6.5420 Randomness and Computation	February 20, 2026
Homework 2	
Lecturer: Ronitt Rubinfeld	*Due Date: March 4, 2026 at 11:59pm*

Homework Problems

The following problems are to be turned in. *Please write each solution on a different page, and remember to indicate who you collaborated with for each problem.*

1. **Randomness doesn't help in the circuit model of computation.** Given a boolean function $f(\cdot)$ on boolean inputs, a sequence $C = C_1, C_2, ...$ of circuits is a *circuit family for* $f(\cdot)$ if C_n has n inputs and computes $f(x_1, \ldots, x_n)$ at its output for all n bit inputs $(x_1, \ldots, x_n)$. The family C is said to be *polynomial-sized* if the size of C_n is bounded above by $p(n)$ for every n, where $p(\cdot)$ is a polynomial. A *randomized circuit family for* $f(\cdot)$ is a circuit family for $f(\cdot)$ that, in addition to the n inputs $x_1, \ldots, x_n$, takes m inputs $r_1, \ldots, r_m$, each of which is equiprobably and independently 0 or 1. In addition, for every n, circuit C_n must satisfy

   (a) if $f(x_1, \ldots, x_n) = 0$ then output 0 regardless of the values of the random inputs $r_1, \ldots, r_m$.

   (b) if $f(x_1, \ldots, x_n) = 1$ then output 1 with probability $\geq 1/2$.

   Show: If a boolean function has a randomized polynomial sized circuit family, then it has a deterministic polynomial sized circuit family.

2. **Isolation.** Let $\{M_1, M_2, \cdots, M_k\}$ be subsets of $[1 \cdots n]$, that is $M_i \subseteq [n]$[1]. Given a set S containing N integers, we randomly assign weights $w_x \in_{\mathcal{R}} S$, to each $x \in [n]$. We also define the weight of M_i to be the sum of the weights of its elements i.e. $w(M_i) = \sum_{x \in M_i} w_x$. The goal of this problem is to prove that the minimum weight set is likely unique. To clarify, a unique minimum weight M_i is one, such that, for every other M_j, we have $w(M_j) > w(M_i)$. We will prove that

$$\mathbb{P}[\text{There is a unique } w(M_i) \text{ of minimum weight}] \geq 1 - \frac{n}{|S|}.$$

   The astonishing fact is that this holds regardless of what subsets $\{M_1, M_2, \cdots, M_k\}$ are. We begin by defining the quantity $\alpha(x)$ for all $x \in [n]$.

$$\alpha(x) = \min_{i \in [k], x \notin M_i} w(M_i) - \min_{i \in [k], x \in M_i} w(M_i \setminus \{x\})$$

   Note that above, we use the set-minus notation $M_i \setminus \{x\}$ to denote the set M_i with the element x removed. In other words, $w(M_i \setminus \{x\}) = w(M_i) - w_x$.

   (a) Calculate the probability (over the choice of weights) that $\alpha(x)$ is equal to $w(x)$ for a *specific* $x \in [n]$. Next, upper bound the probability that this happens for *some* $x \in [n]$. Specifically, show that:

$$\mathbb{P}[\exists x \text{ such that } \alpha(x) = w(x)] \leq \frac{n}{|S|}$$

[1] This notation $[n]$ stands for the set of integers $\{1, 2, \cdots, n\}$.

(b) Now, we show that it is unlikely to that two distinct M_j and M_l have the same minimum weight (compared to all other $w(M_i)$ where $i \in [k]$). Apply the result from part (a) for some suitable x, to obtain the main result:

$$\mathbb{P}[\text{There is a unique } w(M_i) \text{ of minimum weight}] \geq 1 - \frac{n}{|S|}.$$

3. **Hitting times and cover times.** Consider an irreducible Markov chain on n states.

Prove that

$$t_{\text{hit}} \leq C \leq t_{\text{hit}} \cdot H_{n-1}$$

where:

$$\begin{aligned} T_{ij} &= \mathbf{E}_i \left[\text{earliest time state } j \text{ visited}\right] \\ t_{\text{hit}} &= \max_{i,j} T_{ij} \\ C &= \max_i \mathbf{E}_i \left[\text{earliest time all states visited}\right] \\ H_n &= \sum_{k=1}^{n} \frac{1}{k} \end{aligned}$$

Hint: Fix a starting state, and consider a random permutation $\sigma_1, \ldots, \sigma_{n-1}$ of the other states. Let T_k be the first time that all of the states $\sigma_1, \ldots, \sigma_k$ have been visited, and bound $\mathbf{E}[T_k - T_{k-1}]$.

4. **Random bipartite graphs are good vertex expanders.** A graph $G = (V, E)$ is called a (K, A) vertex expander if for every subset $W \subset V$ of cardinality $|W| \leq K$, the inequality $|N(W)| \geq A|W|$ holds, where $N(W)$ denotes the set of all vertices in $V \setminus W$ adjacent to some vertex in W. An analogue of this applies to bipartite graphs: a bipartite graph $G = (L, R, E)$ is called a (K, A) vertex expander if the above condition holds for every $W \subset L$ with $|W| \leq K$.

Let $|L| = |R| = n$ and consider a random bipartite graph obtained by taking the union of three random perfect matchings between L and R.

Prove that there exist constants $\alpha, \epsilon > 0$ such that this random graph is a bipartite $(\alpha n, 1 + \epsilon)$ vertex expander with probability $1 - o(1)$ as $n \to \infty$.

Hint: The inequalities $\left(\frac{n}{k}\right)^k \leq \binom{n}{k} \leq \left(\frac{en}{k}\right)^k$ will be helpful.