There are 5 questions for a total of 50 points.

---

(10) 1. In the class, we showed that the family $\mathcal{H} = \{h_{a,b} | 1 \leq a \leq p-1, 0 \leq b \leq p\}$ is 2-universal for prime $p \geq n$, where $h_{a,b}(x) = ((ax+b) \mod p) \mod n$ Consider the hash function family

$$\mathcal{H}' = \{h_a | 1 \leq a \leq p-1\},$$

where

$$h_a(x) = (ax \mod p) \mod n.$$

Show the following:

(a) $\mathcal{H}'$ is not 2-universal.

(b) For any $x, y \in \{0, 1, 2, ..., p-1\}$, if h is chosen uniformly at random from $\mathcal{H}'$ then $\mathbf{Pr}[h(x) = h(y)] \leq \frac{2}{n}$. (In other words $\mathcal{H}'$ is *almost* 2-universal.)

(10) 2. Let U be a universe with $|U| \geq n$ and let $V = \{0, 1, ..., n-1\}$. A family of hash functions $\mathcal{H}$ from U to V is said to be k-universal if, for any elements $x_1, x_2, ..., x_k$ and for a hash function h chosen uniformly at random from $\mathcal{H}$, we have

$$\mathbf{Pr}[h(x_1) = h(x_2) = ... = h(x_k)] \leq \frac{1}{n^{k-1}}.$$

Suppose n balls are hashed into n bins using a 3-universal hash function family. Show that with probability at least (1/2), the maximum loaded bin has at most $(2n)^{1/3}$ balls.

(10) 3. Given a bag of r red balls and g green balls, suppose that we uniformly sample n balls from the bag without replacement. Let R denote the number of red balls in the sample. What is the expected value of R? How concentrated is R around its expectation $E[R]$?

(10) 4. Let $f(X_1, ..., X_n)$ satisfy the Lipschitz condition so that, for any i and any values $x_1, ..., x_n$ and y_i,

$$|f(x_1, ..., x_{i-1}, x_i, x_{i+1}, ..., x_n) - f(x_1, ..., x_{i-1}, y_i, x_{i+1}, ..., x_n)| \leq c.$$

We set $Z_0 = \mathbf{E}[f(X_1, ..., X_n)]$, and $Z_i = \mathbf{E}[f(X_1, ..., X_n) \mid X_1, ..., X_i]$. Give an example to show that, if the X_i's are not independent, then it is possible that $|Z_i - Z_{i-1}| > c$.

(10) 5. Consider the bit-fixing routing algorithm for routing a permutation on the n-dimensional hypercube. Suppose that n is even. Write each source node i as the concatenation of two binary strings a_i and b_i, each of length $n/2$. Let the destination of i's packet be the concatenation of b_i and a_i. Show that this permutation causes the bit-fixing routing algorithm to take $\Omega(2^{n/2})$ steps.