}{m_1} \cdots \binom{k_r}{m_r}$ subsets ω with $m_i = |\omega \cap S_i|$, since for each $i = 1, \ldots, r$, we have to choose m_i elements of ω from S_i for all $i = 1, \ldots, r$ independently. The proof now follows. $\square$

(2.4) Corollary. *Suppose that r is fixed. Given $n \times n$ matrices $A_1, \ldots, A_r$, computing*

$$D\big(\underbrace{A_1, \ldots, A_1}_{k_1 \text{ copies}}, \ldots, \underbrace{A_r, \ldots, A_r}_{k_r \text{ copies}}\big)$$

using the formula of Lemma 2.3, takes $O(n^{r+3})$ arithmetic operations.

Proof. The number of summands does not exceed $(n+1)^r$ (a better estimate is $(n/r+1)^r$) and the determinant of an $n \times n$ matrix can be computed using $O(n^3)$ arithmetic operations. $\square$

3. Symmetrized Determinant of a Matrix over an Algebra

Let $\mathcal{A}$ be an associative algebra over $\mathbb{F}$, where $\mathbb{F}$ is a field of characteristic 0. Hence $\mathcal{A}$ is a vector space over $\mathbb{F}$ with an addition "+" and associative (but not necessarily commutative) multiplication $\cdot$. For example, one can choose $\mathcal{A}$ to be the algebra $\mathrm{Mat}(d, \mathbb{F})$ of all $d \times d$ matrices over $\mathbb{F}$. We will assume that as a vector space, $\mathcal{A}$ is finite-dimensional, $\dim_{\mathbb{F}} \mathcal{A} < \infty$.

(3.1) Definition. Let $A=(a_{ij})$, $a_{ij}\in\mathcal{A}$ be an $n\times n$ matrix over $\mathcal{A}$. We call

$$\operatorname{sdet} A=\frac{1}{n!}\sum_{(\sigma,\tau)\in S_n\times S_n}(\operatorname{sgn}\sigma)(\operatorname{sgn}\tau)a_{\sigma(1)\tau(1)}a_{\sigma(2)\tau(2)}\cdots a_{\sigma(n)\tau(n)}$$

the *symmetrized determinant* of A. In other words, $\operatorname{sdet} A$ is obtained by taking a diagonal of A (that is, picking one entry from each row and column of A), multiplying the entries on the diagonal in all possible orders, taking the average of the resulting $n!$ products and adding that average with the appropriate sign found by the same rule as for the usual commutative determinant. Hence $\operatorname{sdet} A\in\mathcal{A}$. We denote by $\operatorname{Mat}(n,\mathcal{A})$ the set of $n\times n$ matrices $A=(a_{ij})$ with $a_{ij}\in\mathcal{A}$.

Remark. If $\mathcal{A}$ is commutative, the expressions

$$\frac{1}{n!}\sum_{(\sigma,\tau)\in S_n\times S_n}(\operatorname{sgn}\sigma)(\operatorname{sgn}\tau)a_{\sigma(1)\tau(1)}\cdots a_{\sigma(n)\tau(n)}$$

and

$$\sum_{\sigma\in S_n}(\operatorname{sgn}\sigma)a_{1\sigma(1)}\cdots a_{n\sigma(n)}$$

coincide but if $\mathcal{A}$ is not commutative, they may differ.

(3.2) Theorem. *Let $e_1,\dots,e_r$ span $\mathcal{A}$ as an $\mathbb{F}$-vector space. Let $A=(a_{ij})$ be an $n\times n$ matrix over $\mathcal{A}$, so*

$$A=A_1e_1+\ldots+A_re_r,$$

where $A_1,\dots,A_r$ are $n\times n$ matrices with the entries in $\mathbb{F}$.

