Assignment 2: CS 203 (Spring 2020)
Rishabh Kumar Chaudhary (180609)

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:

   (a) We can say that Y counts the number of trials for the toss to get first head and after we have encountered the first head, Z depicts the no. of more trials for the second head. Thus, $\Pr(Y = i \mid Y + Z = n)$ is the probability of a head at i^{th} toss given that there were a total of n tosses with two heads and one of them at n^{th} toss.

   (b) We know that $P(Y = i \mid Y + Z = n) = \frac{P((Y=i)\cap(Y+Z=n))}{P(Y+Z=n)}$. Here,

   $$P(Y = i) = (1-p)^{i-1} * p \tag{1}$$

   We can also say that

   $$P(Y + Z = n) = \sum_{k=1}^{n-1} P(Y = k, Z = n - k) \tag{2}$$

   We cannot take k=0 or k=n because Y or Z cannot take 0 value. Inserting 2 and 1 in above equation gives us:

   $$P(Y = i \mid Y + Z = n) = \frac{P(Y = i, Z = n-i)}{P(Y + Z = n)} = \frac{(1-p)^{i-1} \times p \times (1-p)^{n-i-1} \times p}{\sum_{k=1}^{n-1}(1-p)^{k-1} \times p \times (1-p)^{n-k-1} \times p}$$

   $$= \frac{(1-p)^{n-2} \times p^2}{\sum_{k=1}^{n-1}(1-p)^{n-2} \times p^2} \tag{3}$$

   In the 3 equation, we can see that a constant is being added n-1 times in the denominator. Therefore, equation 3 is equivalent to

   $$\frac{(1-p)^{n-2} \times p^2}{(n-1) \times (1-p)^{n-2} \times p^2} = \frac{1}{n-1}$$

   □

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:

(a)
$$P(u = q) = P(u = 1 \mid q = 1) \times P(q = 1) + P(u = 0 \mid q = 0) \times P(q = 0) \tag{4}$$

Since p and q are independent variables, we can say that

$$P(u = 0 \mid q = 0) = P(u = 0) = \frac{1}{2} = P(u = 1 \mid q = 1) \tag{5}$$

Inserting 5 in 4 gives:

$$P(u = q) = \frac{1}{2} \times (P(q = 0) + P(q = 1))$$

Also,

$$P(q = 0) + P(q = 1) \leq 1$$

Therefore,

$$P(u = q) \leq \frac{1}{2} \tag{6}$$

(b) Let $p = D_i\bar{x}$

$$D_i\bar{x} = \sum_{j=1}^{n} D_{ij}x_j \tag{7}$$

Suppose that $D_{ik} \neq 0$, then

$$\sum_{j=1}^{n} D_{ij}x_j = D_{ik}x_k + y \text{ where } y = \sum_{j=1 \text{ and } j \neq k}^{n} D_{ij}x_j \tag{8}$$

We will partition the equation 8 over y implying that

$$P(p = 0) = P(p = 0 \mid y = 0) \times P(y = 0) + P(p = 0 \mid y \neq 0) \times P(y \neq 0) \tag{9}$$

It is quite clear that y and x_k are independent. Therefore,

$$P(p = 0|y = 0) = P(x_k = 0 \mid y = 0) = P(x_k = 0) = \frac{1}{2} \tag{10}$$

$$P(p = 0 \mid y \neq 0) = P(x_k = 1 \cap D_{ik} = -y) \leq P(x_k = 1) = \frac{1}{2} \tag{11}$$

Putting 11 and 10 in 9 implies that

$$P(p = 0) \leq \frac{1}{2} \times P(y = 0) + \frac{1}{2} \times P(y \neq 0)$$

$$\implies P(p = 0) \leq \frac{1}{2} \times (P(y = 0) + (1 - P(y = 0)))$$

$$\implies P(D_i\bar{x} = 0) \leq \frac{1}{2}$$

(c) Suppose that i_{th} row of D is D_i. Since $AB \neq C$, there exists at least one element D_{ij} which is non-zero. By the result of part (b) we can say that,

$$P(D_i\bar{x} = 0) \leq \frac{1}{2} \tag{12}$$

$$P(D\bar{x} = 0) = P(D_1 = 0 \cap D_2 = 0 \cap \dots D_i = 0 \dots D_n = 0) \leq P(D_i = 0) \leq \frac{1}{2} \tag{13}$$

(d) If we perform this algorithm 100 times then each iteration will have a probability less than half, and total probability of error will be reduced to 2^{-100}. In each iteration multiplications taking time $O(n^2)$ will take place. Thereby, increasing the time of running the algorithm by 100 times.

□

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 $X_1, \dots, X_n$, 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

$$\Pr(X \geq a) \leq e^{-\frac{a^2}{2n}}. \tag{14}$$

(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 14.

