Probabilistically Checkable Proofs Spring 2008

Exercise no. 1

Due: March 5th, 2008

Recall that $PCP_{c,s}[r,q]_\Sigma$ is the class of all decision problems that have a probabilistically checkable proof in which the verifier uses r random bits to choose q queries in a proof over alphabet Σ and achieves completeness c and soundness s. We use n to denote the input size.

1. **Soundness amplification.** Show that for every $0 < \epsilon < 1$,

$$PCP_{\frac{2}{3},\frac{1}{3}}[r,q]_\Sigma \subseteq PCP_{1-\epsilon,\epsilon}[O(r \cdot \log \frac{1}{\epsilon}), O(q \cdot \log \frac{1}{\epsilon})]_\Sigma$$

2. **Alphabet size vs. query complexity.** Show the following:

   (a) *From large alphabet to binary alphabet:* $PCP_{c,s}[r,q]_\Sigma \subseteq PCP_{c,s}[r, q \cdot \log|\Sigma|]_{\{0,1\}}$.

   (b) *From many queries to two queries:* $PCP_{1,s}[r,q]_{\{0,1\}} \subseteq PCP_{1,1-\frac{1}{q}+\frac{s}{q}}[r + \log q, 2]_{\{0,1\}^q}$. (Note the deterioration in the soundness!)

3. **Lower bounds.**

   (a) *Lower bound on query complexity:* Show that for $|\Sigma| \leq \text{poly}n$, $PCP_{c,s}[O(\log n), 1]_\Sigma \subseteq P$.

   (b) *Lower bound on soundness:* Show that for $|\Sigma|^q \leq \text{poly}n$, $PCP_{1,(\frac{1}{|\Sigma|})^q}[O(\log n), q]_\Sigma \subseteq P$.

4. **Hardness of approximation.** Show that it is NP-hard to approximate Clique to within some constant $c > 0$ assuming the PCP Theorem, namely, $NP \subseteq PCP_{1,\frac{1}{2}}[O(\log n), O(1)]_{\{0,1\}}$.

5. **Zero testing.** Let $\mathbb{F}$ be a finite field with more than two elements. Let $\mathbb{F}_d[x_1,\ldots,x_n]$ denote the set of polynomials of degree at most d over variables $x_1,\ldots,x_n$ taking values in $\mathbb{F}$.

   Devise an efficient algorithm that given a set of polynomials $p_1,\ldots,p_m \in \mathbb{F}_d[x_1,\ldots,x_n]$ generates a set of polynomials $q_1,\ldots,q_{m'} \in \mathbb{F}_d[x_1,\ldots,x_n]$ satisfying the following:

   - *Completeness:* If there is an assignment $\rho : \{x_1,\ldots,x_n\} \to \mathbb{F}$, such that for every $1 \leq i \leq m$ it holds that $p_i(\rho(x_1),\ldots,\rho(x_n)) = 0$, then for every $1 \leq i \leq m'$ it holds that $q_i(\rho(x_1),\ldots,\rho(x_n)) = 0$.
   - *Soundness:* If for every assignment $\rho : \{x_1,\ldots,x_n\} \to \mathbb{F}$ there is $1 \leq i \leq m$ such that $p_i(\rho(x_1),\ldots,\rho(x_n)) \neq 0$, then for every assignment $\rho : \{x_1,\ldots,x_n\} \to \mathbb{F}$ for at least $\frac{1}{2}$ of the $1 \leq i \leq m'$ it holds that $q_i(\rho(x_1),\ldots,\rho(x_n)) \neq 0$.

   Use the following fact (*explicit linear code*): one can efficiently construct a matrix $A = (a_{ij})_{m' \times m}$ over the field such that for every $\vec{x} \neq \vec{0} \in \mathbb{F}^m$ it holds that $(A\vec{x})_i \neq 0$ for at least half of the $1 \leq i \leq m'$.