Mathematics for Computer Science: Homework 3

Xingyu Su 2015010697

March 18, 2019

LPV 5.4.3

Let A and B be independent events. Express the probability $P(A \cup B)$ in terms of the probabilities of A and B.

Answer:

Because A and B are independent events, so $P(A \cap B) = 0$.
Then $P(A \cup B) = P(A) + P(B) - P(A \cap B) = P(A) + P(B)$

LPV 5.4.4

We select a subset X of the set $S = \{1, 2, \ldots, 100\}$ randomly and uniformly (so that every subset has the same probability of being selected). What is the probability that

(a) X has an even number of elements;
(b) both 1 and 100 belong to X;
(c) the largest element of X is 50;
(d) X has at most 2 elements.

Answer:

(a)

$$P(a) = \frac{1}{2^{100}} \left(\binom{0}{100} + \binom{2}{100} + \cdots + \binom{98}{100} + \binom{100}{100} \right) = \frac{1}{2}$$

(b)

$$P(b) = \frac{2^{98}}{2^{100}} = \frac{1}{4}$$

(c)

$$P(c) = \frac{2^{49}}{2^{100}} = \frac{1}{2^{51}} \approx 4.44 \times 10^{-16}$$

(d)

$$P(d) = \frac{\binom{0}{100} + \binom{1}{100} + \binom{2}{100}}{2^{100}} \approx 4 \times 10^{-27}$$

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 heads; the number of all heads was even.

(b) The first coin flip was head; the number of all heads was more than the number of tails.
(c) The number of heads was even; the number of heads was more than the number of tails.

Answer:

(a) To get same probability for even and odd number of all heads for left $2 \sim n$ coins, n should be an odd number with $n > 1$. Thus, $n = 3, 5, 7, \ldots, 2k+1, \ldots$

(b) Since the symmetry will guarantee the probability of more heads and more tails are always the same. So any $n \geq 1$ is reasonable.

(c) To keep the symmetry, n should be an even number. Thus, $n = 2, 4, 6, \ldots, 2k, \ldots$

LPV 6.3.5

Let p be a prime and $1 \leq a \leq p-1$. Consider the numbers $a, 2a, 3a, \ldots, (p-1)a$. Divide each of them by p, to get residues $r_1, r_2, \ldots, r_{p-1}$. Prove that every integer from 1 to $p-1$ occurs exactly once among these residues.

[Hint: First prove that no residue can occur twice.]

Answer:

First prove that no residue can occur twice. Assume there are two different coefficients k, s $(k > s)$ that have same residues $r_k = r_s = r$. Denote the division as:

$$ka = k'p + r$$
$$sa = s'p + r$$

Then

$$(k-s)a = (k'-s')p$$

Where $(k-s)$ and $(k'-s')$ are positive integers. But p is a prime number and $0 < k-s < p-1$ $1 \leq a \leq p-1$ can not have factorization p. So there comes conflict and the Assumption is wrong.

Since there is no residue occur twice and all residues have $1 \leq r_1, r_2, \ldots, r_{p-1} \leq p-1$. So every integer from 1 to $p-1$ occurs exactly once among these residues.

LPV 6.5.2

Consider a regular p-gon, and for a fixed $k(1 \leq k \leq p-1)$, consider all k-subsets of the set of its vertices. Put all these k-subsets into a number of boxes: We put two k-subsets into the same box if they can be rotated into each other. For example, all k-subsets consisting of k consecutive vertices will belong to one and the same box.

(a) Prove that if p is a prime, then each box will contain exactly p of these rotated copies.
(b) Show by an example that (a) does not remain true if we drop the assumption that p is a prime.
(c) Use (a) to give a new proof of Lemma 6.5.2.

Answer:

(a) Since each set can be rotated p times, we just need to prove that each of the p rotated copies of a set are different. Suppose that there is a copy occurs k times during the rotation. Then every other copy **must** occur k times. Now we get $k|p$, and obviously $k! = p$ so $k = 1$. In result, the identity is proved.

(b) Consider a case shown in Figure 1.

