6.5420 Randomness and Computation February 3, 2026

Homework 1

Lecturer: Ronitt Rubinfeld *Due Date: February 18, 2026 at 11:59pm*

Practice Problems

The following problems are to help you understand the upcoming lectures. (Hopefully, some of them will be fun to think about). Please make sure you can do them—if you have questions about them, please ask on Piazza or in office hours. Do not turn them in.

P1. **Von Neumann trick.** Given a coin with probability p of getting "heads", give a procedure for simulating one toss of a fair coin (50% chance of heads). The expected running time of the procedure should be polynomial in $\frac{1}{p} + \frac{1}{1-p}$.

P2. **Verifying matrix multiplication.** The following uses a very important technique that we will make use of extensively throughout the course. You are given $n \times n$ matrices A, B, C whose elements are from $\mathbb{Z}_2$ (integers mod 2). Show a (randomized) algorithm running in $O(n^2)$ time which verifies $A \cdot B = C$. The algorithm should always output "pass" if $A \cdot B = C$ and should output "fail" with probability at least 3/4 if $A \cdot B \neq C$. Assume the field operations $+, \times, -$ can be done in $O(1)$ steps.

P3. A 3-SAT formula takes the "and" of a set of clauses, where each clause takes the "or" of a set of literals (each literal is a variable, or the negation of a variable). Show that for any 3-SAT formula in which every clause contains literals corresponding to 3 distinct variables, there is an assignment that satisfies at least 7/8 of the clauses.

P4. **Amplification: One-sided error.** Consider a boolean function $f : \{0,1\}^* \to \{0,1\}$. You are given a randomized algorithm $\mathcal{R}$ for f with the following properties:

- If x is an input where $f(x) = 0$, then $\mathcal{R}(x) = 0$ always.
- If x is an input where $f(x) = 1$, then $\Pr[\mathcal{R}(x) = 1] \geq 1/10$.
- The running time of $\mathcal{R}(x)$ is polynomial in $|x|$.

Construct a randomized algorithm $\mathcal{R}'$ such that:

- If x is an input where $f(x) = 0$, then $\mathcal{R}'(x, \delta) = 0$ always.
- If x is an input where $f(x) = 1$, then $\Pr[\mathcal{R}'(x, \delta) = 1] \geq 1 - \delta$.
- The running time of $\mathcal{R}'(x, \delta)$ is polynomial in $|x|$ and $\dfrac{1}{\delta}$.

P5. **Amplification: Two-sided error.** Consider a boolean function $f : \{0,1\}^* \to \{0,1\}$. You are given a randomized algorithm $\mathcal{B}$ for f with the following properties:

- $\Pr[\mathcal{B}(x) = f(x)] \geq 2/3$ for any input x.
- The running time of $\mathcal{B}(x)$ is polynomial in $|x|$.

Construct a randomized algorithm $\mathcal{B}'$ such that:

- $\Pr[\mathcal{B}'(x, \delta) = f(x)] \geq 1 - \delta$ for any input x.
- The running time of $\mathcal{B}'(x, \delta)$ is polynomial in $|x|$ and $\dfrac{1}{\delta}$.

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. **Amplification: Approximation.**

   Consider a real-valued function $f : \{0,1\}^* \to \mathbb{R}$. You are given a randomized approximation algorithm $\mathcal{A}$ for f such that

   $$\Pr\left[\frac{f(x)}{1+\epsilon} \leq \mathcal{A}(x,\epsilon) \leq f(x)(1+\epsilon)\right] \geq 3/4$$

   and $\mathcal{A}(x,\epsilon)$ runs in time polynomial in $\frac{1}{\epsilon}$ and $|x|$. Construct a randomized approximation algorithm $\mathcal{B}$ for f such that

   $$\Pr\left[\frac{f(x)}{1+\epsilon} \leq \mathcal{B}(x,\epsilon,\delta) \leq f(x)(1+\epsilon)\right] \geq 1-\delta$$

   and $\mathcal{B}(x,\epsilon,\delta)$ runs in time polynomial in $\frac{1}{\epsilon}$, $|x|$, and $\log\frac{1}{\delta}$.

2. **Bipartite subgraphs of the Erdős-Renyi graph.** The *Erdős-Renyi* graph $G(n,p)$ is a random undirected graph on n vertices where each possible edge appears independently with probability p. That is, we consider each of the $\binom{n}{2}$ pairs of vertices, and independently flip a p-biased coin for each one to decide if it is an edge of $G(n,p)$ or not.

   Prove that with probability $1-o(1)$ as $n\to\infty$, every bipartite subgraph of $G(n,1/2)$ has at most $\frac{n^2}{8}+\frac{n^{3/2}}{\sqrt{8}}$ edges.

3. **Office politics.** A certain organization consists of N employees. In order to operate, the organization must form committees of exactly k employees each. Employees are allowed to be on any number of committees, but to prevent conflicts of interest, no two committees may have more than d people in common.

   Prove that if $N > k > d$ are integers with $k \geq 4$ and $Nd \geq 4k^2$, then it is always possible to form at least $2^{d/5-1}$ committees satisfying the above rules.

4. **Directed cycles.** Let $D=(V,E)$ be a simple directed graph (that is, a directed graph with no self-loops and with at most one edge between ever pair of vertices). Assume that D has <u>minimum outdegree</u> δ and <u>maximum indegree</u> Δ. Show that if

   $$e(\Delta\delta+1)\left(1-\frac{1}{k}\right)^{\delta} \leq 1,$$

   then D contains a (directed, simple) cycle whose length is a multiple of k.
   Hint: Let $f : V \to \{0,1,\ldots,k-1\}$ be a random coloring of V obtained by choosing for each $v \in V$, $f(v) \in \{0,\ldots,k-1\}$ independently according to a uniform distribution. For each $v \in V$, consider the event A_v that there is no $u \in V$ s.t. $(v,u) \in E$ and $f(u) = f(v)+1$ mod k.