1 Approximating the Permanent

Given an $n \times n$ matrix A, the determinant of A can be defined by the formula

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

where S_n is the group of all permutations of the integers $\{1, \ldots, n\}$, and $\mathrm{sgn}(\sigma) \in \pm 1$ is the sign of σ, which can be defined by writing σ as a product of cycles $\sigma = \prod_j C_j$ and setting

$$\mathrm{sgn}(\sigma) = \prod_j (-1)^{\mathrm{length}(C_j)-1}$$

For example, if σ maps $(1,2,3,4,5,6)$ to $(2,3,1,5,4,6)$, the cycle decomposition is $(231)(45)(6)$, and the sign is $\mathrm{sgn}(\sigma) = (-1)^{2+1} = -1$. In the following, we will need the fact that sgn is a group homomorphism onto $\mathbb{Z}_2$, so that $\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau)$ and $\mathrm{sgn}(\sigma) = \mathrm{sgn}(\sigma^{-1})$.

Note that even though we have defined the determinant as a sum of $n!$ terms, determinants may be calculated easily in polynomial time (for example, by Gaussian elimination). Also, it can be shown that the problems of inverting matrices, calculating determinants, and multiplying matrices each have the same asymptotic complexity (up to factors of $n^{o(1)}$), which is known to be between $\Omega(n^2)$ and $O(n^{2.4})$. It is more difficult, however, to calculate the permanent of a matrix, which we now define.

Definition 1 *The permanent of a matrix A is given by the formula*

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

Despite the apparent similarity between permanent and determinant, computing the permanent is known to be **#P** -complete even for $(0,1)$ matrices (Valiant). Therefore, instead of trying for an efficient polynomial method for computing permanents, we seek approximations. Recently, a FPRAS for matrix permanents with nonnegative entries was found by Jerrum, Sinclair and Vigoda. However, this algorithm is rather involved, so we will focus on an earlier approximation algorithm for $(0,1)$ matrices running in $O(3^{n/2}\mathrm{poly}(n))$ by Karmarkar, Karp, Lipton, Lovasz, and Luby. (Actually that paper presented a yet stronger runtime of $O(2^{n/2}\mathrm{poly}(n))$ but we won't show that today.) Before KKLLL, the fastest method, due to Ryser, ran in time $O(2^n n)$ and computed the permanent exactly; it's still the fastest method known for exact computation.

In what follows, A will be a $(0,1)$ matrix. Also, G_A will denote the bipartite graph on $n+n$ vertices with an edge (i,j) for every nonzero $a_{ij} \in A$. Note that $\mathrm{per}(A)$ is exactly the number of perfect matchings in G_A.

The algorithm is based on the following observation by Godsil and Gutman. Construct a random matrix B by replacing each 1 in A by an independent uniform choice of ± 1. Then $\det(B)^2$ is actually an unbiased estimator of $\mathrm{per}(A)$.

Theorem 2 $\mathrm{per}(A) = \mathrm{E}(\det(B)^2)$

Proof : For convenience, will define $B_\sigma = \prod_{i=1}^{n} b_{i,\sigma(i)}$. Also, let $P(A) = \{\sigma : a_{i,\sigma(i)} = 1 \ \forall i\}$. We have

$$\begin{aligned}
\mathrm{E}(\det(B)^2) &= \sum_{\sigma_1,\sigma_2 \in P(A)} \mathrm{sgn}(\sigma_1)\mathrm{sgn}(\sigma_2)\mathrm{E}(B_{\sigma_1} B_{\sigma_2}) \\
&= \sum_{\sigma \in P(A)} \mathrm{sgn}(\sigma)^2 B_\sigma^2 + \sum_{\sigma_1 \neq \sigma_2} \mathrm{sgn}(\sigma_1)\mathrm{sgn}(\sigma_2)\mathrm{E}(B_{\sigma_1} B_{\sigma_2})
\end{aligned}$$

