

数学建模课程笔记

yangmei

2023 年 12 月 13 日

目录

| | |
|---|-----------|
| 第一章 Secret Sharing | 1 |
| 1.1 秘密共享 | 1 |
| 1.2 Combinatorial Mathematics | 1 |
| 1.3 Shamir's Threshold Scheme | 2 |
| 1.3.1 Lagrange Polynomial interpolation | 2 |
| 1.3.2 Shamir 门限机制 (t, n) | 3 |
| 1.4 Asmuth-Bloom's Threshold Scheme | 3 |
| 1.4.1 中国剩余定理 | 3 |
| 1.4.2 Asmuth-Bloom 门限机制 (t, n) | 5 |
| 第二章 Page Rank | 7 |
| 2.1 网页重要度 | 7 |
| 2.2 随机矩阵 | 9 |
| 2.3 链接矩阵 | 10 |
| 2.3.1 悬挂网页修正 | 10 |
| 2.3.2 多解修正 | 11 |
| 2.3.3 重要度向量的存在唯一性 | 12 |
| 2.4 矩阵计算 | 14 |
| 2.4.1 幂法迭代 | 14 |
| 2.4.2 完全正、列随机矩阵的幂法收敛性 | 14 |
| 2.5 随机浏览 | 15 |
| 第三章 数论与组合模型 | 16 |
| 3.1 Nim Game | 16 |

| | |
|--|-----------|
| 目录 | II |
| 3.1.1 位值制计数法 | 16 |
| 3.1.2 Nim Game 的必胜策略 | 16 |
| 3.2 伪币称重问题 | 18 |
| 3.2.1 自适应方案 | 18 |
| 3.2.2 非自适应方案 | 19 |
| 第四章 随机模型 | 20 |
| 4.1 疾病检测 | 20 |
| 4.1.1 概率群试 (group testing) | 20 |
| 4.1.2 The Monty Hall Problem | 21 |

第一章 Secret Sharing

1.1 秘密共享

Secret Sharing: 将秘密分成若干份, 分发给不同的用户。用户特定子集共同提供各自的份额, 才能重构初始秘密。

Threshold Scheme(t, n): 在 n 人之间共享秘密, 其中任意 $t \leq n$ 个人可求出秘密, 任意 $t - 1$ 个人无法求出秘密。

1.2 Combinatorial Mathematics

问题: Eleven scientists are working on a secret project. They wish to lock up the documents in a cabinet so that the cabinet can be opened if and only if six or more of the scientists are present. What is the smallest number of locks needed? What is the smallest number of keys to the locks each scientist must carry?

采用组合数学的方法: “少数”与“多数”:

1. 设相关人共有 $2n + 1$ 个, 任意 n 人组成的“少数”团体不能打开安全门, 任意 $n + 1$ 人组成的“多数”团体可以打开安全门
2. 两个不同的“少数”团体联合必包含某个多数团体
3. 任一“少数”团体和不属该团体的任一人联合可成为多数团体

锁与钥匙:

1. 安全门上至少需要 $\binom{2n+1}{n}$ 把锁 $\binom{11}{5} = 462$

任一“少数”团体至少有一把锁不能打开

任意两个少数” 各不相同

2. 每个人至少需要 $\binom{2n}{n}$ 把钥匙 $\binom{10}{5} = 252$ 每个人需拥有他所不属于的所有少数” 团体所打不开的锁的钥匙

用数学上集合的语言来表述：给锁编号 $1, 2, \dots, l$ ，打开所有门的钥匙的全集即为 $K = 1, 2, \dots, l$ ，任意第 i 人拥有的钥匙集合为 S_i ，则满足：

- (1) $S_{i_1} \cup S_{i_2} \cup \dots \cup S_{i_n} \subset K/k_i$
 (2) $S_{i_1} \cup S_{i_2} \cup \dots \cup S_{i_n} \cup S_{i_{n+1}} = K$

则有：

1. 那么对于不同的 n 的并，所对应的 k_i 不同，任意一个 k_i 必有一族 $\{i_1, i_2, \dots, i_n\}$ 与之对应则 $k_i \in K$ 共有 C_{2n+1}^n 个
 2. $k_i \in S_{i_{n+1}}$ ，这样的 k_i 有 C_{2n+1}^{n+1} 个

