

Mathematics for Computer Science: Homework 5

Instructed by *Andrew C. Yao*

Due on April 3, 2008

Botao Hu J72 2007011292

hupo001@gmail.com

Contents

1	Exercise 6.10.5	2
2	Exercise 6.10.6	2
3	Exercise 6.10.7	2
4	Exercise 6.10.10	2
5	Exercise 6.10.11	3
6	Exercise 6.10.16	3
7	Exercise 6.10.17	3
8	Exercise 6.10.18	4
9	Exercise 6.10.19	4
10	Exercise 6.10.20	5
11	Special Problem 1	5
12	Special Problem 2	6
13	Special Problem 3	7
14	Special Problem 4	10

1 Exercise 6.10.5

Prove that every prime larger than 3 gives a remainder of 1 or -1 if divided by 6.

Answer:

Suppose $p \not\equiv \pm 1 \pmod{6}$, we derive a logical contradiction. If $p \equiv \pm 2 \pmod{6}$, $\gcd(\pm 2, 6) = 2 \mid p$, which is a contradiction because p is a prime. If $p \equiv 3 \pmod{6}$, $\gcd(3, 6) = 3 \mid p$, which is a contradiction because p is a prime. Thus, $p \equiv 1 \pmod{6}$ or $p \equiv -1 \pmod{6}$.

2 Exercise 6.10.6

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

Answer:

Let r be the remainder if we divide n by k . By the polynomial division, we have

$$a^n - 1 = (a^k - 1)(a^{n-k} + a^{n-2k} + \cdots + a^r) + a^r - 1$$

Obviously,

$$a^k - 1 \mid a^n - 1 \iff a^k - 1 \mid a^r - 1$$

Because $0 \leq r < k$ and $a > 1$, we have

$$0 \leq a^r - 1 < a^k - 1$$

So

$$a^k - 1 \mid a^r - 1 \iff r = 0$$

Thus,

$$a^k - 1 \mid a^n - 1 \iff k \mid n$$

3 Exercise 6.10.7

Prove that if $a > 3$, then a , $a + 2$, and $a + 4$ cannot be all primes. Can they all be powers of primes?

Answer:

Suppose that $a, a + 2, a + 4$ are all primes. Because there must exist a multiple of 3 among $a, a + 1, a + 2$, there must exist a multiple of 3 among $a, a + 2, a + 4$ because $a + 4 \equiv a + 1 \pmod{3}$. This is a contradiction with the assumption that $a, a + 2, a + 4$ are all primes when $a > 3$. So $a, a + 2, a + 4$ cannot be all primes. But they can be all powers of primes, for example, $a = 5, a + 2 = 7, a + 4 = 9 = 3^2$.

4 Exercise 6.10.10

Show that a number with 30 digits cannot have more than 100 prime factors.

Answer:

Let n 's prime factorization be $n = \prod_{i=1}^k p_i^{a_i}$ ($a_i > 0$).

$$2^{\sum_{i=1}^k a_i} \leq \prod_{i=1}^k p_i^{a_i} = n < 10^{30} < 2^{100}$$

Thus, $\sum_{i=1}^k a_i < 100$. n can not have more than 100 prime factors.

5 Exercise 6.10.11

Show that a number with 160 digits has a prime power divisor that is at least 100. This is not true if we want a prime divisor that is at least 100.

Answer:

Suppose that all prime power divisors of the number with 160 digits are less than 100. Find all prime $p < 100$: {2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97}. For each p , find the maximal $p^a < 100$: {64, 81, 25, 49, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97}. Multiply them and get the product

$$69720375229712477164533808935312303556800 < 10^{160}$$

The result is calculated with Mathematica.

```
In[1] := Times @@ (Function[x, NestWhile[##x &, x, ##x < 100 &]]
          /@ (Prime @ Range @ PrimePi @ 100))
Out[1] = 69720375229712477164533808935312303556800
```

So a number with 160 digits has a prime power divisor that is at least 100.

