Advanced Topics in Complexity – Ex. 2

Due date: 19.5.02

Question 1

Let $M$ be a Boolean matrix and $C(M)$ be the minimal number of rectangles in a monochromatic cover of $M$. Prove that $\text{rank}(M) \leq C(M) \log C(M)$.

Hint: Use the connection between deterministic and non-deterministic communication complexity.

Question 2

Part 1. Let $f : \{0, 1\}^n \times \{0, 1\}^n \to \{0, 1\}$ be a function such that for some $\alpha > 0$ and for every rectangle $R$:

$$\text{BIAS}(R, f) \leq \alpha 2^{0.5n} \sqrt{|R|}.$$ 

Prove that $D_{\epsilon}(f) \geq n - \log \frac{1}{1-2\epsilon} - \log \alpha$.

Hint: You can use the fact that for every non-negative numbers $s_1, \ldots, s_t$ if $\sum_{i=1}^t s_i \leq s$ then $\sum_{i=1}^t \sqrt{s_i} \leq \sqrt{st}$.

Part 2. Prove that $R_{\epsilon}(\text{IP}) \geq n - \log \frac{1}{1-2\epsilon} - O(1)$.

Part 3. Prove that for most functions $f : \{0, 1\}^n \times \{0, 1\}^n \to \{1, -1\}$ it holds that $R_{\epsilon}(f) \geq n - \log \frac{1}{1-2\epsilon} - O(1)$.

Hint: Pick $f$ at random with uniform distribution, that is, for every $x, y$ pick every value $f(x, y)$ independently such that $\Pr[f(x, y) = 1] = \Pr[f(x, y) = -1] = 1/2$.

Question 3

A Las-Vegas protocol for $f$ with error $\epsilon$ is a protocol such that for every $x, y$:

- The protocol outputs the value $f(x, y)$ with probability at least $1 - \epsilon$.
- The protocol never outputs the value $1 - f(x, y)$, however the protocol might return the value “don’t know.”

The complexity of the protocol is the maximum complexity over all choices of $x, y$ and the random inputs. Define $Z_{\epsilon}(f)$ as the minimum complexity of a Las-Vegas protocol for $f$ with error $\epsilon$. Similarly, $Z_{\epsilon}^{\text{pub}}(f)$ is the minimum complexity of a Las-Vegas protocol with public random coins for $f$ with error $\epsilon$.

Part 1. Prove that $N(f) \leq Z_{\epsilon}(f) \leq D(f)$.

Part 2. Prove that $Z_{\epsilon}(f) = \Theta(R_{\epsilon}^1(f) + R_{\epsilon}^1(\overline{f}))$.

Part 3. Prove that $Z_{\epsilon+\delta}(f) = O(Z_{\epsilon}^{\text{pub}}(f) + \log n + \log \frac{1}{\delta})$. 
Question 4

In the lecture we proved that there is a randomized protocol for GT with complexity $O(\log n \log \log n)$. However, this proof was not constructive (since we used the transformation from the public coin model). In this question you will show how to construct such a protocol.

An $(\ell, k, d)$ error correcting code over alphabet $\Sigma$ is a mapping $E : \{0, 1\}^k \rightarrow \Sigma^\ell$ such that for every $x \neq y$ it holds that $E(x)_i \neq E(y)_i$ for at least $d$ values of $i$ (where $E(x)_i$ is the $i$th coordinate of $E(x)$).

Part 1. Prove that there exists an explicit $(n, \log n, n/2)$ error correcting code $E_1$ with alphabet $\{0, 1\}$.

Hint: You can use the fact that $\Pr_r[\text{IP}(X, r) = \text{IP}(y, r)] = 1/2$ for every $x, y \in \{0, 1\}^{\log n}$.

Part 2. Prove that there exists an explicit $(2n, n, n/2)$ error correcting code $E_2$ with alphabet $\mathbb{Z}_p$, where $p \approx 2n$.

Hint: Use polynomials over $\mathbb{Z}_p$ as described in the protocol for EQ.

Part 3. Prove that there exists an explicit $(\ell, n, \ell/4)$ error correcting code $E$ with alphabet $\{0, 1\}$, where $\ell = O(n^2)$.

Hint: Encode every coordinate of $E_2$ using $E_1$.

Part 4. Use the code $E$ from Part 3 to construct an explicit protocol for GT.

Hint: Use the same coordinates of $E$ each time you need to check equality.