TU Dresden, Fakultät Informatik
Daniel Borchmann

Summer Term 2016

Advanced Topics in Complexity Theory

Exercise 8: An Interactive Protocol for the Permanent[1]

2016-06-14

The goal of this exercise is to discuss an interactive proof systems for the permanent. For this we shall make use of *downward self-reducibility* of the permanent: for computing the permanent of a matrix $A \in \mathbb{Z}^{n \times n}$, it is enough to be able to compute the permanent of smaller matrices. More precisely, we have the following fact.

Exercise 8.1 Show that

$$\operatorname{perm}(A) = \sum_{i=1}^{n} a_{1i} \cdot \operatorname{perm}(A_{1,i}),$$

where $A = (a_{ij})$ and $A_{1,i}$ is the submatrix of A that results from A by removing the first row and the i-th column of A.

Let $p \in \mathbb{N}$ be prime such that $p > n$ and let $\mathbb{F}_p = \mathrm{GF}(p)$. For $i \in \{1, \dots, n\}$ define $D_A(i) = A_{1,i}$. Define the polynomial $p_{jk}(x)$ to be the unique polynomial of degree at most $n-1$ such that

$$p_{jk}(i) = (D_A(i))_{jk}.$$

Finally, define $D_A(x) = (p_{jk}(x))$.

Exercise 8.2 Compute $D_A(x)$ (over $\mathbb{Q}$) for the matrix

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Exercise 8.3 Argue that $\operatorname{perm}(D_A(x))$ is a univariate polynomial degree at most $(n-1)^2$.

Define the language

$$L_{\text{perm}} = \{ \langle A, p, k \rangle \mid p > n^4 \text{ prime and } \operatorname{perm}(A) = k \}.$$

We want to show that $L_{\text{perm}} \in \mathsf{IP}$. We use the following recursive protocol for this: for $n = 1$, computing the permanent is trivial. For $n > 1$, we conduct the following interaction:

- The prover sends to the verifier a polynomial $g(x)$ of degree $(n-1)^2$, which is supposedly $\operatorname{perm}(D_A(x))$.

[1] This exercise is based on Sanjeev Arora and Boaz Barak: *Computational Complexity A Modern Approach*, Cambridge University Press, 2009, Section 8.7.

- Check whether

  $$k = \sum_{i=1}^{n} a_{1,i} g(i).$$

  If this check fails, *reject.* Otherwise, uniformly pick some $b \in \mathbb{F}_p$ and ask the prover to show $g(b) = \mathrm{perm}(D_A(b))$.

Exercise 8.4 Show that the protocol is correct. More precisely, show that

1. if $\mathrm{perm}(A) = k$, the prover can make the verifier accept with probability 1;

2. if $\mathrm{perm}(A) \neq k$, the prover can make the verifier accept with probability less than $1/2$. For this assume inductively that we are given an interactive proof systems for matrices of size $(n-1) \times (n-1)$ with soundness ε. Show that then the above protocol yields an interactive proof systems with soundness $\varepsilon + \frac{(n-1)^2}{p}$. Conclude that the overall soundness of the protocol is at most $\frac{n^3}{p} \leq \frac{1}{2}$.