6 Exercise 6.10.16

Prove that for every positive integer m there is a Fibonacci number divisible by m (well, of course, $F_0 = 0$ is divisible by any m , we mean a larger one).

Answer:

Let $F_i^* = F_i \pmod m$. Consider the adjacent item $(F_i^*, F_{i+1}^*) \in \{0, 1, \dots, m-1\}^2$. Because the total set $\{0, 1, \dots, m-1\}^2$ is finite, there must exist i and j such that $0 < i < j$ and $(F_i^*, F_{i+1}^*) = (F_j^*, F_{j+1}^*)$. After one iterations of the recurrence formula $F_{i-1} = F_{i+1} - F_i$, we get $F_{i-1}^* = F_{j-1}^*$. Similarly, executing i iterations of the recurrence formula, we must get $F_0^* = F_{i-j}^* = 0$ where $i - j > 0$. So F_{i-j} can be divisible by m .

7 Exercise 6.10.17

Find integers x and y such that $25x + 41y = 1$.

Answer:

Execute the Euclidean Algorithm for $\gcd(25, 41)$ as following.

$$\begin{aligned}
 & \gcd(25, 41) \\
 &= \gcd(25, 41 - 25) = \gcd(25, -25 + 41) \\
 &= \gcd(25 - (-25 + 41), -25 + 41) = \gcd(25 \cdot 2 - 41, -25 + 41) \\
 &= \gcd(25 \cdot 2 - 41, -25 + 41 - (25 \cdot 2 - 41)) = \gcd(25 \cdot 2 - 41, -25 \cdot 3 + 41 \cdot 2) \\
 &= \gcd(25 \cdot 2 - 41 - (-25 \cdot 3 + 41 \cdot 2), -25 \cdot 3 + 41 \cdot 2) = \gcd(25 \cdot 5 - 41 \cdot 3, -25 \cdot 3 + 41 \cdot 2) \\
 &= \gcd(25 \cdot 5 - 41 \cdot 3, -25 \cdot 3 + 41 \cdot 2 - (25 \cdot 5 - 41 \cdot 3) \cdot 3) = \gcd(25 \cdot 5 - 41 \cdot 3, -25 \cdot 18 + 41 \cdot 11) \\
 &= \gcd(25 \cdot 5 - 41 \cdot 3 - (-25 \cdot 18 + 41 \cdot 11) \cdot 2, -25 \cdot 18 + 41 \cdot 11) = \gcd(0, -25 \cdot 18 + 41 \cdot 11)
 \end{aligned}$$

For $t \in \mathbb{Z}$, we have x and y as follows such that $25x + 41y = 1$.

$$\begin{aligned}
 x &= -18 + \frac{41}{\gcd(25, 41)}t = -18 + 41t \\
 y &= 11 - \frac{25}{\gcd(25, 41)}t = 11 - 25t
 \end{aligned}$$

8 Exercise 6.10.18

Find integers x and y such that

$$2x + y \equiv 4 \pmod{17} \quad (8.1)$$

$$5x - 5y \equiv 9 \pmod{17} \quad (8.2)$$

Answer:

Because $5 \cdot 7 \equiv 1 \pmod{17}$, we multiply the both sides of Equation 8.2 by $5^{-1} \equiv 7 \pmod{17}$ and get $7(5x - 5y) \equiv 7 \cdot 9 \pmod{17}$, namely,

$$x - y \equiv 12 \pmod{17} \quad (8.3)$$

Adding Equation 8.1 with Equation 8.3, we have $(2x + y) + (x - y) \equiv 4 + 12 \pmod{17}$, namely $3x \equiv 16 \pmod{17}$. Because $3 \cdot 6 \equiv 1 \pmod{17}$, we multiply it by $3^{-1} \equiv 6 \pmod{17}$ and get $6 \cdot 3x \equiv 6 \cdot 16 \pmod{17}$, namely,