For an r-tuple $k_1,\dots,k_r$ of non-negative integers such that $k_1+\ldots+k_r=n$, let $\Phi(k_1,\dots,k_r)$ be the set of all maps $\phi:\{1,\dots,n\}\longrightarrow\{1,\dots,r\}$ such that $|\phi^{-1}(1)|=k_1,\dots,|\phi^{-1}(r)|=k_r$. Let us define elements $u(k_1,\dots,k_r)\in\mathcal{A}$ by

$$u(k_1,\dots,k_r)=\sum_{\phi\in\Phi(k_1,\dots,k_r)}e_{\phi(1)}e_{\phi(2)}\cdots e_{\phi(n)}.$$

Then

$$\operatorname{sdet} A=\sum_{\substack{k_1,\dots,k_r\geq 0\\ k_1+\ldots+k_r=n}}D(\underbrace{A_1,\dots,A_1}_{k_1\text{ copies}},\dots,\underbrace{A_r,\dots,A_r}_{k_r\text{ copies}})u(k_1,\dots,k_r).$$

Proof. Let $A_k=(a_{ij}^k)$, where $a_{ij}^k\in\mathbb{F}$ for $i,j=1,\dots,n$ and $k=1,\dots,r$. Hence $a_{ij}=\sum_{k=1}^r a_{ij}^k e_k$.

By Definition 3.1,

$$\begin{aligned}\operatorname{sdet} A &= \frac{1}{n!}\sum_{(\sigma,\tau)\in S_n\times S_n} (\operatorname{sgn}\sigma)(\operatorname{sgn}\tau) a_{\sigma(1)\tau(1)}a_{\sigma(2)\tau(2)}\cdots a_{\sigma(n)\tau(n)}\\ &= \frac{1}{n!}\sum_{(\sigma,\tau)\in S_n\times S_n} (\operatorname{sgn}\sigma)(\operatorname{sgn}\tau)\Big(\sum_{k=1}^r a^k_{\sigma(1)\tau(1)}e_k\Big)\ldots\Big(\sum_{k=1}^r a^k_{\sigma(n)\tau(n)}e_k\Big)\end{aligned}$$

Let Φ be the set of all maps $\phi:\{1,\ldots,n\}\longrightarrow\{1,\ldots,r\}$. Then

$$\Big(\sum_{k=1}^r a^k_{\sigma(1)\tau(1)}e_k\Big)\cdots\Big(\sum_{k=1}^r a^k_{\sigma(n)\tau(n)}e_k\Big) = \sum_{\phi\in\Phi} a^{\phi(1)}_{\sigma(1)\tau(1)}\cdots a^{\phi(n)}_{\sigma(n)\tau(n)}e_{\phi(1)}\cdots e_{\phi(n)}.$$

Hence

$$\begin{aligned}\operatorname{sdet} A &= \frac{1}{n!}\sum_{(\sigma,\tau)\in S_n\times S_n} (\operatorname{sgn}\sigma)(\operatorname{sgn}\tau)\sum_{\phi\in\Phi} a^{\phi(1)}_{\sigma(1)\tau(1)}\cdots a^{\phi(n)}_{\sigma(n)\tau(n)}e_{\phi(1)}\cdots e_{\phi(n)}\\ &= \sum_{\phi\in\Phi}\frac{1}{n!}\sum_{(\sigma,\tau)\in S_n\times S_n} (\operatorname{sgn}\sigma)(\operatorname{sgn}\tau) a^{\phi(1)}_{\sigma(1)\tau(1)}\cdots a^{\phi(n)}_{\sigma(n)\tau(n)}e_{\phi(1)}\cdots e_{\phi(n)}\\ &= \sum_{\phi\in\Phi} D\big(A_{\phi(1)},\ldots,A_{\phi(n)}\big)e_{\phi(1)}\cdots e_{\phi(n)}.\end{aligned}$$

Now, set Φ is a disjoint union of the sets $\Phi(k_1,\ldots,k_r)$ and by the symmetry of the mixed discriminant (see (2.2)), for any $\phi\in\Phi(k_1,\ldots,k_r)$ we have

$$D(A_{\phi(1)},\ldots A_{\phi(n)}) = D\big(\underbrace{A_1,\ldots,A_1}_{k_1 \text{ copies}},\ldots,\underbrace{A_r,\ldots,A_r}_{k_r \text{ copies}}\big).$$