(c) Since each box contains p subsets of size k, the total number of subsets $\binom{p}{k}$ must satisfy $p|\binom{p}{k}$

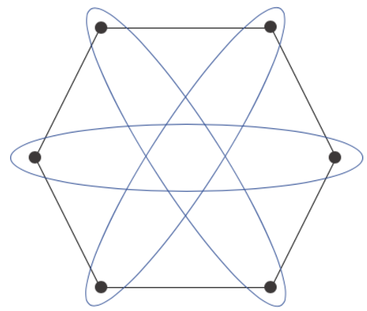

Figure 1: A hexagon shows (a) is wrong when p is not a prime number

LPV 6.5.4

Give a third proof of Fermat's "Little" Theorem based on Exercise 6.3.5.
[Hint: Consider the product $a(2a)(3a)\cdots((p-1)a)$]

Answer:
From Exercise 6.3.5, we know that if ka can be denote as $m_k p + r_k$ for $k = 1, 2, \cdots, p-1$, then every integer from 1 to $p-1$ occurs exactly once among $r_1, r_2, \cdots, r_{p-1}$. Consider the product $a(2a)(3a)\cdots((p-1)a)$, we have:

$$a(2a)(3a)\cdots((p-1)a) = (p-1)!a^{p-1}$$

Then:

$$\begin{aligned}(p-1)!(a^{p-1}-1) &= a(2a)(3a)\cdots((p-1)a) - (p-1)! \\ &= (m_1p + r_1)(m_2p + r_2)\cdots(m_{p-1}p + r_{p-1}) - r_1r_2\cdots r_{p-1} \\ &= c_1p^{p-1} + c_2p^{p-2} + \cdots + c_{p-1}p\end{aligned}$$

Which obviously satisfies $p|a^{p-1}-1$.

Special Problem 1

Alice and Bob each independently tosses an unbiased coin n times. Let X and Y be the random variables corresponding to the number of HEADs in Alice' and Bob's results. Your solutions must be closed-form formulas in n.
(a) Determine the expected value of the random variable $X - Y$.
(b) Determine the variance of the random variable $X - Y$.
(c) Let S denote the event that $X = Y$, and let $s(n) = Pr\{S\}$. Determine $s(n)$.
(d) Let T denote the event that $X = Y + 1$, and let $t(n) = Pr\{T\}$. Determine $t(n)$.

Answer:
Easy to know that X and Y are independent, and:

$$P(X = k) = P(Y = k) = \frac{1}{2^n}\binom{n}{k}$$

Special Problem 1 continued on next page...

$$E(X) = E(Y) = \frac{1}{2^n} \sum_{k=0}^{n} k \binom{n}{k} = \frac{n}{2}$$

$$D(X) = D(Y) = \frac{1}{2^n} \sum_{k=0}^{n} (k - \frac{n}{2})^2 \binom{n}{k} = \frac{n}{4}$$

(a)

$$E(X - Y) = E(X) - E(Y) = \sum_{k=0}^{n} kP(X = k) - kP(Y = k) = 0$$

(b)

$$D(X - Y) = D(X) + D(Y) = \frac{n}{2}$$

(c)

$$s(n) = P(X = Y) = \sum_{k=0}^{n} P(X = k)P(Y = k) = \frac{1}{2^{2n}} \sum_{k=0}^{n} \binom{n}{k}^2$$

Consider equation $(1 + x)^n(1 + x)^n = (1 + x)^{2n}$, we have:

$$\left(\binom{n}{0} + x\binom{n}{1} + \cdots x^n\binom{n}{n}\right)^2 = \binom{2n}{0} + x\binom{2n}{1} + \cdots x^{2n}\binom{2n}{2n}$$

Compare the coefficients of x^n, we get:

$$\begin{aligned}\binom{2n}{n} &= \binom{n}{0}\binom{n}{n} + \binom{n}{1}\binom{n}{n-1} + \cdots + \binom{n}{n} + \binom{n}{0} \\ &= \binom{n}{0}^2 + \binom{n}{1}^2 + \cdots + \binom{n}{n}^2\end{aligned}$$

So

$$s(n) = \frac{1}{2^{2n}} \sum_{k=0}^{n} \binom{n}{k}^2 = \frac{1}{2^{2n}} \binom{2n}{n} = \frac{(2n)!}{(n!)^2 2^{2n}}$$

(d)

$$t(n) = P(X = Y + 1) = \sum_{k=0}^{n-1} P(X = k + 1)P(Y = k) = \frac{1}{2^{2n}} \sum_{k=0}^{n-1} \binom{n}{k+1}\binom{n}{k}$$

Similar to (c), compare the coefficients of x^{n+1}, we get:

$$\begin{aligned}\binom{2n}{n+1} &= \binom{n}{n}\binom{n}{1} + \binom{n}{n-1}\binom{n}{2} + \cdots + \binom{n}{1}\binom{n}{n} \\ &= \binom{n}{0}\binom{n}{1} + \binom{n}{1}\binom{n}{2} + \cdots + \binom{n}{n-1}\binom{n}{n}\end{aligned}$$

So

$$t(n) = \frac{1}{2^{2n}} \sum_{k=0}^{n-1} \binom{n}{k}\binom{n}{k+1} = \frac{1}{2^{2n}} \binom{2n}{n+1} = \frac{(2n)!}{(n+1)!(n-1)!2^{2n}}$$

Acknowledgement:

None