$$x \equiv 11 \pmod{17} \quad (8.4)$$

Subtracting Equation 8.1 with Equation 8.3 twice, we have $(2x + y) - 2(x - y) \equiv 4 - 2 \cdot 12 \pmod{17}$, namely $3y \equiv 14 \pmod{17}$. Because $3 \cdot 6 \equiv 1 \pmod{17}$, we multiply it by $3^{-1} \equiv 6 \pmod{17}$ and get $6 \cdot 3y \equiv 6 \cdot 14 \pmod{17}$, namely

$$y \equiv 16 \pmod{17} \quad (8.5)$$

9 Exercise 6.10.19

Prove that $\sqrt[3]{5}$ is irrational.

Answer:

To derive a logic contradiction, we suppose that $\sqrt[3]{5}$ is rational, which can be written as the quotient of two positive integers: $\sqrt[3]{5} = a/b$. Get the cubes of both sides, we have $a^3 = 5b^3$. Consider the prime factorization of both sides. Suppose that 5 occurs m times in the prime factorization of a and n times in the prime factorization of b . Since $a^3 = 5b^3$, we have $3m = 3n + 1$, which is impossible because $3m \equiv 0 \not\equiv 3n + 1 \equiv 1 \pmod{3}$.

10 Exercise 6.10.20

Prove that the two forms of Fermats Theorem, Theorem 6.5.1 and (6.1), are equivalent.

If p is a prime and a is an integer, then $p \mid a^p - a$.

\iff

If p is a prime and a is an integer not divisible by p , then $p \mid a^{p-1} - 1$.

Answer:

\implies : Because $p \nmid a$ and $p \mid a^p - a = a(a^{p-1} - 1)$, p cannot be the factor of a , but must be the factor of $a^{p-1} - 1$, namely $p \mid a^{p-1} - 1$.

\impliedby : $p \mid a^{p-1} - 1 \mid (a^{p-1} - 1)a = a^p - a$

11 Special Problem 1

Define a function $s(n, k)$ for all integers $1 \leq k \leq n$ inductively as follows: $s(n, 1) = s(n, n) = 1$ for all $n \geq 1$, and for $n > 1$, $s(n, k) = ks(n-1, k) + s(n-1, k-1)$ for all $1 < k < n$. Prove that if p is a prime, then $s(p, k)$ is divisible by p for all $1 < k < p$.

(**Hint:** Note that the recurrence relation is similar to the one satisfied by $\binom{n}{k}$. You may first want to interpret $s(n, k)$ in a combinatorial way.)

Answer:

We observe that $s(n, k)$ is the number of ways to partition a set of n elements into k nonempty subsets. $s(n, k)$ contains two cases: to distribute n -th element into the current k subsets, or build a new subset which contains only n -th element. So $s(n, k) = ks(n-1, k) + s(n-1, k-1)$. There is another way to interpret this formula. Enumerate i as the number of elements in the first subset. There are $\frac{1}{k} \binom{n}{i}$ ways to compose the first subset where the divisor k is used to let the subset which contains the minimal remaining element be the first set in order to eliminate the repetition. We rewrite the recurrence formula of $s(n, k)$ as

$$s(n, k) = \frac{1}{k} \sum_{i=1}^{n-k+1} \binom{n}{i} s(n-i, k-1)$$

Lemma 11.1 *The recurrence formula $s(n, k) = \frac{1}{k} \sum_{i=1}^{n-k+1} \binom{n}{i} s(n-i, k-1)$ is equivalent to the recurrence formula $s(n, k) = ks(n-1, k) + s(n-1, k-1)$.*