1.3 Shamir's Threshold Scheme

1.3.1 Lagrange Polynomial interpolation

定理 1.3.1. *Given k points in the 2-dimensional plane $(x_1, y_1) \dots (x_k, y_k)$. with distinct x_i 's, there is one and only one polynomial $q(x)$ of degree $k - 1$ such that $q(x_i) = y_i$ for all x_i .*

设多项式 $q(x) = a_0 + a_1x + a_2x^2 + \dots + a_{k-1}x^{k-1}$, $\deg(q) = k - 1$ ，利用 $k - 1$ 组值求得 $q(x)$ 的各项系数系数矩阵：

$$\begin{vmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{k-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_k & x_k^2 & \cdots & x_k^{k-1} \end{vmatrix} \neq 0$$

这是一个 Vandermode 行列式

1.3.2 Shamir 门限机制 (t, n)

任选 $t - 1$ 个整数 x_1, x_2, \dots, x_{t-1} 和 n 个互不相同的整数 c_1, c_2, \dots, c_n 。素数 $p > n + 1$ 求 $b_j \equiv (K + c_j x_1 + c_j^2 x_2 + \dots + c_j^{t-1} x_{t-1}) \pmod{p}, j = 1, \dots, n$ 其中 $K \in \mathbb{Z}$ 为秘密

$$f(c) = K + x_1 c + x_2 c^2 + \dots + x_{t-1} c^{t-1}, b_j \equiv f(c_j) \pmod{p}, j = 1, \dots, n$$

将秘密份额 (c_j, b_j) 告知第 j 人

证明. 证明 Shamir 门限机制的合理性

(1) 若 t 个人 j_1, \dots, j_t 共享秘密份额 $(c_{j_i}, b_{j_i}), i = 1, \dots, t$

方程组 $b_i \equiv (K + c_{j_i} x_1 + c_{j_i}^2 x_2 + \dots + c_{j_i}^{t-1} x_{t-1}) \pmod{p}, i = 1, \dots, t$ 在模 p 意义下有唯一解由于系数矩阵为

$$\begin{vmatrix} 1 & c_1 & c_1^2 & \dots & c_1^{t-1} \\ 1 & c_2 & c_2^2 & \dots & c_2^{t-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & c_{t-1} & c_{t-1}^2 & \dots & c_{t-1}^{t-1} \\ 1 & c_t & c_t^2 & \dots & c_t^{t-1} \end{vmatrix} \neq 0$$

其行列式为 Vandermode 行列式, 即 $\det = \prod_{i=1}^{t-1} (c_i - c_{i+1})$, 因此 $\det \neq 0$ 同时 $\text{rank}(\text{row}) = \text{rank}(\text{column})$, 方程有唯一解。

(2) 若 $t - 1$ 个人 j_1, \dots, j_{t-1} 共享秘密份额 $(c_{j_i}, b_{j_i}), i = 1, \dots, t - 1$

方程组 $b_{j_i} \equiv (K + c_{j_i} x_1 + c_{j_i}^2 x_2 + \dots + c_{j_i}^{t-1} x_{t-1}) \pmod{p}, i = 1, \dots, t - 1$ 含 $t - 1$ 个方程, t 个未知数, 在模 p 意义下有无穷多组解

□

1.4 Asmuth-Bloom's Threshold Scheme

1.4.1 中国剩余定理

定义 1.4.1 (逆). 设 a, b 为整数, m 为正整数, 若 $ab \equiv 1 \pmod{m}$, 则称 a 模 m 可逆, 且 b 是 a 在模 m 意义下的逆元, 记为 $a^{-1} \pmod{m}$

a 对模 m 可逆的 $\Leftrightarrow (a, m) = 1$, 即 a 与 m 互质

| | | | | | |
|--------------------------|----|----|--|--|--|
| $27^{-1} \pmod{64} = 19$ | | | | | |
| | 1 | 27 | | | |
| | | 64 | | | |
| $64 = 2 \times 27 + 10$ | 1 | 27 | | | |
| | 2 | 10 | | | |
| $27 = 2 \times 10 + 7$ | 5 | 7 | | | |
| $1 + 2 \times 2 = 5$ | 2 | 10 | | | |
| $10 = 1 \times 7 + 3$ | 5 | 7 | | | |
| $5 + 1 \times 2 = 7$ | 7 | 3 | | | |
| $7 = 2 \times 3 + 1$ | 19 | 1 | | | |
| $5 + 2 \times 7 = 19$ | 7 | 3 | | | |