Summarizing, we get

$$\operatorname{sdet} A = \sum_{\substack{k_1,\ldots,k_r\geq 0\\ k_1+\ldots+k_r=n}} D\big(\underbrace{A_1,\ldots,A_1}_{k_1 \text{ copies}},\ldots,\underbrace{A_r,\ldots,A_r}_{k_r \text{ copies}}\big)\sum_{\phi\in\Phi(k_1,\ldots,k_r)} e_{\phi(1)}\cdots e_{\phi(n)}$$

and the proof follows. □

Next, we present an algorithm for computing the symmetrized determinant of a matrix over $\mathcal{A}$. We assume that there is a basis $e_1,\ldots,e_r$ of $\mathcal{A}$ as a vector space and that the entries a_{ij} of $A\in\operatorname{Mat}(n,\mathcal{A})$ are given by their coefficients in the basis: $a_{ij}=a^1_{ij}e_1+\ldots+a^r_{ij}e_r$. The multiplication in $\mathcal{A}$ is described by the structural constants $\{\beta^k_{ij}\}$ that are the scalars from $\mathbb{F}$ such that

$$e_ie_j=\sum_{k=1}^r \beta^k_{ij}e_k. \tag{3.3}$$

We need a simple Lemma.

(3.4) Lemma. *Let $u(k_1, \ldots, k_r) \in \mathcal{A}$ be the elements defined in Theorem 3.2. Let $I = \{i : k_i > 0\}$. Then*

$$u(k_1, \ldots, k_r) = \sum_{i \in I} u(k_1, \ldots, k_{i-1}, k_i - 1, k_{i+1}, \ldots, k_r) e_i.$$

Proof. For $\phi \in \Phi(k_1, \ldots, k_r)$ we have

$$e_{\phi(1)} \cdots e_{\phi(n)} = \Big(e_{\phi(1)} \cdots e_{\phi(n-1)} \Big) e_{\phi(n)}, \qquad \text{where} \quad \phi(n) \in I.$$

If $\phi(n) = i$ then the restriction $\phi' : \{1, \ldots, n-1\} \longrightarrow \{1, \ldots, r\}$ belongs to the set $\Phi(k_1, \ldots, k_{i-1}, k_i - 1, k_{i+1}, \ldots, k_r)$. Vice versa, every $\phi' \in \Phi(k_1, \ldots, k_{i-1}, k_i - 1, k_{i+1}, \ldots, k_r)$ extends to $\phi \in \Phi(k_1, \ldots, k_r)$ by letting $\phi(n) = i$. The proof now follows. □

(3.5) Algorithm for computing $\operatorname{sdet} A$ **for** $A \in \operatorname{Mat}(n, \mathcal{A})$

Input: An algebra $\mathcal{A}$ given by the structural constants $\{\beta_{ij}^k\}$ in some $\mathbb{F}$-basis $e_1, \ldots, e_r$ of $\mathcal{A}$ and an $n \times n$ matrix $A \in \operatorname{Mat}(n, \mathcal{A})$ given by $n \times n$ matrices $A_1, \ldots, A_r \in \operatorname{Mat}(n, \mathbb{F})$ such that $A = A_1 e_1 + \ldots + A_r e_r$.

Output: The element $\operatorname{sdet} A \in \mathcal{A}$ given by its coefficients in the basis $e_1, \ldots, e_r$.

Algorithm: First, for all r-tuples of non-negative integers $k_1, \ldots, k_r$ such that $k_1 + \ldots + k_r = n$, using the identity of Lemma 2.3, we compute the mixed discriminant

$$D\big(\underbrace{A_1, \ldots, A_1}_{k_1 \text{ copies}}, \ldots, \underbrace{A_r, \ldots, A_r}_{k_r \text{ copies}}\big).$$

Now, using Lemma 3.4 recursively, we compute $u(k_1, \ldots, k_r)$. We start with

$$u(0, \ldots, 0, \underset{i\text{-th position}}{1}, 0, \ldots, 0) = e_i$$

and applying Lemma 3.4 and (3.3), successively compute the expansions of $u(k_1, \ldots, k_r)$ with $k_1 + \ldots + k_r = 1, \ldots, n$ in the basis $e_1, \ldots, e_r$. Finally, we use Theorem 3.2 to compute $\operatorname{sdet} A$.