For a prime p , we have

$$s(p, k) = \frac{1}{k} \sum_{i=1}^{p-k+1} \binom{p}{i} s(p-i, k-1)$$

Applying Lemma 6.5.2 in LPV, we have

$$p \mid \binom{p}{i} \quad (1 \leq i \leq p-k+1)$$

Because p is a prime and $0 < k < p$, $\gcd(k, p) = 1$. Thus,

$$p \mid \frac{1}{k} \binom{p}{i} \mid \frac{1}{k} \binom{p}{i} s(p-i, k-1)$$

Summating all items up, we get

$$p \mid s(p, k)$$

12 Special Problem 2

Review of Chernoff Bounds Let X_1, X_2, \dots, X_n be independent Poisson trials (as discussed in class) such that $\Pr\{X_i = 1\} = p_i$; let $X = \sum_{1 \leq i \leq n} X_i$ and $\mu = E(X)$. In class we stated the following Chernoff bounds: For all $\delta > 0$,

$$\Pr\{X \geq (1 + \delta)\mu\} \leq \left(\frac{e^\delta}{(1 + \delta)^{1+\delta}} \right)^\mu, \quad (12.1)$$

and if $a \geq 6E(X)$, then

$$\Pr\{X \geq a\} \leq 2^{-a}.$$

From the other end, we have for all $0 < \delta < 1$,

$$\Pr\{X \leq (1 - \delta)\mu\} \leq \left(\frac{e^{-\delta}}{(1 - \delta)^{1-\delta}} \right)^\mu. \quad (12.2)$$

Use the above Chernoff Bounds to prove the following inequalities: For all $0 < \delta \leq 1$

(a)

$$\Pr\{X \geq (1 + \delta)\mu\} \leq e^{-\mu\delta^2/3} \quad (12.3)$$

(b)

$$\Pr\{X \leq (1 - \delta)\mu\} \leq e^{-\mu\delta^2/2} \quad (12.4)$$

Remark Note that it follows from (a) and (b) that $\Pr\{|X - E(X)| > a\} \leq 2e^{-a^2/3E(X)}$ for all $0 < a \leq E(X)$.

Answer:

(a) Applying the Chernoff Bounds 12.1, we have

$$\begin{aligned} \Pr\{X \geq (1 + \delta)\mu\} &\leq \left(\frac{e^\delta}{(1 + \delta)^{1+\delta}} \right)^\mu \\ &= \exp \mu [\delta - (1 + \delta) \ln(1 + \delta)] \\ &\leq \exp \mu \left(\frac{-\delta^2}{3} \right) \end{aligned} \quad (\text{by Lemma 12.1})$$

Lemma 12.1 For $\delta \in [0, 1]$, we have

$$\delta - (1 + \delta) \ln(1 + \delta) \leq \frac{-\delta^2}{3}$$

Proof Let

$$f(\delta) = \delta - (1 + \delta) \ln(1 + \delta) + \frac{\delta^2}{3}$$

Calculate the derivative of $f(\delta)$:

$$f'(\delta) = -\ln(1 + \delta) + \frac{2\delta}{3}$$

Because $f'''(\delta) = \frac{1}{(1+\delta)^2} \geq 0$ for $\delta \geq 0$, there doesn't exist the maximal value of $f'(\delta)$ for $\delta \in [0, 1]$. The maximum of $f'(\delta)$: $\max\{f'(0), f'(1)\} \leq 0$. So $f'(\delta) \leq 0$ for $\delta \in [0, 1]$. Because $f(0) = 0$ and $f'(\delta) \leq 0$, $f(\delta) \leq 0$ for $\delta \in [0, 1]$. ■

(b) Applying the Chernoff Bounds 12.2, we have

$$\begin{aligned} \Pr\{X \leq (1 - \delta)\mu\} &\leq \left(\frac{e^{-\delta}}{(1 - \delta)^{1-\delta}}\right)^\mu \\ &= \exp \mu [-\delta - (1 - \delta) \ln(1 - \delta)] \\ &\leq \exp \mu \left(\frac{-\delta^2}{2}\right) \end{aligned} \quad (\text{by Lemma 12.2})$$

