Mathematics for Computer Science: Homework 3

Instructed by *Andrew C. Yao & Wang Yuexuan*

Due on March 25, 2010

Zhang Kunwei J92 2009011269

LPV 5.4.5

We flip a coin n times ($n \geq 1$). For which values of n are the following pairs of events independent?
(a) The first coin flip was head; the number of all heads was even.
(b) The first coin flip was head; the number of all heads was more than then number of tails.
(c) The number of heads was even; the number of heads was more than the number of tails.

Answer:

Let A_n, B_n, C_n be the event "the first coin flip was head", "the number of all heads was even", "the number of heads was more than the number of tails", respectively.

$P(A_n) = \frac{2^{n-1}}{2^n} = \frac{1}{2}$

$P(B_n) = \frac{\sum_{2k\leq n}\binom{n}{2k}}{2^n} = \frac{\sum_{2k\leq n}\binom{n-1}{2k}+\sum_{2k\leq n}\binom{n-1}{2k-1}}{2^n} = \frac{\sum_{k\leq n-1}\binom{n-1}{k}}{2^n} = \frac{2^{n-1}}{2^n} = \frac{1}{2}$

$P(C_n) = \frac{\sum_{n<2k}\binom{n}{k}}{2^n} = \frac{1}{2}\left(\frac{\sum_{n<2k}\binom{n}{k}}{2^n} + \frac{\sum_{n<2k}\binom{n}{n-k}}{2^n}\right) = \frac{1}{2}\left(\frac{\sum_{n<2k}\binom{n}{k}}{2^n} + \frac{\sum_{n>2k}\binom{n}{k}}{2^n}\right) = \begin{cases} \frac{1}{2}\times\frac{2^n-\binom{n}{p}}{2^n} & n=2p \\ \frac{1}{2} & n=2p+1 \end{cases}$

$P(A_nB_n) = \frac{\sum_{2k\leq n-1}\binom{n-1}{2k}}{2^n} = \frac{\sum_{2k\leq n-1}\binom{n-2}{2k}+\sum_{2k\leq n-1}\binom{n-2}{2k-1}}{2^n} = \frac{\sum_{k\leq n-2}\binom{n-2}{k}}{2^n} = \begin{cases} \frac{2^{n-2}}{2^n} & n\geq 2 \\ 0 & n=1 \end{cases} = \begin{cases} \frac{1}{4} & n\geq 2 \\ 0 & n=1 \end{cases}$

$P(A_nC_n) = \frac{1}{2}\cdot\frac{\sum_{n-1\leq 2k}\binom{n-1}{k}}{2^n} = \frac{1}{4}\left(\frac{\sum_{n-1\leq 2k}\binom{n-1}{k}}{2^n} + \frac{\sum_{n-1\leq 2k}\binom{n-1}{n-1-k}}{2^n}\right) = \begin{cases} \frac{1}{4} & n=2p \\ \frac{1}{4}\times\frac{2^{n-1}+\binom{n-1}{p}}{2^{n-1}} & n=2p+1 \end{cases}$

$$\begin{aligned} P(B_nC_n) &= \frac{\sum_{n<4k}\binom{n}{2k}}{2^n} \\ &= \frac{\sum_{n<4k}\binom{n-1}{2k}+\sum_{n<4k}\binom{n-1}{2k-1}}{2^n} \\ &= \frac{\sum_{n-1\leq 2k}\binom{n-1}{k}}{2^n} \\ &= \begin{cases} 0 & n=1 \\ \frac{1}{4} & n=2p>1 \\ \frac{1}{4}\times\frac{2^{n-2}+\binom{n-1}{p}}{2^{n-2}} & n=2p+1>1 \end{cases} \end{aligned}$$

Then we have:
(a) A and B is independent when $P(A_n)P(B_n) = P(A_nB_n) \Leftrightarrow n \geq 2$.
(b) A and C is independent when $P(A_n)P(C_n) = P(A_nC_n) \Leftrightarrow n \in \emptyset$.
(c) B and C is independent when $P(B_n)P(C_n) = P(B_nC_n) \Leftrightarrow n \in \emptyset$.

LPV 6.10.6

Let $a > 1$, and $k, n > 0$. Prove that $a^k - 1 | a^n - 1$ if and only if $k|n$.

Answer:

If $k|n$, then $a^n - 1 = \left(a^k - 1\right)\left(1 + a^k + a^{2k} + \ldots + a^{n-k}\right) \Rightarrow a^k - 1 | a^n - 1$.

