CS 409M : Introduction to Cryptography Fall 2024

Assignment 1
A Discrete Probability Path

Instructor: Sruthi Sekar *TAs:* Giriraj Singh, Nilabha Saha

Problem 1: The Matchmaking Theatre

b eligible bachelors and m beautiful female models happen randomly to have purchased single seats in the same $(b+m)$-seat row of a theatre. On the average, how many pairs of adjacent seats are ticketed for (heterosexual) marriageable couples?

Problem 2: Fermat's Urns

Two urns contain the same number of balls, some black and some white in each. From each urn are drawn n (≥ 3) balls with replacement. Find the number of drawings and composition of the two urns so that the probability that all white balls are drawn from the first urn is equal to the probability that the drawing from the second urn is either all white or all black.
Assume that each urn has at least one ball of each colour.

Problem 3: Summing the Tail

Prove the tail-sum formula for expectation of a non-negative integer-valued discrete random variable.

Tail Sum Formula

If X is a non-negative integer-valued discrete random variable, then:

$$\mathbb{E}[X] = \sum_{i=0}^{\infty} \Pr[X > i]$$

Problem 4: The Rise and Fall of the Amoeba Empire

There is one amoeba in a pond. After every minute, the amoeba may die, stay the same, split into two, or split into three with equal probability. All its offsprings, if it has any, will behave the same (and independent of other amoebas). What is the probability that the amoeba population will die out?

Problem 5: Bar's Retirement

Bar the bear decides he wants to manage beehives in his old age. He has just received k bees that he wants to allocate to his n beehives. Since Bar is old, he often loses count when trying to allocate the bees to beehives. He decides to just allocate the bees randomly to his hives. That is, for each bee, he chooses a beehive uniformly at random. Help Bar prove that his strategy yields an approximately uniform distribution of bees with high probability.

a) Let X_i be the number of bees in the i-th beehive. Compute $\mathbb{E}[X_i]$.

b) Show that X_i and X_j are not independent.

c) Let $M = \max(X_1, X_2, \ldots, X_n)$. Show that $\Pr[M \geq 2k/n] \leq ne^{-k/(3n)}$.

Problem 6: In All Your Gorgeous Colours

Suppose there are n different colours of coupons, and we want to collect at least one coupon from every colour. We start out with nothing, and at each step, we get a new random coupon, equally likely to be any of the n colours, and independent of the previous coupons.

a) What is the expected time T when we are done collecting?

b) What is the variance of T?

c) Use Chebyshev's inequality to bound the probability that T deviates farther from its expectation by an amount α.

Problem 7: Birthday Paradox Generalisation

Let q elements $y_1, y_2, \ldots, y_q$ be chosen uniformly and independently at random from a set of size N, then show that:

$$\mathrm{coll}(q, N) = \Pr[\exists i \neq j \text{ s.t. } y_i = y_j] \leq \frac{q^2}{2N}$$

Problem 8: Return of Birthday Paradox Generalisation

Let $q \leq \sqrt{2N}$ elements be $y_1, y_2, \ldots, y_q$ be chosen uniformly and independently at random from a set of size N, then show that:

$$\mathrm{coll}(q, N) = \Pr[\exists i \neq j \text{ s.t. } y_i = y_j] \geq \frac{q(q-1)}{4N}$$

Hint: For all $x \in [0, 1]$, we have the inequalities $1 - x \leq e^{-x} \leq 1 - (x/2)$.