Lemma 12.2 For $\delta \in [0, 1]$, we have

$$-\delta - (1 - \delta) \ln(1 - \delta) \leq \frac{-\delta^2}{2}$$

Proof Let

$$f(\delta) = -\delta - (1 - \delta) \ln(1 - \delta) + \frac{\delta^2}{2}$$

Calculate the derivative of $f(\delta)$:

$$f'(\delta) = \ln(1 - \delta) + \delta$$

Because $f(0) = 0$, $f'(0) = 0$ and $f''(\delta) = 1 - \frac{1}{1-\delta} \leq 0$ for $\delta \in [0, 1]$, $f(\delta) \leq 0$ for $\delta \in [0, 1]$. ■

13 Special Problem 3

There are n processors, and m jobs. For each job, we randomly and independently assign it to a processor (with each processor equally likely to be chosen). Let X_i be the random variable corresponding to the number of jobs assigned to processor i , and let $X = \max_{1 \leq i \leq n} X_i$.

(a) Assume $m = 20 \lceil n \ln n \rceil$. Show that $\Pr\{10 \ln n \leq X \leq 40 \ln n\} \geq 1 - \frac{2}{n}$ for all $n > 100$.

(b) Assume $m = n > 10$. Show that there exists a constant $c > 0$ such that, for all n , $\Pr\{X > c \ln n / \ln \ln n\} \leq \frac{1}{n^3}$.

Remark We may describe the assertion of (a) as “ $|X| = \Theta(\ln n)$ with probability $1 - O(1/n)$ ”, and (b) as “ $|X| = O(\ln n / \ln \ln n)$ with probability $1 - O(1/n^3)$ ”.

(c) Assume $m = n$. Suppose each processor can only process the first three jobs assigned to it, and reject any additional jobs. Let Y be the random variable corresponding to the total number of rejected jobs (by all processors). Derive a formula for $g(n) = E(Y)$. Determine the value of $\lim_{n \rightarrow \infty} g(n)/n$.

Answer:

Because each job is assigned randomly and independently to a processor, X_i can be considered as the sum of m 0-1 random variables $X_{i,j}$ by which we denotes whether the j -th job is assigned into the i -th processor.

$$\Pr\{X_i = k\} = \left(\frac{1}{n}\right)^k \left(\frac{n-1}{n}\right)^{m-k} \binom{m}{k}$$

$$E(X_i) = \sum_{k=0}^m k \Pr\{X_i = k\} = \frac{m}{n}$$

(a)

$$E(X_i) = \frac{m}{n} = 20 \ln n$$

$$\begin{aligned} \Pr\{10 \ln n \leq X \leq 40 \ln n\} &= \Pr\left\{\bigcap_{i=1}^n (X_i \leq 40 \ln n)\right\} - \Pr\left\{\bigcap_{i=1}^n (X_i < 10 \ln n)\right\} \\ &= 1 - \Pr\left\{\bigcup_{i=1}^n (X_i > 40 \ln n)\right\} - \Pr\left\{\bigcap_{i=1}^n (X_i < 10 \ln n)\right\} \\ &\geq 1 - \sum_{i=1}^n \Pr\{X_i > 40 \ln n\} - \sum_{i=1}^n \Pr\{X_i < 10 \ln n\} \\ &\geq 1 - n \Pr\{X_i > (1+1)E(X_i)\} - n \Pr\{X_i < (1-0.5)E(X_i)\} \\ &\geq 1 - n \exp\left(E(X_i) \left(\frac{-1^2}{3}\right)\right) - n \exp\left(E(X_i) \left(\frac{-0.5^2}{2}\right)\right) \\ &\hspace{15em} \text{(by Inequality 12.3 and 12.4)} \\ &= 1 - \frac{1}{n^{17/3}} - \frac{1}{n^{3/2}} \\ &\geq 1 - \frac{1}{n} - \frac{1}{n} \\ &= 1 - \frac{2}{n} \end{aligned}$$