大衍求一數云置奇右上一定居右下立天元一於左上
先以右上除右下所得商數與左上一相生入左下然
後乃以右行上下以少除多遞互除之所得商數隨即
遞互累乘歸左行上下須使右上末後奇一而止乃驗
左上所得以爲乘率或奇數已見單一者便爲乘率此按

例 1.4.2 (大衍求一術求逆元).

定义 1.4.3 (一次同余方程). 形如 $ax \equiv b \pmod{m}$ 的方程, 其中 a, b, m 为整数, $m > 0$.

定理 1.4.4 (线性同余方程有解和唯一). (1) 当且仅当 $\gcd(a, m) | b$ 时, 线性同余方程有解。

(2) 当 $\gcd(a, m) = 1$ 时, 方程的解为 $a^{-1}b$, 且小于 m 的非负整数解唯一。

其中 a^{-1} 是 a 在模 m 意义下的逆元。

定理 1.4.5 (中国剩余定理 (数论)). 设 m_1, m_2, \dots, m_k 为两两互质的正整数, a_1, a_2, \dots, a_k 为任意整数, 记 $M = m_1 m_2 \cdots m_k$, 则一次同余方程组

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

(1) 有小于 M 的唯一正整数解 $x = M_1 M_1^{-1} a_1 + M_2 M_2^{-1} a_2 + \cdots + M_k M_k^{-1} a_k \pmod{M}$, 其中 $M_i = M/m_i$, M_i^{-1} 是 M_i 在模 m_i 意义下的逆元。

(2) 对任意 $l \in \mathbb{Z}$, $x + l \cdot m$ 也是同余方程组的解。

定理 1.4.6 (中国剩余定理 (代数多项式)). 设 $f_i(x)|i=1, \dots, n$ 是两两互素的多项式, $a_1(x), a_2(x), \dots, a_n(x)$ 是 n 个多项式, 则存在多项式 $g(x)$, $q_i(x)(i=1, 2, \dots, n)$, 使得 $g(x) = f_i(x)q_i(x) + a_i(x)$ 对一切 i 成立。

例 1.4.7 (物不知数).

$$\begin{cases} x \equiv 2(\text{mod}3) & N_1 = 5 \cdot 7 = 35 & N_1^{-1}(\text{mod}3) = 2 \\ x \equiv 3(\text{mod}5) & N_2 = 3 \cdot 7 = 21 & N_2^{-1}(\text{mod}5) = 1 \\ x \equiv 2(\text{mod}7) & N_3 = 3 \cdot 5 = 15 & N_3^{-1}(\text{mod}7) = 1 \end{cases}$$

$$m = 3 \cdot 5 \cdot 7 = 105 \quad 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 2 = 233$$

$$x = 23 \equiv 233 \pmod{105}$$

1.4.2 Asmuth-Bloom 门限机制 (t, n)

设秘密为 K

(1) 选取整数 p 与 m_1, \dots, m_n

$p > K$ 且 p 与 $m_j, 1 \leq j \leq n$ 互素, $m_1 < \dots < m_n$ 且 m_1, \dots, m_n 两两互素

$$\frac{m_1 \cdots m_t}{m_{n-t+2} \cdots m_n} > p$$

即为 m_1, \dots, m_n 中任意 t 个数的乘积与任意 $t-1$ 个数的乘积之比大于 p

(2) 令 $K' = K + r \cdot p$, 其中 $r \in \mathbb{N}$ 满足

$$(i) 0 \leq r \leq \frac{m_1 \cdots m_t}{p} - 1$$

$$(ii) K' = K + r \cdot p \leq K + m_1 \cdots m_t - p < m_1 \cdots m_t$$

再令 $k_j \equiv K'(\text{mod}m_j), 1 \leq j \leq n$, 将秘密份额 (k_j, m_j) 告知第 j 人

证明. 证明 Asmuth-Bloom 门限机制的合理性

$k_j \equiv K'(\text{mod}m_j), 1 \leq j \leq n$, 因此 K' 满足的方程: $K' \equiv k_j(\text{mod}m_j), 1 \leq j \leq n$

