LAST TUTORIAL ON RANDOMIZED ALGORITHMS

Interactive protocols and probabilistically checkable proofs

1. *Are provers or proofs more powerful?.* What is the relation between IP and PCP[poly(n), poly(n)]? Try to guess first. Showing one inclusion is enough (it is conjectured that the inclusion is strict).

2. *Class IP.*

a) Show that NP $\subseteq$ IP
b) Show that if the definition of IP is adjusted so that the probability of error is zero, then the resulting class equals NP.
c) Show that co-RP $\subseteq$ IP
d) Bonus: Show that IP $\subseteq$ PSPACE. (Extra bonus: PSPACE $\subseteq$ IP — ask for hint for that.)

3. *PCP classes.*

a) Show that P = PCP[0, 0]
b) Show that NP = PCP[0, poly(n)]
c) Show that co-RP = PCP[poly(n), 0]
d) Show that PCP[log(n), poly(n)] $\subseteq NP$ (in fact, these classes are equal)

4. *PCP and adaptive queries.* Show that as long as there are only $O(1)$ queries on the proof, the class PCP[$r(n), O(1)$] remains the same no matter whether the queries are adaptive or need to be chosen non-adaptively (only based on the input and the random bits but not on the results of previous queries).

5. *Polynomial-time interactive protocol for permanent.* Show that permanent is in IP — that is, the decision problem whether or not $\text{perm}(A) = k$ for a given matrix $A \in \{0,1\}^{n \times n}$ and $k \in \mathbb{N}$ is in IP.

A sketch of the protocol follows — your task is to prove that it works and fill in the details.

Denote $M^{1,i}$ the matrix M without the first row and i-th column. Denote $D(x)$ the matrix $(n-1) \times (n-1)$ where elements are polynomials of degree n such that $\forall i \in [n]\colon D(i) = A^{1,i}$. Then permanent of $D(x)$ is a polynomial of degree $n(n-1)$ in variable x.

Notice that:

- We can construct $D(x)$ using interpolation.
- $\text{perm}(M) = \sum_{i=1}^{n} M_{1,i} \cdot \text{perm}(M^{1,i})$
- $\text{perm}(M) \leq n! \leq 2^{n^2}$

The protocol:

- If $n \leq 2$ check the answer.
- Let the prover generate a prime p such that $2^{n^2} < p < 2^{2n^2}$ and check that it is really a prime.
- Request polynomial $g \in \mathbb{Z}_p[x]$ of degree at most n^2 such that $g(x) = \text{perm}(D(x))$. Check $k = \sum_{i=1}^{n} M_{1,i} \cdot \text{perm}(D(i))$.
- Pick $a \in \mathbb{Z}_p$ uniformly at random and recursively check that $\text{perm}(D(a)) = g(a)$.

Observe that if $g(x) \neq \text{perm}(D(x))$ then $\Pr_{a \in \mathbb{Z}_p}[g(a) = \text{perm}(D(a))] \leq n^2/p$.