in=0.15in

6.5420 Randomness and Computation March 18, 2026

Homework 4

Lecturer: Ronitt Rubinfeld *Due Date: April 15, 2026 at 11:59pm*

Optional Problem

The following problem is optional; no need to turn it in.

Quadratic non-residuosity. $\mathbb{Z}_n^\times$ is the multiplicative group of integers relatively prime to n. An element $s \in \mathbb{Z}_n^\times$ is said to be a *quadratic residue modulo* n if there exists $r \in \mathbb{Z}_n^\times$ such that $s \equiv r^2 \pmod{n}$. Construct a private-coin interactive proof system for the language of pairs (s, n) such that s is *not* a quadratic residue modulo n.

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. **Existence of k-wise independent hash functions.** If X and Y are finite sets and $1 \leq k \leq |X|$ is an integer, a *k-wise independent hash function* from X to Y is defined as a random function $h : X \to Y$ such that for any k distinct elements $x_1, \ldots, x_k \in X$, the distribution of $h(x_1), \ldots, h(x_k)$ is jointly uniform over Y^k. In this problem we will see one way of efficiently constructing k-wise independent hash functions.

   Let F be a finite field, and $0 \leq k < |F|$ be an integer. Define the random function $h : F \to F$ by

   $$h(x) = \sum_{i=0}^{k} c_i x^i$$

   where $c_0, \ldots, c_k$ are i.i.d. uniformly random elements of F. (Note: 0^0 is defined as 1.)

   Prove that h is a $(k+1)$-wise independent hash function. You may use the fact that if $z_0, \ldots, z_k$ are distinct elements of F, then the square *Vandermonde matrix*

   $$\begin{bmatrix} z_0^0 & z_0^1 & z_0^2 & \cdots & z_0^k \\ z_1^0 & z_1^1 & z_1^2 & \cdots & z_1^k \\ z_2^0 & z_2^1 & z_2^2 & \cdots & z_2^k \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ z_k^0 & z_k^1 & z_k^2 & \cdots & z_k^k \end{bmatrix}$$

   is always invertible.

2. **SAT formulae with unique solutions.** The NP-complete problem SAT takes as input a Boolean formula $\phi(x_1, \ldots, x_n)$ and asks whether it has a satisfying assignment. One might wonder whether SAT is easier to solve if you are guaranteed that the formula has no more than one satisfying assignment. In this problem you will show that—as far as randomized algorithms are concerned—this task is just as difficult.

   Suppose you are given an algorithm $\mathcal{A}$ with the following behavior: If ψ is unsatisfiable, then $\mathcal{A}(\psi)$ returns NO. If ψ has exactly one satisfying assignment, then $\mathcal{A}(\psi)$ returns YES. If ψ has more than one satisfying assignment, then $\mathcal{A}(\psi)$ may choose to return YES or NO arbitrarily.

   Using $\mathcal{A}$, construct a randomized polynomial-time algorithm $\mathcal{B}$ which solves SAT with one-sided error. That is, if ϕ is unsatisfiable then $\mathcal{B}(\phi)$ must always output NO, whereas if ϕ is satisfiable then $\mathcal{B}(\phi)$ must output YES with probability at least $1/2$.

   Hint: Start by designing an algorithm $\mathcal{B}_k$ which works provided that the input ϕ has either 0 satisfying assignments or $[2^{k-1}, 2^k]$ of them.

   Further hints will be posted on the course website.

3. **Perfect completeness in verification.** Interactive proof systems are probabilistic, so there is some probability of the verifier incorrectly accepting or rejecting. It turns out that interactive proof systems can be made *perfectly complete*, meaning that for strings in the language, the prover can convince the verifier to accept with probability 1. For this problem we'll prove this in the case of a protocol with just two rounds.

   Suppose there exists a randomized polynomial-time algorithm $V(x, y)$, where $|y|$ is polynomial in $|x|$, with the following behavior: If $x \notin L$, then $V(x, y)$ outputs NO with probability at least $\frac{2}{3}$ for all y. If $x \in L$, then there exists y such that $V(x, y)$ outputs YES with probability at least $\frac{2}{3}$.

   Use V to construct a randomized polynomial-time algorithm $W(x, y)$, where $|y|$ is a polynomial (of your choice) in $|x|$, with the following behavior: If $x \notin L$, then $W(x, y)$ outputs NO with probability at least $\frac{2}{3}$ for all y. If $x \in L$, then there exists y such that $W(x, y)$ always outputs YES.

   Hint: Let $A \subseteq \{0,1\}^\ell$ be a set of strings, and consider the collection of translations $A \oplus t = \{a \oplus t : a \in A\}$ where $t \in \{0,1\}^\ell$. Show that:

   - If A is "small" then $\bigcup_{i=1}^{\ell}(A \oplus t_i)$ is also "small" for any choice of $t_1, \ldots, t_\ell \in \{0,1\}^\ell$.
   - If A is "large", then there exists $t_1, \ldots, t_\ell \in \{0,1\}^\ell$ so that $\bigcup_{i=1}^{\ell}(A \oplus t_i) = \{0,1\}^\ell$.

   Further hints will be posted on the course website.

4. **Testing dictator functions.**

   A *dictator function*, also called a *projection function*, is a function $f : \{1,-1\}^n \to \{1,-1\}$ of the form $f(x) = x_i$ for some $i \in [n]$. Our aim is to determine whether an unknown function is a dictator.

   Consider the following procedure $\mathcal{T}$. Given parameter δ, the procedure chooses $x, y, z \in \{1,-1\}^n$ by first choosing x, y uniformly from $\{1,-1\}^n$, next choosing w by setting each bit w_i to -1 with probability δ and $+1$ with probability $1-\delta$ (independently for each i), and finally setting z to be $x \circ y \circ w$, where $\circ$ denotes the bitwise multiply operation. Finally, $\mathcal{T}$ accepts if $f(x)f(y)f(z) = 1$ and rejects otherwise.

   (a) Prove that for any function f, the probability that $\mathcal{T}(\delta, f)$ accepts is exactly

   $$\frac{1}{2} + \frac{1}{2}\sum_{S \subseteq [n]} (1-2\delta)^{|S|}\hat{f}(S)^3.$$

   (b) Use part (a) to prove that if f is a dictator function, then $\mathcal{T}(\delta, f)$ accepts with probability $1-\delta$.

(continued on next page)

(c) Let $0 < \epsilon < 1$ be a constant. Use part (a) to prove that if f is any function where $\mathcal{T}(\delta, f)$ accepts with probability at least $1 - \epsilon$, then there exists $S \subseteq [n]$ such that $(1 - 2\delta)^{|S|}\hat{f}(S) \geq 1 - 2\epsilon$.

(d) Using part (c), show that if $\epsilon < 0.1$ and $\delta = \frac{3}{4}\epsilon$ then if f is a function where $\mathcal{T}(\delta, f)$ accepts with probability at least $1-\epsilon$, then there exists $S \subseteq [n]$ such that f is ϵ-close to χ_S and $|S| \leq 1$.

(e) Use $\mathcal{T}$ together with parts (b) and (d) to construct a two-sided test $\mathcal{U}$ for dictator functions. That is: if f is a dictator function then $\mathcal{U}(\epsilon, f)$ accepts with probability at least $\frac{2}{3}$; and if f is ϵ-far from being a dictator then $\mathcal{U}(\epsilon, f)$ accepts with probability at most $\frac{1}{3}$.

(Note that constant functions are not considered dictator functions.)

The running time of $\mathcal{U}$ should be polynomial in n and $\dfrac{1}{\epsilon}$.