An important observation is that if $\dim_{\mathbb{F}} \mathcal{A} = r$ is fixed, the algorithm has polynomial time complexity.

(3.6) Theorem. *For a fixed r, given an $n \times n$ matrix $A \in \operatorname{Mat}(\mathcal{A}, n)$, Algorithm 3.5 computes $\operatorname{sdet} A \in \mathcal{A}$ using $O(n^{r+3})$ arithmetic operations.*

Proof. Theorem 3.2 and Lemma 3.4 imply that the algorithm indeed returns the correct value. The number of all r-tuples of non-negative integers $k_1, \ldots, k_r$ such that $k_1 + \ldots + k_r \leq n$ is $\binom{n+r}{r}$, which is a polynomial in n of degree r. The complexity bound follows from this and Corollary 2.4. □

4. Permanent Estimators

Let us fix an $\mathbb{R}$-algebra $\mathcal{A}$. We assume that as a real vector space, $\mathcal{A}$ is finite-dimensional, so as a vector space $\mathcal{A}$ is isomorphic to $\mathbb{R}^m$ for some m. Suppose that there is a scalar product $\langle \cdot, \cdot \rangle : \mathcal{A} \times \mathcal{A} \longrightarrow \mathbb{R}$. In other words, for every two elements $a, b \in \mathcal{A}$, a real number $\langle a, b \rangle$ is defined, such that

$\langle a, b \rangle = \langle b, a \rangle$;

$\langle \alpha a + \beta b, c \rangle = \alpha \langle a, c \rangle + \beta \langle b, c \rangle$ for $a, b, c \in \mathcal{A}$ and $\alpha, \beta \in \mathbb{R}$ and

$\langle a, a \rangle \geq 0$ for all $a \in \mathcal{A}$.

For example, if $\mathcal{A} = \mathrm{Mat}(d, \mathbb{R})$ is a matrix algebra, one may choose $\langle a, b \rangle = \mathrm{Tr}(ab^t)$. Generally, we don't assume any relation between the multiplication in $\mathcal{A}$ and the scalar product. We also allow the form $\langle \cdot, \cdot \rangle$ to be degenerate, that is, we allow $\langle a, a \rangle = 0$ for some non-zero a. As usual, we define $\|a\|^2 = \langle a, a \rangle$.

Suppose further, that there is a Borel probability measure μ on $\mathcal{A}$ with the properties:

$$\mathbf{E}\, x = \int_{\mathcal{A}} x \; d\mu = 0 \tag{4.1}$$

and for any (non-commutative) polynomial

$$p(x_1, \ldots, x_n) = \sum_{1 \leq i_1, \ldots, i_n \leq n} \gamma_{i_1, \ldots, i_n} x_{i_1} \cdots x_{i_n}, \quad \text{where} \quad \gamma_{i_1, \ldots, i_n} \in \mathbb{R}$$

we have

$$\mathbf{E}\, \langle p(x_1, \ldots, x_n), p(x_1, \ldots, x_n) \rangle < +\infty, \tag{4.2}$$

provided $x_1, \ldots, x_n \in \mathcal{A}$ are chosen independently and at random.

(4.3) Theorem. *Let $\mathcal{A}$ be an $\mathbb{R}$-algebra with a scalar product $\langle \cdot, \cdot \rangle$ and a probability measure μ satisfying (4.1)–(4.2). Let us define a constant $c(n, \mu) \geq 0$ as follows:*

$$c(n, \mu) = \mathbf{E}\, \|Z\|^2, \quad \textit{where} \quad Z = \frac{1}{n!} \sum_{\sigma \in S_n} Y_{\sigma(1)} \cdots Y_{\sigma(n)}$$

and $Y_1, \ldots, Y_n$ are sampled independently and at random from $\mathcal{A}$.

