**CSE431: Complexity Theory** March 1, 2023

# Homework 4

*Anup Rao* Due: March 10, 2023

Read the fine print[1]. Each problem is worth 10 points:

1. Consider the following algorithm for computing the permanent. Recall that the permanent is defined as:

$$\mathsf{perm}(M) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} M_{i\sigma(i)}.$$

The formula for the permanent looks very similar to the formula for the determinant (for which we do have polynomial time algorithms):

$$\det(M) = \sum_{\sigma \in S_n} \mathsf{sign}(\sigma) \prod_{i=1}^{n} M_{i\sigma(i)}.$$

Here $\mathsf{sign}(\sigma)$ is either 1 or $-1$. This motivates the following randomized algorithm. Given the matrix $M$, let us sample the matrix $A$ randomly as follows:

$$A_{ij} = \begin{cases} -\sqrt{M_{ij}} & \text{with probability } 1/2, \\ \sqrt{M_{ij}} & \text{with probability } 1/2. \end{cases}$$

All entries are sampled independently. (Note that $A_{ij}$ may be a complex number if $M_{ij}$ is negative).

The algorithm is to just output $\det(A)^2$, which can be computed in polynomial time. Show that the expected value of the output of this algorithm is the same as the permanent. Hint: Use linearity of expectation to expand the expression for the output of the algorithm. Argue that the only terms in the expansion that have non-zero expectation correspond to the monomials of the permanent.

Does this algorithm prove that computing whether or not $\mathsf{perm}(M) > 0$ is in **BPP**? Discuss the consequences of finding a randomized algorithm in **BPP** for determining whether $\mathsf{perm}(M) > 0$? What would that imply about the relationship between the complexity classes **BPP**, **NP** and the functions computable by polynomial sized circuits?

[1] In solving the problem sets, you are allowed to collaborate with fellow students taking the class, but **each submission can have at most one author**. If you do collaborate in any way, you must acknowledge, for each problem, the people you worked with on that problem. The problems have been carefully chosen for their pedagogical value, and hence might be similar to those given in past offerings of this course at UW, or similar to other courses at other schools. Using any pre-existing solutions from these sources, for from the web, constitutes a violation of the academic integrity you are expected to exemplify, and is strictly prohibited. Most of the problems only require one or two key ideas for their solution. It will help you a lot to spell out these main ideas so that you can get most of the credit for a problem even if you err on the finer details. Please justify all answers. Some other guidelines for writing good solutions are here: `http://www.cs.washington.edu/education/courses/cse421/08wi/guidelines.pdf`.

**Solution:** We have

$$\begin{aligned}
\mathbb{E}\left[\det(A)^2\right] &= \mathbb{E}\left[\Big(\sum_{\sigma\in S_n} \mathsf{sign}(\sigma)\prod_{i=1}^{n} A_{i\sigma(i)}\Big)^2\right] \\
&= \mathbb{E}\left[\sum_{\sigma,\sigma'\in S_n} \mathsf{sign}(\sigma)\mathsf{sign}(\sigma')\prod_{i=1}^{n} A_{i\sigma(i)}A_{i\sigma'(i)}\right] \\
&= \mathbb{E}\left[\sum_{\sigma\in S_n}\prod_{i=1}^{n} A^2_{i\sigma(i)}\right] + \mathbb{E}\left[\sum_{\sigma\neq\sigma'\in S_n}\prod_{i=1}^{n} \mathsf{sign}(\sigma)\mathsf{sign}(\sigma')A_{i\sigma(i)}A_{i\sigma'(i)}\right],
\end{aligned}$$

where here we separated the contributions of the pairs of the permutations where both permutations were the same. Now, since $A^2_{i,\sigma(i)} = M_{i,\sigma(i)}$, the first expectation is the same as the permanent!

