Assignment 2: CS 203 (Spring 2020)
Solutions

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) Consider the experiment: keep tossing a coin until one gets 2 heads. The expression can be interpreted as the probability of getting first head at ith toss, given that second head occurs at nth toss.

   (b) $\Pr(Y = i \mid Y + Z = n) = \Pr(Y = i, Z = n - i)/\Pr(Y + Z = n)$.
   $\Pr(Y = i, Z = n-i) = \Pr(Y = i). \Pr(Z = n-i) = \{p(1-p)^{i-1}\} \cdot \{p(1-p)^{n-i-1}\} = p^2(1-p)^{n-2}$.
   This is independent on i so for every $i = 1, \ldots, n-1$ this probability is same and zero otherwise.
   Hence, $\Pr(Y = i \mid Y + Z = n) = \frac{1}{n-1}$.

   □

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) $\Pr(u = q) = \Pr(u = q | q = 0) \Pr(q = 0) + \Pr(u = q | q \neq 0) \Pr(q \neq 0)$. Now $\Pr(u = q | q = 0) = \frac{1}{2}$ and $\Pr(u = q | q \neq 0) \leq 1/2$.
   So, $\Pr(u = q) \leq \frac{1}{2} \Pr(q = 0) + \frac{1}{2} \Pr(q \neq 0) = \frac{1}{2}$.

(b) Wlog, $d_{i1} \neq 0$. So, $\Pr(d_{i1}x_1 + \ldots + d_{in}x_n = 0) = \Pr(x_1 = -\frac{1}{d_{i1}}(d_{i2}x_2 + \ldots + d_{in}x_n))$. Let $s = -\frac{1}{di1}(d_{i2}x_2 + \ldots + d_{in}x_n)$.
$\Pr(x_1 = s) = \sum_{r_2,\ldots,r_n \in \{0,1\}} \Pr(x_1 = s \ \& \ x_2 = r_2, \ldots, x_n = r_n)$.
$\Pr(x_1 = s) = \sum_{r_2,\ldots,r_n \in \{0,1\}} \Pr(x_1 = q) \Pr(x_2 = r_2, \ldots, x_n = r_n)$ with q a value of s.
$\Pr(x_1 = s) \leq \frac{1}{2} \sum_{r_2,\ldots,r_n \in \{0,1\}} \Pr(x_2 = r_2, \ldots, x_n = r_n) = \frac{1}{2}$ using (a).

(c) $\Pr(D\bar{x} = \bar{0}) = \Pr(D_1\bar{x} = 0 \ \& \ldots \& \ D_n\bar{x} = 0) \leq \Pr(D_i\bar{x} = 0) \leq \frac{1}{2}$.

(d) The algo gives one-sided error, so we repeat the algo 100 times independently to get error prob $\frac{1}{2^{100}}$ with constant (100) overhead in number of multiplications.

□

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:

(a) $(2i)! = (i!)(i+1.i+2\ldots.i+i) \geq (i!)2^i$ as $2 \leq i+1, 2 \leq i+2, \ldots, 2 \leq i+i$ for $i \geq 1$.
So, $1/(2i)! \leq 1/(i!)2^i$. And so $\frac{t^{2i}}{(2i)!} \leq \frac{(t^2/2)^i}{i!}$.

(b) $E[e^{tX_i}] = \frac{1}{2}e^t + \frac{1}{2}e^{-t}$. Use the expansion for e^t and e^{-t} and add to get,
$E[e^{tX_i}] = \sum_{i \geq 0} \frac{t^{2i}}{(2i)!}$. Use (a) to get $E[e^{tX_i}] \leq \sum_{i \geq 0} \frac{(t^2/2)^i}{i!}$.
$E[e^{tX_i}] \leq e^{t^2/2}$ using geometric sum.

(c) Use independence to get $E[e^{tX}] = e^{t^2 n/2}$. Using Markov inequality, $P(X \geq a) = P(e^{tX} \geq e^{ta}) \leq e^{t^2 n/2 - ta}$. Substitute $t = a/n$ to get required bound.

□

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:

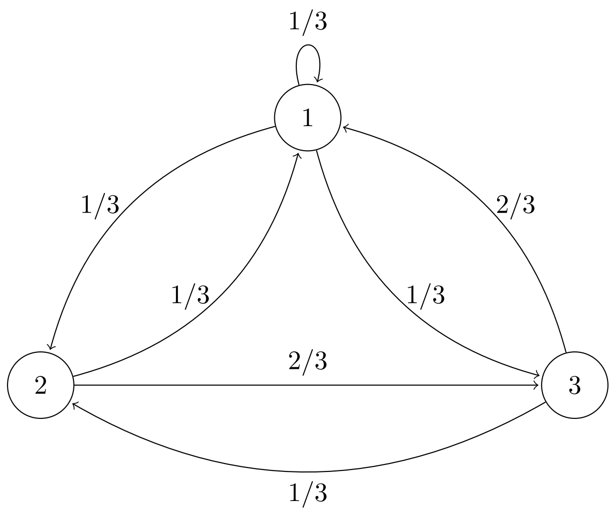

Figure 1: State transition diagram

(a)

(b) $\Pr(X_0 = 3) = 1 - 1/2 - 1/4 = 1/4$.
$\Pr(X_0 = 3, X_1 = 2, X_2 = 1) = \Pr(X_0 = 3)\Pr(X_1 = 2, X_2 = 1|X_0 = 3)$
$= \Pr(X_0 = 3)\Pr(X_1 = 2|X_0 = 3)\Pr(X_2 = 1|X_1 = 2, X_0 = 3)$.
$= \Pr(X_0 = 3)\Pr(X_1 = 2|X_0 = 3)\Pr(X_2 = 1|X_1 = 2)$ using the property of Markov process.
$= (1/4).(1/3).(1/3) = 1/36$.

$\square$

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.*