For a given real non-negative matrix $A = (a_{ij})$, let us define a random $n \times n$ matrix $B \in \mathrm{Mat}(n, \mathcal{A})$, $B = (b_{ij})$ as follows:

$$b_{ij} = \sqrt{a_{ij}} X_{ij},$$

where X_{ij} are sampled independently and at random from $\mathcal{A}$. Then

$$\mathbf{E}\, \|\operatorname{sdet} B\|^2 = c(n, \mu) \operatorname{per} A.$$

Proof. By Definition 3.1,

$$\operatorname{sdet} B = \frac{1}{n!} \sum_{(\sigma,\tau)\in S_n\times S_n} (\operatorname{sgn}\sigma)(\operatorname{sgn}\tau)\left(\prod_{i=1}^{n} a_{\sigma(i)\tau(i)}\right)^{1/2} X_{\sigma(1)\tau(1)}\cdots X_{\sigma(n)\tau(n)}.$$

Hence $\|\operatorname{sdet}(B)\|^2$ can be written as the sum of the terms

(4.3.1)

$$\left(\frac{1}{n!}\right)^2 (\operatorname{sgn}\sigma_1)(\operatorname{sgn}\tau_1)(\operatorname{sgn}\sigma_2)(\operatorname{sgn}\tau_2)\left(\prod_{i=1}^{n} a_{\sigma_1(i)\tau_1(i)}\right)^{1/2}\left(\prod_{i=1}^{n} a_{\sigma_2(i)\tau_2(i)}\right)^{1/2}\times$$
$$\left\langle X_{\sigma_1(1)\tau_1(1)}\cdots X_{\sigma_1(n)\tau_1(n)},\ X_{\sigma_2(1)\tau_2(1)}\cdots X_{\sigma_2(n)\tau_2(n)}\right\rangle$$

for all 4-tuples $(\sigma_1, \sigma_2, \tau_1, \tau_2) \in S_n \times S_n \times S_n \times S_n$.

Suppose that the sets of indices

$$\Big\{\big(\sigma_1(i), \tau_1(i)\big) : i = 1, \ldots, n\Big\} \quad \text{and} \quad \Big\{\big(\sigma_2(i), \tau_2(i)\big) : i = 1, \ldots, n\Big\}$$

coincide. This is the case if and only if there is a permutation $\pi \in S_n$ such that $\sigma_2(i) = \sigma_1(\pi(i))$ and $\tau_2(i) = \tau_1(\pi(i))$ for $i = 1, \ldots, n$, in which case the term (4.3.1) can be written as

$$\left(\frac{1}{n!}\right)^2 \prod_{i=1}^{n} a_{\sigma_1(i)\tau_1(i)}\times$$
$$\left\langle X_{\sigma_1(1)\tau_1(1)}\cdots X_{\sigma_1(n)\tau_1(n)},\ X_{\sigma_1(\pi(1))\tau_1(\pi(1))}\cdots X_{\sigma_1(\pi(n))\tau_1(\pi(n))}\right\rangle.$$

Let us fix $\sigma_1, \tau_1 \in S_n$ and let π range over S_n. Then the expected value of the corresponding sum of monomials is

$$\frac{c(n,\mu)}{n!} \prod_{i=1}^{n} a_{\sigma_1(i)\tau_1(i)}.$$

If the sets of indices

$$\Big\{\big(\sigma_1(i), \tau_1(i)\big) : i = 1, \ldots, n\Big\} \quad \text{and} \quad \Big\{\big(\sigma_2(i), \tau_2(i)\big) : i = 1, \ldots, n\Big\}$$

in (4.3.1) do not coincide, then there is a term X_{ij}, which is in the right hand side of the scalar product, but not in the left hand side. The conditional expectation with respect to X_{ij} is 0 because of (4.1) and the linearity of expectation. Hence the expectation of the corresponding term is 0. Summarizing, the expected value of $\|\operatorname{sdet} B\|^2$ is

$$\sum_{(\sigma_1,\tau_1)\in S_n\times S_n} \frac{c(n,\mu)}{n!}\prod_{i=1}^{n} a_{\sigma_1(i)\tau_1(i)} = c(n,\mu)\operatorname{per} A.$$

□

Algorithm 3.5 and Theorem 3.6 ensure the property (1.2.1) of the estimator. Theorem 4.3 implies (1.2.3) and (1.2.2) (up to a constant $c(n,\mu)$; for sufficiently generic measure and scalar product the constant is strictly positive). One can see that (1.2.4) is satisfied as well.