The first term is just $\mathrm{per}(A)$ since $(\pm 1)^2 = 1$. For the second term, let $\sigma_1, \sigma_2 \in P(A)$, $\sigma_1 \neq \sigma_2$. Choose i s.t. $\sigma_1(i) \neq \sigma_2(i)$. Since entries of B are independent, we have

$$\mathrm{E}(B_{\sigma_1} B_{\sigma_2}) = \mathrm{E}(b_{i,\sigma_1(i)})\mathrm{E}(\cdots) = 0$$

and the second term vanishes. $\square$

Since $\det(B)^2$ can be computed in polynomial time, we can use this to approximate $\mathrm{per}(A)$ if the variance is not too large. Specifically, if we let $Y = \det(B)^2$, we must bound the critical ratio $\mathrm{E}(Y^2)/\mathrm{E}(Y)^2$.

Let $\mathcal{G}_A$ be the set of subgraphs of G_A which are the disjoint union of a matching and a 2-regular graph (several disjoint cycles). We will denote by $\mathrm{cyc}(H)$ the number of cycles for a given $H \in \mathcal{G}_A$.

Claim 3 $\mathrm{E}(Y)^2 = \sum_{H \in \mathcal{G}_A} 2^{\mathrm{cyc}(H)}$

Proof : We know $\mathrm{E}(Y) = \mathrm{per}(A)$, so

$$\mathrm{E}(Y)^2 = \sum_{\sigma_1,\sigma_2 \in P(A)} 1$$

Given $\sigma_1, \sigma_2 \in P(A)$, let the graph $G(\sigma_1, \sigma_2)$ be the union of the matchings corresponding to σ_1 and σ_2. Then $G(\sigma_1, \sigma_2) \in \mathcal{G}_A$ since the graph is a matching on those points where σ_1 and σ_2 agree, and a 2-regular graph elsewhere. Conversely, given $H \in \mathcal{G}_A$, there are $2^{\mathrm{cyc}(H)}$ pairs (σ_1, σ_2) that produce H. To see this, note that the values of σ_i are forced on the matching, and once a single edge in a cycle is chosen to belong to σ_1 or σ_2, all other edges in the cycle are forced in alternating order. Thus

$$\mathrm{E}(Y)^2 = \sum_{H \in \mathcal{G}_A} 2^{\mathrm{cyc}(H)}$$

$\square$

Therefore, if we can write $\mathrm{E}(Y^2)$ in terms of a similar sum over $\mathcal{G}_A$, we will have our bound on the critical ratio.

Theorem 4 $\mathrm{E}(Y^2) = \sum_{H \in \mathcal{G}_A} 6^{\mathrm{cyc}(H)}$

Proof : Since $Y = \det(A)^4$, we get

$$\mathrm{E}(Y^2) = \sum_{\sigma_1,\sigma_2,\sigma_3,\sigma_4 \in P(A)} \mathrm{sgn}(\sigma_1\sigma_2\sigma_3\sigma_4)\mathrm{E}(B_{\sigma_1} B_{\sigma_2} B_{\sigma_3} B_{\sigma_4})$$

Note that if a variable b_{ij} occurs an odd number of times in $B_{\sigma_1} B_{\sigma_2} B_{\sigma_3} B_{\sigma_4}$, then the expectation of this term will vanish, since $\mathrm{E}(b_{ij}^{2k+1}) = 0$. If all b_{ij}'s occur an even number of times, $B_{\sigma_1} B_{\sigma_2} B_{\sigma_3} B_{\sigma_4} = 1$. We will call $(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ an even 4-tuple if all b_{ij}'s occur with even powers. This allows us to write

$$\mathrm{E}(Y^2) = \sum_{\substack{\sigma_1,\sigma_2,\sigma_3,\sigma_4 \in P(A) \\ \text{even } 4-\text{tuple}}} \mathrm{sgn}(\sigma_1\sigma_2\sigma_3\sigma_4)$$

