Assignment 2: CS 203 (Spring 2020)

1. (5+15=20 marks) **Independent Geometric Random Variables**

   A *geometric random variable* counts the number of tosses until you get a head (as defined in notes). Let Y and Z be two independent, geometric random variables with parameter p.

   (a) Interpret the expression $\Pr(Y = i \mid Y + Z = n)$ in terms of tossing only one coin.

   (b) Show that $\Pr(Y = i \mid Y + Z = n) = \frac{1}{n-1}$ for $i = 1, \ldots, n-1$.

   Solution: $\square$

2. (10+13+5+7=35 marks) **Verifying Matrix Multiplication**

   Given three $n \times n$ matrices A, B and C; how fast can we test whether $AB = C$? An obvious answer is to multiply A and B and compare the resulting matrix with C which currently requires $O(n^{2.3728})$ multiplications [1]. We can use a faster method inspired by probabilistic techniques to test $AB = C$ as follows:

   1 Pick $x_1, \ldots, x_n \in \{0, 1\}$ randomly, uniformly and independently. Let $\bar{x} = (x_1, \ldots, x_n)$.

   2 Test $A(B\bar{x}) = C\bar{x}$? If they match then return **Yes** otherwise **No**.

   The above algorithm only requires $O(n^2)$ multiplications. Let us try to prove that the probability of error is 'small'.

   (a) Let q be a rational number. Pick a boolean value $u \in \{0, 1\}$ randomly uniformly. Show that $\Pr_u(u = q) \leq \frac{1}{2}$.

   (b) Let $D = (d_{ij})$ be a $n \times n$ matrix with the ith row as D_i. If $D_i \neq \bar{0}$, show that $\Pr_x(D_i\bar{x} = 0) \leq \frac{1}{2}$.

   (c) Assume $AB \neq C$. Let $D = AB - C$. Show that the error probability $\Pr_x(D\bar{x} = \bar{0}) \leq \frac{1}{2}$.

   (d) How will you change the algorithm to improve its error probability to 2^{-100}? How much overhead does this cause? Give the best possible estimate.

   Solution: $\square$

3. (8+10+7=25 marks) **Improved Chernoff's Bound**

   We can improve Chernoff's bound in special cases of random variables as opposed to 0/1 random variables (using simpler proof techniques).

   Let X is a sum of n independent random variables $X_1, \ldots, X_n$, each taking values in $\{1, -1\}$, with $\Pr(X_i = 1) = \Pr(X_i = -1) = \frac{1}{2}$. Then for any $a > 0$, we will prove that

   $$\Pr(X \geq a) \leq e^{-\frac{a^2}{2n}}. \tag{1}$$

   (a) Prove the inequality $\frac{t^{2i}}{(2i)!} \leq \frac{(t^2/2)^i}{i!}$.

   (b) Take a variable $t > 0$. Show that $E[e^{tX_i}] \leq e^{t^2/2}$.

   (c) Prove inequality 1.

   Solution: $\square$

4. (5+15=20 marks) **Markov Chain**

A homogeneous Markov chain has state space $S = \{1, 2, 3\}$ with the transition matrix M as follows:

$$M = \begin{bmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & 0 & \frac{2}{3} \\ \frac{2}{3} & \frac{1}{3} & 0 \end{bmatrix}$$

(a) Draw the state transition diagram corresponding to M.

(b) Let $\Pr(X_0 = 1) = \frac{1}{2}$ and $\Pr(X_0 = 2) = \frac{1}{4}$. Find $\Pr(X_0 = 3, X_1 = 2, X_2 = 1)$.

Solution: $\square$

References

[1] François Le Gall. *Powers of tensors and fast matrix multiplication. International Symposium on Symbolic and Algebraic Computation, ISSAC'14, Kobe, Japan, July 23-25, 2014.*