(b) Similarly,

$$E(X_i) = \frac{m}{n} = 1$$

$$\begin{aligned} \Pr\{X > \frac{c \ln n}{\ln \ln n}\} &= \Pr\left\{\bigcup_{i=1}^n (X_i > \frac{c \ln n}{\ln \ln n})\right\} \\ &\leq \sum_{i=1}^n \Pr\{X_i > \frac{c \ln n}{\ln \ln n}\} \\ &= n \Pr\{X_i > (1 + \frac{c \ln n}{\ln \ln n} - 1)E(X_i)\} \\ &\leq n \exp\left(\frac{-E(X_i)}{3} \left(\frac{c \ln n}{\ln \ln n} - 1\right)^2\right) \hspace{5em} \text{(by Inequality 12.3)} \\ &\leq n \exp\left(\frac{-(2\sqrt{\ln n})^2}{3}\right) \hspace{5em} \text{(by Lemma 13.1)} \\ &= \frac{1}{n^{1/3}} \end{aligned}$$

Lemma 13.1 *There exists a constant c such that for large enough n ,*

$$c \ln n / \ln \ln n - 1 \geq 2\sqrt{\ln n}$$

Proof

$$\begin{aligned} \lim_{n \rightarrow +\infty} \frac{2\sqrt{\ln n}}{\ln n / \ln \ln n} &= \lim_{n \rightarrow +\infty} \frac{\sqrt{\ln n} \ln \ln n}{\ln n} \\ &= \lim_{n \rightarrow +\infty} \frac{2 + \ln \ln n}{\sqrt{\ln n}} && \text{(by L'Hospital Principle)} \\ &= \lim_{n \rightarrow +\infty} \frac{1}{\sqrt{n} \ln n} && \text{(by L'Hospital Principle)} \\ &= 0 \end{aligned}$$

So $2\sqrt{\ln n} = o(\ln n / \ln \ln n)$. Thus, there exists a constant c such that for large enough n , $c \ln n / \ln \ln n - 1 \geq 2\sqrt{\ln n}$ ■

- (c) Denote the number of jobs rejected by the i -th processor by Y_i . Enumerating k as X_i , there is $\binom{m}{k}$ ways to choose X_i jobs with probability $\frac{(n-1)^{m-k}}{n^m}$. So

$$E(Y_i) = E(\max\{X_i - 3, 0\}) = \sum_{k=3}^m (k-3) \binom{m}{k} \frac{(n-1)^{m-k}}{n^m}$$

$$\begin{aligned} E(Y) &= \sum_{i=1}^n E(Y_i) \\ &= \sum_{i=1}^n \sum_{k=3}^m (k-3) \binom{m}{k} \frac{(n-1)^{m-k}}{n^m} \\ &= \frac{n}{n^m} \frac{d}{dx} \left(\frac{1}{x^3} \left((n-1+x)^m - \sum_{k=0}^2 x^k \binom{m}{k} (n-1)^{m-k} \right) \right) \Big|_{x=1} \\ &= \frac{n}{n^m} \left(\frac{(n-1+x)^{m-1} (mx - 3x - 3n + 3)}{x^4} \right. \\ &\quad \left. + \frac{3(n-1)^m}{x^4} + \frac{2m(n-1)^{m-1}}{x^3} + \frac{(m-1)m(n-1)^{m-2}}{2x^2} \right) \Big|_{x=1, n=m} \\ &= \frac{n}{n^m} \left(-2n^n + 3(n-1)^n + 2(n-1)^{n-1}n + \frac{1}{2}(n-1)^{n-1}n \right) \\ &= -2n + \frac{1}{2}(11n-6)(1-1/n)^{n-1} \end{aligned}$$

$$\begin{aligned} \lim_{n \rightarrow +\infty} \frac{E(Y)}{n} &= \lim_{n \rightarrow +\infty} \left(-2 + \frac{1}{2}(11-6/n)(1-1/n)^{n-1} \right) \\ &= \lim_{n \rightarrow +\infty} \left(-2 + \frac{1}{2}(11-6/n) \frac{1}{e} \right) \\ &= \frac{11}{2e} - 2 \end{aligned}$$

14 Special Problem 4

In class we discussed the *Hypercube Network*, which is a directed graph on the vertex set $V = \{0, 1\}^n$ with n directed edges from each vertex i to its n neighbors (each neighbor being at Hamming distance 1 from i). Thus, there are $N = 2^n$ vertices and Nn (directed) edges. Let $\Omega = (U, p)$ be the probability space where U is the set of all $d = (d_0, d_1, \dots, d_{N-1})$ with $d_i \in V$, and $p(u) = 1/|U|$ for all $u \in U$. Take a random d , and let ρ_j be the path followed from j to d_j under the fixing-bit routing algorithm.

