CSCE 658: Randomized Algorithms – Spring 2024
Problem Set 1

Due: Thursday, February 1, 2024, 5:00 pm CT

Problem 1. (30 points total) Suppose we want to generate some randomness. A natural way is to use a fair coin to generate the randomness.

1. (10 points) Suppose we have a coin that lands heads with probability $\frac{1}{2}$ and tails with probability $\frac{1}{2}$. Describe, with proof, a procedure that uses this coin to generate a random bit that is 0 with probability $\frac{1}{3}$ and 1 with probability $\frac{2}{3}$.

   HINT: The procedure is allowed to fail to generate an output bit, provided that 1) *conditioned* on the event that a bit is output, the output bit is 0 with probability $\frac{1}{3}$ and 1 with probability $\frac{2}{3}$, and 2) the probability that a bit is output is positive.

2. (10 points) Unfortunately, now we only have a coin that lands heads with probability $\frac{1}{3}$ and tails with probability $\frac{2}{3}$. Describe, with proof, a procedure that uses this coin to generate a random bit that is 0 with probability $\frac{1}{2}$ and 1 with probability $\frac{1}{2}$.

3. (10 points) Unfortunately, now we do not even know the probability distribution of our coin. Indeed, suppose we now have a coin that lands heads with an unknown probability $p \in (0, 1)$. Let $k \geq 1$ be an integer. Describe, with proof, a procedure that uses this coin to generate a random bit that is 0 with probability $\frac{1}{k}$ and 1 with probability $1 - \frac{1}{k}$.

Problem 2. (30 points total) Karger's min-cut algorithm

1. (10 points) Let $\mathcal{A}$ be an algorithm that prints "SUCCESS" with probability $p > 0$ each time it is called. Show that if we call the algorithm $\mathcal{A}$ independently a total of $m := \mathcal{O}\left(\frac{1}{p}\right)$ times, then with probability at least 0.99, it will print "SUCCESS" at least one of the m times.

   HINT: You may use the fact that $1 - x \leq e^{-x}$ for all real numbers x.

2. (10 points) Recall that in class, we showed that Karger's min-cut algorithm succeeds with probability at least $1 - \frac{2}{n(n-1)}$. Describe with proof, an algorithm that uses Karger's min-cut algorithm as a black-box subroutine, i.e., it cannot change any algorithmic aspects of Karger and finds the min-cut with probability at least 0.99. Your algorithm must use a total of $\mathcal{O}(n^3)$ edge contractions.

3. (10 points) A graph G can have many different min cuts. Use the analysis of Karger's min-cut algorithm to show that a connected graph G on n vertices has at most $\frac{n(n-1)}{2}$ different min cuts.

(Continued on next page)

Problem 3. (30 points total) Suppose that we improve Karger's min-cut algorithm in the following manner. We first run Karger's algorithm and contract edges until there is a graph G' that consists of k vertices and super-vertices. We then independently run Karger's algorithm m times in parallel on G' and report the minimum of the outputs of the m independent instances.

Show that if $k = \sqrt{n}$ and $m = 4n \log n$, then there exists a constant C such that we output the min-cut with probability at least $\frac{C}{n}$.

HINT: First analyze the probability that G' preserves a fixed min-cut of G.

NOTE: The goal in Problem 2 was to find the min-cut with probability 0.99, using $\mathcal{O}(n^3)$ edge contractions. This improved version of Karger's algorithm uses $\mathcal{O}(n^{2.5})$ edge contractions.

Problem 4. (30 points total) Random variables and probability distributions.

1. (10 points) Let X and Y be random real-valued variables with probability distributions p and q respectively. Suppose that we have $\mathbb{E}[X] = \mathbb{E}[Y]$. Either prove that $p \equiv q$, i.e., $p(x) = q(x)$ for all $x \in \mathbb{R}$, or give a counterexample, with justification.

2. (10 points) Let X and Y be random real-valued variables with probability distributions p and q respectively. Suppose that $p(x) = q(-x)$ for all $x \in \mathbb{R}$. Show that $\mathbb{E}[X^2] = \mathbb{E}[Y^2]$.

3. (10 points) Let X and Y be random real-valued variables with probability distributions p and q respectively. Suppose that we have $\mathbb{E}[X] = \mathbb{E}[Y]$ and $\mathrm{Var}[X] = \mathrm{Var}[Y]$. Either prove that $p \equiv q$, i.e., $p(x) = q(x)$ for all $x \in \mathbb{R}$, or give a counterexample, with justification.