We claim that the second expectation is 0. To see this observe that for each pair $\sigma, \sigma'$ with $\sigma \neq \sigma'$, there must be some coordinate $i$ such that $\sigma(j) \neq \sigma'(j)$. So, for a fixed $\sigma \neq \sigma'$, we can write:

$$\begin{aligned}
&\mathbb{E}\left[\prod_{i=1}^{n} \mathsf{sign}(\sigma)\mathsf{sign}(\sigma')A_{i\sigma(i)}A_{i\sigma'(i)}\right] \\
&= \mathbb{E}\left[\prod_{i\neq j}^{n} \mathsf{sign}(\sigma)\mathsf{sign}(\sigma')A_{i\sigma(i)}A_{i\sigma'(i)}\right]\mathbb{E}\left[A_{j\sigma(j)}A_{j\sigma'(j)}\right] \\
&= \mathbb{E}\left[\prod_{i\neq j}^{n} \mathsf{sign}(\sigma)\mathsf{sign}(\sigma')A_{i\sigma(i)}A_{i\sigma'(i)}\right]\mathbb{E}\left[A_{j\sigma(j)}\right]\mathbb{E}\left[A_{j\sigma'(j)}\right] \\
&= 0,
\end{aligned}$$

because the expect value of a product of independent variables is the same the product of the expected values. This shows that the overall expected value of the squared determinant of $A$ is equal to the permanent of $M$.

What does consequence does this have for complexity classes? Well, none, because this is not actually an efficient randomized algorithm. It may well be that the expected value is 10, but with very high probability the determinant is 0, so we get no information about the permanent from carrying out this calculation. If the permanent was in **BPP**, then we would obtain a randomized algorithm for all of **NP** which would be very interesting: it would show **BPP** $\subseteq$ **NP**.

2. Use Gaussian-Elimination to describe an arithmetic circuit of size $O(n^3)$ for computing the determinant of an $n \times n$ matrix.

   **Solution**: Skipped.

3. In class we defined an artithmetic circuit to be one that has + and $\times$ gates. Here we discuss the case where / (division) gates are allowed, and the field is the real numbers. If there are / gates, then the output of the circuit can be viewed as $p(X)/q(X)$, where $p, q$ are polynomials.

(a) Show that if there is a polynomial sized circuit computing $p(X)/q(X)$, then there is a polynomial sized circuit that simultaneously computes both $p(X)$ and $q(X)$, without using any division gates.

**Solution**: We prove this by induction on $s$, the size of the circuit. For every gate $f$ of the circuit that uses division gates, we shall make two gates in our new circuit: $g$, $h$, such that $f(X) = g(X)/h(X)$. If $f$ is an input or constant, set $g = f$, $h = 1$.

If $f$ is a multiplication gate with $f = f_1 \cdot f_2$, then by induction we have already made $g_1, g_2, h_1, h_2$ such that $f_1(X) = g_1(X)/h_1(X)$ and $f_2(X) = g_2(X)/h_2(X)$. Then we compute $g = g_1 g_2$, $h = h_1 h_2$, which gives $f = g/h$.

If $f$ is an addition gate with $f = f_1 + f_2$, then we compute $h = h_1 h_2$, and $g = g_1 h_2 + g_2 h_1$.

If $f$ is a division gate with $f = f_1/f_2$, we compute $g = g_1 h_2$, $h = g_2 h_1$.

In all three cases, we see that we only need a constant number of gates to carry out the computation of a single gate. So, our final circuit will be of size $O(s)$.

(b) Suppose the original circuit computes a polynomial $f(X) = p(X)/q(X)$, so $q(X)$ is promised to divide $p(X)$. Assume that $f(X)$ is of degree $n$. Show that you can use the result of the previous step to compute $f(X)$ without division. To do this, observe that if $q(0) = 1$, then $(1 - q(X))$ and has no constant term, and we have

$$\frac{p(X)}{q(X)} = \frac{p(X)}{1 - (1 - q(X))} = \sum_{i=0}^{\infty} p(X) \cdot (1 - q(X))^i,$$

and so the degree $d$ homogenous part of $f(X)$ can be computed from this expression. Since $q(X)$ is not 0, there must be an input $x$ for which $q(x) \neq 0$. Use this input (translate and scale the polynomials) and the above observations to compute $f$ without any division gates.

**Solution**: Skipped.