Suppose we have $a^k - 1|a^n - 1$. Let $n = n_0 + tk$ $(n_0 < k)$, and then $a^k - 1|a^{tk} - 1 \Rightarrow a^k - 1|a^{n_0+tk} - a^{n_0}$ $\Rightarrow a^k - 1|a^n - 1 - \left(a^{n_0+tk} - a^{n_0}\right)$ i.e. $a^k - 1|a^{n_0} - 1$. $a^{n_0} - 1 < a^k - 1 \Rightarrow a^{n_0} - 1 = 0 \Rightarrow n_0 = 0 \Rightarrow n = tk \Rightarrow k|n$.

LPV 6.10.16

Prove that for every positive integer m there is a Fibonacci number divisible by m.

Answer: $(F_{k-1} \bmod m, F_k \bmod m) \in \{(x_1, x_2)\,|0 \le x_1, x_2 < m\}$. The left is infinity, and the right is finity. According to the Pigeonhole Principle, $\exists k_1 < k_2$ s.t. $(F_{k_1-1}, F_{k_1}) \equiv (F_{k_2-1}, F_{k_2}) \pmod m$. Then we can prove $F_n \equiv F_{n+(k_2-k_1)} \pmod m$ for all $n \in \mathbb{Z}$ by induction. Thus $F_{k_2-k_1} \equiv F_0 \equiv 0 \pmod m$ i.e. $m|F_{k_1-k_2}$.

LPV 6.10.18

Find integers x and y such that

$$\begin{cases} 2x + y \equiv 4 & \pmod{17} \\ 5x - 5y \equiv 9 & \pmod{17} \end{cases}$$

Answer:

$15x \equiv 5\,(2x + y) + (5x - 5y) \equiv 5 \times 4 + 9 \equiv 12 \pmod{17} \Rightarrow x \equiv 12 \times 15^{17-2} \equiv 11 \pmod{17}$

$y \equiv 2x + y - 2x \equiv 4 - 2 \times 11 \equiv 16 \pmod{17}$

Special Problem 1

Consider a random walk on a circle with nodes $v_0, v_1, \ldots, v_{n-1}$, and an edge between v_i and $v_{(i+1) \bmod n}$ for each of $i = 0, 1, 2, \ldots, n{-}1$. Starting initially at v_0, in each step we move from the current node v_i randomly to either $v_{(i-1) \bmod n}$ or $v_{(i+1) \bmod n}$ with equal probability. After N steps, let p_N be the probability that all n nodes have been visited. Prove that $p_N \ge 1 - \frac{cn}{N^{\frac{1}{2}}}$ for some positive constant c.

Answer: Let q_n be the probability of event Q, the walk stop at a place at least one circle away from the original point. Then event Q is a sufficient condition of the event "all n nodes have been visited", thus $p_n \ge q_n$. The probability $1 - q_N$ is equal to the probability that we flip a coin for N times, and get $H \le T + n - 1$ and $T \le H + n - 1$ i.e. $\frac{N-n+1}{2} \le H \le \frac{N+n-1}{2}$.

Special Problem 1 continued on next page...

Let $a_N = \sqrt{N}\frac{n\cdot N!}{2^N((N/2)!)^2}$. We have,

$$\begin{aligned}
p_N &\geq q_n \\
&\geq 1 - \frac{\sum_{\frac{N-n+1}{2}\leq H\leq\frac{N+n-1}{2}}\binom{N}{H}}{2^N} \\
&\geq 1 - \frac{\sum_{\frac{N-n+1}{2}\leq H\leq\frac{N+n-1}{2}}\binom{N}{N/2}}{2^N} \\
&\geq 1 - n\binom{N}{N/2}2^{-N} \\
&= 1 - \frac{n\cdot N!}{2^N\left((N/2)!\right)^2} \\
&= 1 - \frac{a_N}{\sqrt{N}}
\end{aligned}$$

And,

$$\begin{aligned}
\lim_{N\to\infty} a_N &= \lim_{N\to\infty}\sqrt{N}\frac{n\cdot\sqrt{2\pi N}\,(N/e)^N}{2^N\left(\sqrt{2\pi N/2}\,(N/2e)^{N/2}\right)^2} \\
&= \lim_{N\to\infty}\sqrt{N}\frac{n\cdot\sqrt{2\pi}N^{N+\frac{1}{2}}}{2^N\left(\sqrt{2\pi}\,(N/2)^{\frac{N}{2}+\frac{1}{2}}\right)^2} \\
&= \sqrt{\frac{2}{\pi}n}
\end{aligned}$$

