COMP 760 - Assignment 2 - Due: Feb 18th.

You are allowed to collaborate in solving these questions, but each person should write and submit her own solution.

1. Show that for every function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, we have $U^{pub}(f) = O(1)$.

2. Show that PP^{cc} is the class of problems with $\mathrm{disc}(f_n) \geq 2^{-\log^c(n)}$.

3. Show that $\mathrm{PP}^{cc} \supseteq \mathrm{NP}^{cc} \cup \mathrm{CoNP}^{cc}$.

4. Consider a problem $\{f_n\}$ in BPP^{cc}.

   (a) Show that there is a randomized protocol $P(x, y, r)$ which uses only $|r| = O(\log n)$ random bits, and still achieves
   $$\Pr[P(x, y, r) \neq f_n(x, y)] \leq \frac{1}{3}.$$

   (b) Show that there is a randomized protocol $Q(x, y, r)$ which uses only $m := |r| = O(\log^2 n)$ random bits, and achieves
   $$\Pr[Q(x, y, r) \neq f_n(x, y)] \leq \frac{1}{3m}.$$

   (c) Let m, and $Q(x, y, r)$ be as above, and we will interpret r as taking values in $\mathbb{F}_2^m$ according to some distribution. Use probabilistic method to prove the following statements:

   - If $f_n(x, y) = 1$ then there exists a choice of $a_1, \ldots, a_m \in \mathbb{F}_2^m$ such that for every $z \in \mathbb{F}_2^m$ there is at least one $i \in \{1, \ldots, m\}$ for which $Q(x, y, a_i + z) = 1$.
   - If $f_n(x, y) = 0$ then for every choice of $a_1, \ldots, a_m \in \mathbb{F}_2^m$, one can find a $z \in \mathbb{F}_2^m$ such that $Q(x, y, a_i + z) = 0$ for all $i \in \{0, \ldots, m\}$.

   (d) Conclude that $\mathrm{BPP}^{cc} \subseteq \Sigma_2^{cc} \cap \Pi_2^{cc}$.

5. Consider the group $\mathbb{F}_p^t$ where p is a prime. The characters of this group are the functions $\chi_a : \mathbb{F}_p^t \to \mathbb{C}$ for $a \in \mathbb{F}_p^n$, defined as $\chi_a : x \mapsto \exp(\frac{2\pi i}{p} \sum_{j=1}^t x_j a_j)$. It is easy to see that these are orthonormal and thus every function $f : \mathbb{F}_p^t \to \mathbb{C}$ has a unique Fourier expansio $f = \sum_{a \in \mathbb{F}_p^t} \widehat{f}(a)\chi_a$.

   Given $f : \mathbb{F}_p^t \to \mathbb{C}$, we can define the (n, t, f)-pattern matrix as before: entries are $f(x|_V + w)$ where $x \in \mathbb{F}_p^n$ is the row label, and $(V, w) \in \mathcal{V}(n, t) \times \mathbb{F}_p^t$ is the column label, and the summation $x|_V + w$ is in the group $\mathbb{F}_p^t$. What are the singular values of this pattern matrix?