COS 522 Complexity — Homework 8.

Benny Applebaum

Total of 140 points

Exercise 1 (10 points)**.** Do Exercise 19.2

Exercise 2 (10 points)**.** Do Exercise 19.8

Exercise 3 (10 points)**.** Do Exercise 19.11

Exercise 4 (20 points)**.** Do Exercise 19.13

Exercise 5 (30 points)**.** Do Exercise 19.14

Exercise 6 (30 points)**.** Do Exercise 19.18

The private information retrieval problem. Suppose that we have k-servers that hold k copies of a database $x \in \{0,1\}^n$ and a user who wants to query the database in some location i. Our goal is to design a randomized protocol that allows the user to learn x_i without letting the servers learn the index i. (The servers cannot talk to each other.) Formally, such a protocol consists of two probabilistic algorithms A, B as follows:

- Given an index i the user computes $A(i;r)$ (where r is the randomness) which outputs k functions $(Q_1, \ldots, Q_k)$, where $Q_j : \{0,1\}^n \to \{0,1\}^m$.
- The user sends Q_i to the i-th server and gets $z_i = Q_i(x)$ as an answer.
- The user computes $B(i, r, z_1, \ldots, z_k)$ and output the result.

The protocol should satisfy two properties:

- (Correctness) For every i and x, $\Pr_r[(B(i, r, Q_1(x), \ldots, Q_k(x)) = x_i] \geq 2/3$, where Q_i is the i-th output of $A(i;r)$.
- (Privacy) The j-th query of $A(i;r)$ does not expose the index i. Formally, there exist k fixed distributions $D_1, \ldots, D_k$ s.t. for every input i, the marginal distribution of the j-th query of $A(i;r)$ is D_j.

The communication complexity of the scheme is the number of bits that are sent from the servers to the user, i.e., m.

Exercise 7 (30 points)**.** Let $\mathrm{PIR_k(n)}$ be the communication complexity of the best scheme with k servers.

- Prove that $\mathrm{PIR_1} = \Theta(\mathrm{n})$. (That is, prove an upper bound and a lower bound.)
- Prove that $\mathrm{PIR_2} = \mathrm{O}(1)$. Hint: Use local decoding.