Solution:

(a)

$$\frac{t^{2i}}{(2i)!} = \frac{(t^2)^i}{(2i)(2i-1)\dots(2i-(i-1)) \times (i!)}$$

$$= \frac{(t^2)^i}{2^i \times (i)(i-1/2)(i-1)\dots(i-(i-1)/2) \times (i!)} \leq \frac{(t^2)^i}{2^i \times i!} = \frac{(t^2/2)^i}{i!}$$

(b)

$$P(X_i = 1) = P(X_i = -1) = \frac{1}{2}$$

$$\implies P(e^{tX_i} = e^t) = P(e^{tX_i} = e^{-t}) = \frac{1}{2}$$

$$E[e^{tX_i}] = P(e^{tX_i} = e^t) \times e^t + P(e^{tX_i} = e^{-t}) \times e^{-t}$$

$$= \frac{1}{2} \times e^t + \frac{1}{2} \times e^{-t} \tag{15}$$

$$e^t = \sum_{k=0}^{\infty} \frac{t^k}{k!} = 1 + t + \frac{t^2}{2!} + \dots \tag{16}$$

Inserting 16 in 15 implies that

$$E[e^{tX_i}] = \frac{1}{2} \times (1 + t + \frac{t^2}{2!} + \frac{t^3}{3!} + \dots + 1 - t + \frac{t^2}{2!} - \frac{t^3}{3!} \dots)$$

$$= \frac{1}{2} \times 2 \times (1 + \frac{t^2}{2!} + \frac{t^4}{4!} + \dots) = \sum_{k=0}^{\infty} \frac{t^{2k}}{(2*k)!}$$

$$e^{t^2/2} = \sum_{k=0}^{\infty} \frac{(t^2/2)^k}{k!} = \sum_{k=0}^{\infty} \frac{(t)^{2k}}{2^k \times k!}$$

By the result of part (a), we can say that

$$\sum_{k=0}^{\infty} \frac{t^{2k}}{(2*k)!} \leq \sum_{k=0}^{\infty} \frac{(t/2)^k}{k!} = \sum_{k=0}^{\infty} \frac{(t)^{2k}}{2^k \times k!} = e^{t^2/2}$$

(c) Since both n and a are positive, we can say that

$$P(X \geq a) = P(e^{(aX/n)} \geq e^{a^2/n})$$

Using markov's inequality,

$$P(e^{(aX/n)} \geq e^{a^2/n}) \leq \frac{E[e^{(aX/n)}]}{e^{a^2/n}} \tag{17}$$

Since X_is are mutually independent, we can say that

$$E[e^{(aX/n)}] = \prod_{i=1}^{n} E[e^{aX_i/n}] \tag{18}$$

Using the result of part (b) in equation 18

$$\prod_{i=1}^{n} E[e^{aX_i/n}] \leq e^{n \times (a/n)^2/2} = e^{a^2/(2n)} \tag{19}$$

Inserting 19 in 17 gives

$$P(e^{(aX/n)} \geq e^{a^2/n}) \leq \frac{e^{a^2/(2n)}}{e^{a^2/n}} = e^{-a^2/(2n)}$$

□

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

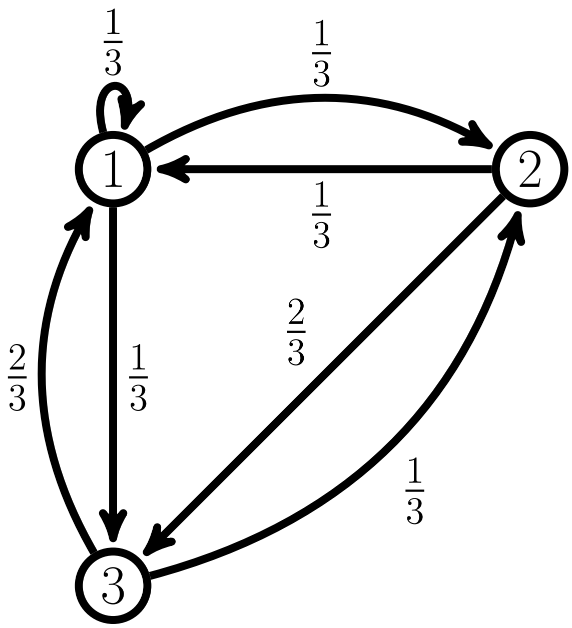
A homogeneous Markov chain has state space $S = \{1, 2, 3\}$ with the transition matrix M as follows:

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

(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:



(a)

(b)

$$P(X_0 = 3) = 1 - P(X_0 = 1) - P(X_0 = 2) = 1 - \frac{1}{2} - \frac{1}{4} = \frac{1}{4} \tag{20}$$

$$\begin{aligned} P(X_0 = 3, X_1 = 2, X_2 = 1) &= P(X_0 = 3) \times P(X_1 = 2 \mid X_0 = 3) \times P(X_2 = 1 \mid X_1 = 2) \\ &= \frac{1}{4} \times M_{32} \times M_{21} = \frac{1}{4} \times \frac{1}{3} \times \frac{1}{3} = \frac{1}{36} \end{aligned}$$

□

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.*