Pick C_1 s.t. $C_1 > \sqrt{\frac{2}{\pi}}$. When $\varepsilon = \left(C_1 - \sqrt{\frac{2}{\pi}}\right)n$, $\exists M$ s.t. when $m > M$,
$|a_m - a_\infty| < \varepsilon \Rightarrow |a_m| - |a_\infty| < \varepsilon \Rightarrow |a_m| < C_1 n$
Let $c = \max\left(\frac{\max_{1\leq k\leq M}|a_k|}{n}, C_1\right)$. $\Rightarrow a_N \leq cn$ for all N, $p_N \geq 1 - \frac{a_N}{\sqrt{N}} \geq 1 - \frac{cn}{\sqrt{N}}$.

Special Problem 2

The probability space concept $\Omega = (U, p)$ can be generalized to the case when U is an infinite set $\{u_1, u_2, u_3, \ldots, u_n, \ldots\}$. As before, an event T is a subset of U , and $\Pr\{T\} = \sum_{u\in T} p(u)$. Consider a random walk on an n-node circle (as in the previous problem) such that it halts as soon as all the nodes have been visited. We are interested in the probability $q_{n,i}$ for the random walk to halt at node v_i (i.e. v_i is the very last node that the random walk visits). Clearly, for $n = 3$, we have $q_{3,1} = q_{3,2} = \frac{1}{2}$.

(a) Specify a probability space $\Omega = (U, p)$ for this random walk. You may use an infinite U. Show that, according to your specification, $\sum_{u\in U} p(u) = 1$.

(b) Derive the values of $q_{4,i}$ for $i = 1, 2, 3$.

(c) Determine $q_{n,i}$ for $1 \leq i \leq n-1$.

Answer:

(a) Let $D(\overrightarrow{x}, s_1, s_2) = \max_{s_1\leq k\leq s_2} x_k - \min_{s_1\leq k\leq s_2} x_k$,

$$U = \bigcup_{0\leq m}\{\overrightarrow{x}\in\mathbb{N}_n^m | x_0 = 0; \forall k\in\mathbb{N}\cap[1,m], |x_k - x_{k-1}| \equiv 1\,(\mathrm{mod}\ n); D(1,m-1) < n-1; D(1,m) = n-1\}$$

For $u \in \mathbb{N}_n^m$, $p(u) = \frac{1}{2^m}$. In Special Problem 1, we proved $p_\infty = 1$. On the other hand, $p_\infty = \sum_u \Pr(\text{"This random walk halts with sequence } \overrightarrow{u}\text{."}) = \sum_{u\in U} p(u)$. So we have $\sum_{u\in U} p(u) = 1$.

(b) & (c) Let $Q_{n,i}(L_0, L_1, d\in\{0,1\})$ be the probability for a random walk in which current node is L_d, and the leftmost, rightmost visited node is $-L_0, L_1$ respectively, to halt at node v_i on an n-node circle.

LEMMA 1: Assume $s_1 \le s \le s_2$. Starting from point s, a random walk will reach point s_1 before point s_2 with the probability of $P(s) = \frac{s_2 - s}{s_2 - s_1}$.

PROOF: $P(s) = \frac{1}{2}(P(s-1) + P(s+1))$. So $\{P(s)\}$ is an arithmetic progression, i.e. linear. And notice $P(s_1) = 1$, $P(s_2) = 0$.

Now we have a recurrence,

$$Q_{n,i}(L_0, L_1, d) = \begin{cases} \frac{(L_0+L_1+1)Q_{n,i}(L_0+1,L_1,0)+Q_{n,i}(L_0,L_1+1,1)}{L_0+L_1+2} & L_0 + L_1 < n-1, d = 0 \\ \frac{Q_{n,i}(L_0+1,L_1,0)+(L_0+L_1+1)Q_{n,i}(L_0,L_1+1,1)}{L_0+L_1+2} & L_0 + L_1 < n-1, d = 1 \\ 1 & L_0 + L_1 = n-1, L_1 = i-1, d = 0 \\ 1 & L_0 + L_1 = n-1, L_1 = i, d = 1 \\ 0 & L_0 + L_1 = n-1, \text{ otherwise} \end{cases}$$

Using this recurrence we can get,

(1)$Q_{n,i}(n-i-1, i-1, 0) = Q_{n,i}(n-i-1, i-1, 1) = 1$. (directly)

