6.5420 Randomness and Computation March 4, 2026

Homework 3

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

PRG Review

Here is a brief review of PRGs as discussed in lecture.

Consider a directed multigraph H with exactly 2 outgoing arcs from each vertex, one of which is labeled 0 and the other 1. A walk in H is determined by a starting vertex $u \in V(H)$ and a binary string $x \in \{0,1\}^*$ where x_i is the label of the i'th edge in the walk. We write $H[u,x]$ to denote the final vertex of such a walk.

We say a function $G : \{0,1\}^s \to \{0,1\}^L$ is an (ϵ, n)-*walk PRG* if for every n-vertex 2-out-regular digraph H and every pair of vertices $u, v \in V(H)$, we have

$$|\Pr[H[u, U_L] = v] - \Pr[H[u, G(U_s)] = v]| \leq \epsilon,$$

where U_a denotes a uniformly random element of $\{0,1\}^a$.

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. **Naive doubling PRG.**

   Let $G : \{0,1\}^s \to \{0,1\}^{L/2}$ be a $(.01, n)$-walk PRG where $n \geq 100$. Suppose we naively try to double the output length of the PRG, by constructing $G_3 : \{0,1\}^s \to \{0,1\}^L$ according to $G_3(\sigma) = G(\sigma) \| G(\sigma)$. Prove that G_3 is not a $(0.49, n)$-walk PRG.

2. **PRG parameters.**

   (a) Prove that if $G : \{0,1\}^s \to \{0,1\}^{s+1}$ is a $(.49, n)$-walk PRG then $s \geq \Omega(\log(n))$.

   (b) Claim: There exists a function $f : \mathbb{N} \to \mathbb{N}$ such that for any $n, L \in \mathbb{N}$ there exists a $(.01, n)$-walk PRG $G : \{0,1\}^s \to \{0,1\}^L$ where $s = f(n)$. In particular, the seed length s depends only on n, not on L.

   For this problem, prove the above claim only considering digraphs H where the random walk Markov chain on H is **ergodic**.

   (c) **Optional part.** Prove the claim in part (b) without the assumption that H is ergodic.

3. **Generating pairwise independent random bits.**

   (a) Let $Z_1, \ldots, Z_k$ be i.i.d. uniformly random bits. Define

   $$X_S = \bigoplus_{i \in S} Z_i$$

   for every subset $S \subseteq [k]$ with $S \neq \emptyset$. Prove that the X_S are uniformly-distributed and pairwise independent.

(b) The above construction uses k truly random bits to generate 2^k pairwise independent bits. Prove that this is optimal, meaning that if $f : \{0,1\}^k \to \{0,1\}^n$ is any function such that $f(Z_1, \ldots, Z_k)$ is a vector of n uniformly-distributed, pairwise independent bits, then $n \leq 2^k$.

Hint: Consider the real matrix $A \in \{-1,1\}^{2^k \times n}$ defined by $A_{ij} = (-1)^{f(i)_j}$ where $i \in [2^k], j \in [n]$. What can you say about the columns of A, from a linear-algebra perspective?

4. **Random walk on the path.**

(a) Let P_n be the path graph on n vertices. Prove that the cover time $C(P_n)$ is $\Omega(n^2/\log n)$ and $O(n^2)$.

(b) **Optional part.** Learn about the *Azuma-Hoeffding inequality* and *stopped martingales* and use them to prove the tighter result $C(P_n) = \Theta(n^2)$.

(c) Let ϕ be a satisfiable 2-CNF formula over n variables $x_1, \ldots, x_n$. For example,

$$\phi(x_1, x_2, x_3) = (x_1 \vee \neg x_2) \wedge (x_2 \vee \neg x_3) \wedge (\neg x_1 \vee \neg x_3)$$

is satisfied by setting all three variables to false. Consider the following random process:

- Start with an arbitrary non-satisfying assignment of boolean values to the n variables.
- Repeat forever:
  - Let C be an arbitrary unsatisfied clause in ϕ.
  - Pick one of the two variables involved in C, uniformly at random.
  - Complement (flip between $\{\text{true}, \text{false}\}$) the value of the chosen variable.
  - If ϕ is now satisfied, stop.

Prove that the above process terminates after at most $O(n^2)$ repetitions.