5. A Series of Estimators Conjectured to be Asymptotically Exact

Let us fix a positive integer d and let $\mathcal{A} = \operatorname{Mat}(d,\mathbb{R})$ be the algebra of real $d\times d$ matrices. We introduce the scalar product $\langle\cdot,\cdot\rangle$ on $\mathcal{A}$ by letting

$$\langle a,b\rangle = \operatorname{Tr}(ab^t).$$

Let μ be the standard Gaussian measure on $\mathcal{A}$ with the density

$$\psi(a) = (2\pi)^{-d^2/2}e^{-\|a\|^2/2}.$$

Thus to sample a random matrix $a\in\mathcal{A}$, we sample each of its d^2 entries independently from the standard normal distribution.

The construction of Section 4 gives us a permanent estimator. Although we don't know the value of $c(n,\mu)$, we don't really need it, since we can approximate it by applying the same algorithm to the identity matrix.

Hence, for each positive integer d, we obtain a permanent estimator.

(5.1) The d-th estimator.

Input: A non-negative $n\times n$ real matrix $A=(a_{ij})$.

Output: A non-negative number α approximating $\operatorname{per} A$.

Algorithm: Sample n^2 matrices u_{ij} of size $d\times d$ from the standard Gaussian distribution in $\operatorname{Mat}(d,\mathbb{R})$. Define $n\times n$ matrices $B=(b_{ij})$, $E=(e_{ij})$ with $b_{ij}, e_{ij}\in \operatorname{Mat}(d,\mathbb{R})$ for $i,j=1,\ldots,n$ as follows:

$$b_{ij} = u_{ij}\sqrt{a_{ij}} \quad\text{and}\quad e_{ij} = \begin{cases} u_{ii} & \text{if } i=j\\ 0 & \text{if } i\neq j.\end{cases}$$

Apply Algorithm 3.5 to compute $d\times d$ matrices $\operatorname{sdet} B$ and $\operatorname{sdet} E$. Compute

$$\alpha = \|\operatorname{sdet} B\|^2/\|\operatorname{sdet} E\|^2.$$

Output α.

We conjecture that the output α approximates per A within an exponential factor γ_d^n and that γ_d approaches 1 as d grows. More precisely, we conjecture that there exist

a sequence $\{\gamma_d\}$ of non-negative real numbers such that $\lim_{d\longrightarrow+\infty}\gamma_d = 1$

and

a sequence of functions $\{f_d(n,\epsilon)\}$ such that for any $\epsilon > 0$ and any d we have $\lim_{n\longrightarrow+\infty} f_d(n,\epsilon) = 0$;

so that for any $n\times n$ non-negative matrix A and any $\epsilon > 0$, the output α of the d-th estimator (5.1) satisfies:

$$\mathbf{P}\left\{(\gamma_d-\epsilon)^n \operatorname{per} A \le \alpha \le (\gamma_d+\epsilon)^n \operatorname{per} A\right\} \ge 1 - f_d(n,\epsilon).$$

Note, that the complexity of the d-th algorithm is $O(n^{d^2+3})$. We discuss some plausible reasons why the conjecture might be true.

(5.2) Why there might be sharp concentration.

From Theorem 4.3 and Chebyshev's inequality, one deduces that the value of $c^{-1}(n,\mu)\|\operatorname{sdet} B\|^2$ is unlikely to overestimate per A:

$$\mathbf{P}\left\{c^{-1}(n,\mu)\|\operatorname{sdet} B\|^2 \ge K \operatorname{per} A\right\} \le 1/K$$

for every $K > 0$. Hence the main problem is to prove that $c^{-1}(n,\mu)\|\operatorname{sdet} B\|^2$ is unlikely to underestimate per A as well.