(2) $\forall k > 0$, $Q_{n,i}(n-i-1-k, i-1, 1) = Q_{n,i}(n-i-1, i-1-k, 0) = \frac{1}{n-1}$. (by induction)

(3) $\forall k > 0$, $Q_{n,i}(n-i-1-k, i-1, 0) = Q_{n,i}(n-i-1, i-1-k, 1) = 1 - \frac{k}{n-1}$. (by induction)

(4) $\forall k > 0, \forall d \in \{0,1\}$, $Q_{n,i}(n-i-1-k, i-2, d) = Q_{n,i}(n-i-2, i-1-k, d) = \frac{1}{n-1}$. (by induction)

(5) $\forall k_1 < n-i-1$, $\forall k_2 < i-1$, $\forall d \in \{0,1\}$, $Q_{n,i}(k_1, k_2, d) = \frac{1}{n-1}$. (by double induction)

Notice $Q_{n,i}(k_1+1, k_2, d) = Q_{n,i}(k_1, k_2+1, d) = \frac{1}{n-1}$ when proving (5).

(6) $q_{n,i} = Q_{n,i}(0,0,0) = \frac{1}{n-1}$. (deduce to (2) or (4) or (5))

Finally we get$q_{n,i} = \frac{1}{n-1}$ for $1 \le i \le n-1$ for (c). Let $n = 4$, and we get the answer for (b), i.e. $q_{4,i} = \frac{1}{3}$ for $i = 1, 2, 3$.

Special Problem 3

Use the Chernoff Bounds

$$\Pr\{X \ge (1+\delta)\mu\} \le \left(\frac{e^\delta}{(1+\delta)^{1+\delta}}\right)^\mu$$

and

$$\Pr\{X \le (1-\delta)\mu\} \le \left(\frac{e^{-\delta}}{(1-\delta)^{1-\delta}}\right)^\mu$$

to prove the following inequalities: For all $0 < \delta \le 1$

(a) $\Pr\{X \ge (1+\delta)\mu\} \le e^{-\mu\delta^2/3}$.

(b) $\Pr\{X \le (1-\delta)\mu\} \le e^{-\mu\delta^2/2}$.

Answer: We need to prove $\left(\frac{e^\delta}{(1+\delta)^{1+\delta}}\right)^\mu \le e^{-\mu\delta^2/3}$ and $\left(\frac{e^{-\delta}}{(1-\delta)^{1-\delta}}\right)^\mu \le e^{-\mu\delta^2/2}$.

$$\begin{aligned} \left(\frac{e^\delta}{(1+\delta)^{1+\delta}}\right)^\mu &\le e^{-\mu\delta^2/3} \\ \Leftrightarrow \frac{e^\delta}{(1+\delta)^{1+\delta}} &\le e^{-\delta^2/3} \\ \Leftrightarrow \delta - (1+\delta)\ln(1+\delta) &\le -\frac{\delta^2}{3} \\ \Leftrightarrow \frac{\delta^2}{3} + \delta - (1+\delta)\ln(1+\delta) &\le 0 \\ \Leftrightarrow f_1(\delta) = \frac{\delta^2 + 3\delta}{1+\delta} - 3\ln(1+\delta) &\le 0 \end{aligned}$$

For this inequality, we have $f_1(0) = 0, f_1'(\delta) = \frac{\delta^2+2\delta+3}{(1+\delta)^2} - \frac{3}{1+\delta} = \frac{\delta(\delta-1)}{(1+\delta)^2} < 0.$

$$\begin{aligned}
\left(\frac{e^{-\delta}}{(1-\delta)^{1-\delta}}\right)^{\mu} &\leq e^{-\mu\delta^2/2} \\
\Leftrightarrow \frac{e^{-\delta}}{(1-\delta)^{1-\delta}} &\leq e^{-\delta^2/2} \\
\Leftrightarrow -\delta - (1-\delta)\ln(1-\delta) &\leq -\frac{\delta^2}{2} \\
\Leftrightarrow \frac{\delta^2}{2} - \delta - (1-\delta)\ln(1-\delta) &\leq 0 \\
\Leftrightarrow f_2(\delta) = \frac{\delta^2 - 2\delta}{1-\delta} - 2\ln(1-\delta) &\leq 0
\end{aligned}$$

For this inequality, we have $f(0) = 0, f_2'(\delta) = \frac{\delta-2}{(1-\delta)^2} - \frac{2}{1-\delta} = \frac{3\delta-4}{(1-\delta)^2} < 0.$

Acknowledgement: Answers here are all original.