Let $G(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ be the union of the matchings corresponding to the σ_i. Since $(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ is an even 4-tuple, each edge in $G(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ comes from either 2 or 4 σ_i's. Thus $G(\sigma_1, \sigma_2, \sigma_3, \sigma_4) \in \mathcal{G}_A$. If we label each edge with the set of indices in $\{1, 2, 3, 4\}$ corresponding to it, the labeled graph uniquely determines the even 4-tuple. Since the labels alternate around cycles, each labeling is uniquely determined by the choice of label for one edge in each cycle, and the total number of labelings corresponding to a graph H is

$$\binom{4}{2}^{\mathrm{cyc}(H)} = 6^{\mathrm{cyc}(H)}$$

Finally, we claim that the sign term $\mathrm{sgn}(\sigma_1\sigma_2\sigma_3\sigma_4)$ is 1 for all even 4-tuples.

To see this, let $\tau = \sigma_1^{-1}\sigma_2\sigma_3^{-1}\sigma_4$ (composing functionally, i.e., starting from the right). By our earlier comments, $\mathrm{sgn}(\tau) = \mathrm{sgn}(\sigma_1\sigma_2\sigma_3\sigma_4)$. Let v be a vertex on the LHS of $G(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$. (I.e., an element of $\{1, ..., n\}$ acted on by these permutations.)

If v is part of a matching edge, then $\tau(v) = v$ and so v is in a cycle of length 1 in τ, which contributes a factor of $+1$ to $\mathrm{sgn}(\tau)$.

If v is part of a cycle, then there are two cases to be considered. If v is part of a cycle with edges are labeled "12"/"34", then $\tau(v) = v$ and, again, v is in a cycle of length 1 in τ, which contributes a factor of $+1$ to $\mathrm{sgn}(\tau)$. If v is part of a cycle with edges labeled "13"/"24" or "14"/"23", then let $\rho = \sigma_3^{-1}\sigma_4$, and note that $\tau(v) = \rho^2(v)$. If v and $\rho(v)$ belong to different cycles in τ then those two cycles evenly split the elements of one cycle of ρ, hence in combination they contribute a factor of $+1$ to $\mathrm{sgn}(\tau)$. If v and $\rho(v)$ belong to the same cycle in τ then there is some k such that $\rho(v) = \tau^k(v) = \rho^{2k}(v)$, so the cycle is of odd length, hence it contributes a factor of $+1$ to $\mathrm{sgn}(\tau)$.

Since each even 4-tuple contributes 1 to $\mathrm{E}(Y^2)$, and there are $6^{\mathrm{cyc}(H)}$ even 4-tuples corresponding to each $H \in \mathcal{G}_A$,

$$\mathrm{E}(Y^2) = \sum_{H \in \mathcal{G}_A} 6^{\mathrm{cyc}(H)}$$

□

We can now bound the critical ratio as follows:

$$\frac{\mathrm{E}(Y^2)}{\mathrm{E}(Y)^2} = \frac{\sum_{H \in \mathcal{G}_A} 6^{\mathrm{cyc}(H)}}{\sum_{H \in \mathcal{G}_A} 2^{\mathrm{cyc}(H)}} \leq \max_{H \in \mathcal{G}_A} 3^{\mathrm{cyc}(H)}$$

Since each cycle contains at least 2 vertices on each side of the bipartite graph, $\mathrm{cyc}(H) \leq n/2$, and $\mathrm{E}(Y^2)/\mathrm{E}(Y)^2 \leq 3^{n/2}$. Therefore, by iteratively sampling the random variable Y, we can produce a $(1+\epsilon)$-approximation to the permanent in time $O(3^{n/2}\mathrm{poly}(n, 1/\epsilon))$.

The exponent in this technique can be reduced by sampling from the complex units $\{\pm 1, \pm i\}$ (KKLLL), or the quaternions (Barvinok). In fact, the critical ratio can be reduced all the way to a constant by using a sufficiently high-dimensional Clifford algebra, a generalization of the complex numbers and quaternions (Chien, Rasmussen and Sinclair). However, Clifford algebras are non-commutative, and there is no known polynomial time algorithm for evaluating such determinants, so this does not translate into a FPRAS. (The known FPRAS for the permanent uses a different method.)