Suppose that in Algorithm 5.1, instead of the symmetrized determinant of B, we take the Cayley determinant Cdet (see Section 1.3). One can prove that

$$\mathbf{E}\ \|\operatorname{Cdet} B\|^2 = d^n \operatorname{per} A$$

(see also [Friedland 00]). Moreover, the method of [Barvinok 99] carries over and one can prove that for any $1 > \epsilon > 0$

$$\mathbf{P}\left\{d^{-n}\|\operatorname{Cdet} B\|^2 \le (\epsilon\mathfrak{c}_d)^n \operatorname{per} A\right\} \le \frac{8}{n\ln^2\epsilon},$$

where constant $\mathfrak{c}_d$ is defined as follows (see [Barvinok 99]): let $\xi_1,\ldots,\xi_d$ be independent random variables having the standard Gaussian density $(2\pi)^{-1/2}e^{-x^2/2}$. Then

$$\mathfrak{c}_d = \exp\left\{\mathbf{E}\ \ln\Bigl(\frac{\xi_1^2+\ldots+\xi_d^2}{d}\Bigr)\right\}.$$

We have $\lim_{d\longrightarrow+\infty}\mathfrak{c}_d = 1$ and, in fact, $\mathfrak{c}_d = 1 + O(1/d)$.

The symmetrized determinant sdet B can be considered as the average of the $n!$ Cayley determinants of the matrices obtained from B by permuting rows in all possible ways. It seems quite plausible to the author that the concentration for $\|\operatorname{sdet} B\|^2$ should be at least as sharp as for $\|\operatorname{Cdet} B\|^2$.

Acknowledgment

I am grateful to Rishi Raj for many helpful discussions.

References

[Aslaksen 96] H. Aslaksen, Quaternionic determinants, *The Mathematical Intelligencer*, **18**(1996), 57–65.

[Bapat and Raghavan 97] R.B. Bapat and T.E.S. Raghavan, *Nonnegative Matrices and Applications*, Encyclopedia of Mathematics and its Applications, **64**, Cambridge Univ. Press, Cambridge, 1997.

[Barvinok 97] A. Barvinok, Computing mixed discriminants, mixed volumes, and permanents, *Discrete & Computational Geometry*, **18** (1997), 205–237.

[Barvinok 99] A. Barvinok, Polynomial time algorithms to approximate permanents and mixed discriminants within a simply exponential factor, *Random Structures & Algorithms*, **14**(1999), no. 1, 29–61.

[Friedland 00] S. Friedland, Radon-Hurwitz matrices and random algorithms to approximate permanents, *preprint*, 2000

[Gelfand and Retakh 97], I. Gelfand and V. Retakh, Quasideterminants. I. *Selecta Mathematica (N.S.)*, **3**(1997), 517–546.

[Girko 90] V.L. Girko, *Theory of Random Determinants*, Mathematics and its Applications, **45**, Kluwer, Dordrecht, 1990.

[Jerrum and Sinclair 89] M. Jerrum and A. Sinclair, Approximating the permanent, *SIAM Journal on Computing*, **18** (1989), 1149–1178.

[Karmarkar *et al.* 93] N. Karmarkar, R. Karp, R. Lipton, L. Lovász and M. Luby, A Monte Carlo algorithm for estimating the permanent, *SIAM Journal on Computing*, **22**(1993), 284–293.

[Linial *et al.* 98] N. Linial, A. Samorodnitsky and A. Wigderson, A deterministic strongly polynomial algorithm for matrix scaling and approximate permanents, *Proc. 30 ACM Symp. on Theory of Computing*, ACM, New York, 1998, 644–652; revised version is in *Combinatorica*, to appear.

[Lovász and Plummer 86] L. Lovász and M.D. Plummer, *Matching Theory*, North - Holland, Amsterdam - New York and Akadémiai Kiadó, Budapest, 1986.

[Papadimitriou 94] C.H. Papadimitriou, *Computational Complexity*, Addison-Wesley, Reading, Mass., 1994.

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109-1109
E-mail address: barvinok@math.lsa.umich.edu