Take a random $d \in U$. For each edge e , let L_e denote the random variable corresponding to the number of vertices $j \in V$ such that ρ_j contains e . Prove the following claims:

(a) $E(L_e) = E(L_{e'})$ for all edges e, e' .

(b) $\sum_{\text{all edges } e} E(L_e) = Nn/2$.

Remark Note that it follows from (a) and (b) that $E(L_e) = 1/2$ for all e .

Answer:

Let us consider the configuration on the edge $e = (i, j)$ where

$$i = (a_1, a_2, \dots, a_k, \dots, a_n), \quad j = (a_1, a_2, \dots, 1 - a_k, \dots, a_n).$$

Based on the bit-fixing routing strategy, a package v_x from x to $\sigma(x)$ via the edge (i, j) satisfies that the sequence $(a_1, a_2, \dots, 1 - a_k)$ must be the prefix sequence of $\sigma(x)$ and the sequence $(a_k, a_{k+1}, \dots, a_n)$ must be the suffix sequence of x . The first $k - 1$ elements of x are free variable. Let S be the set of the start nodes whose path will be via the edge e .

$$S = \{(x_1, x_2, \dots, x_{k-1}, a_k, a_{k+1}, \dots, a_n) \mid x_i \in \{0, 1\} \quad (i = 1, 2, \dots, k - 1)\}$$

Obviously, $|S| = 2^{k-1}$. The last $n - k$ elements of $\sigma(x)$ are free variable. Let T be the set of the finish nodes whose path will be via the edge e .

$$T = \{(a_1, a_2, \dots, 1 - a_k, x_1, x_2, \dots, x_{n-k}) \mid x_i \in \{0, 1\} \quad (i = 1, 2, \dots, n - k)\}$$

Obviously, $|T| = 2^{n-k}$.

Enumerate x which is the number of the nodes whose path via the edge e . There are $\binom{|S|}{x}$ ways to choose x start nodes from S and $|T|^x (2^n - |T|)^{|S|-x}$ ways to choose x finish nodes from T . So the expected values of L_e can be calculated as following:

$$\begin{aligned}
E(L_e) &= \frac{1}{(2^n)^{|S|}} \sum_{x=0}^{|S|} x |T|^x (2^n - |T|)^{|S|-x} \binom{|S|}{x} \\
&= \frac{1}{(2^n)^{|S|}} \frac{d}{dz} \left(\sum_{x=0}^{|S|} z^x |T|^x (2^n - |T|)^{|S|-x} \binom{|S|}{x} \right) \Big|_{z=1} \\
&= \frac{1}{(2^n)^{|S|}} \frac{d}{dz} \left((z|T| + 2^n - |T|)^{|S|} \right) \Big|_{z=1} \\
&= \frac{1}{(2^n)^{|S|}} |S||T| \left((z|T| + 2^n - |T|)^{|S|-1} \right) \Big|_{z=1} \\
&= \frac{|S||T| (2^n)^{|S|-1}}{(2^n)^{|S|}} = \frac{2^{n-k+k-1}}{2^n} = \frac{1}{2}
\end{aligned}$$

The claims below is obvious based on the conclusion above.

- (a) For any pair of edges e and e' ,

$$E(L_e) = E(L_{e'}) = 1/2$$

- (b) There are Nn directed edge in total. So

$$\sum_{\text{all edges } e} E(L_e) = NnE(L_e) = \frac{Nn}{2}$$