$K' = K + r \cdot p < m_1 \cdots m_t$, K' 对 p 取模求出 K : $K \equiv K'(\text{mod}p)$

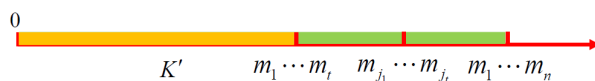
一次同余方程组 (I) $x \equiv k_j(\text{mod}m_j), 1 \leq j \leq n$ 有唯一的小于 $m_1 \cdots m_n$ 的非负整数解 K'

(1) 若 t 个人 j_1, \dots, j_t 共享秘密份额 $(k_{j_i}, m_{j_i}), i = 1, \dots, t$

一次同余方程组 (II) $x \equiv k_{j_i}(\text{mod}m_{j_i}), i = 1, \dots, t$ 有唯一的小于 $m_{j_1} \cdots m_{j_t}$ 的正整数

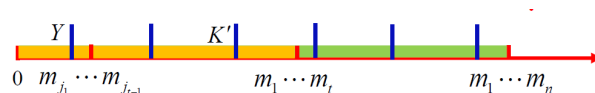
解 X

K' 也为方程 (II) 的解, 且 $K' < m_1 \cdots m_t < m_{j_1} \cdots m_{j_t}$ 。由中国剩余定理, 解的唯一性有 $K' = X$



(2) 若 $t-1$ 个人 j_1, \dots, j_{t-1} 共享秘密份额 $(k_{j_i}, m_{j_i}), i = 1, \dots, t-1$ 一次同余方程组 (III) $x \equiv k_{j_i} \pmod{m_{j_i}}, i = 1, \dots, t-1$ 有唯一的小于 $m_{j_1} \cdots m_{j_{t-1}}$ 的正整数解 Y

$Y + l \cdot m_{j_1} \cdots m_{j_{t-1}} < \frac{1+l}{p} * m_{j_1} m_{j_2} \cdots m_{j_t}, l \in \mathbb{Z}$ 均为方程组 (III) 的解, K' 为这些解中的某一个, K' 的限制条件仅有 $K' < m_1 m_2 \cdots m_t$, 因此 K' 不能唯一确定



□

(1)Liu, C.L. Introduction to Combinatorial Mathematics. McGraw-Hill,1968

(2) Shamir A. How to share a secret. Communications of the ACM, 1979, 22(11): 612-613.

(3) Asmuth AC, Bloom J. A modular approach to key safeguarding. IEEE Transactions on Information Theory, 29, 208-210, 1983.

第二章 Page Rank

2.1 网页重要度

网页重要度的原则与假设

某网页重要，是因为有重要的网页链接到它，对任一网页 A ，确定一数值为其重要度，作为网页排序的依据链接到网页 A 的所有网页对网页 A 的重要度均有贡献，贡献大小与这些网页自身的重要度有关

1. (传递性) 重要度大的网页链接到网页 A 时对网页 A 的重要度的贡献比重要度小的网页链接到网页 A 时对网页 A 的重要度的贡献大：某网页对其它网页重要度的贡献之和等于它的重要度
2. (等效性) 网页对它所链接的每个网页的重要度的贡献相等：某网页对其它网页的重要度贡献与它所链接的网页数量呈反比
3. (叠加性) 链接到网页 A 的网页越多，网页 A 越重要：网页 A 的重要度是所有链接到 A 的网页对网页 A 的重要度的贡献之和
4. (无关性) 网页链接其它网页的多少，与其本身的重要度无关

网页链接图

定义 2.1.1 (网页链接图). 互联网中网页之间的链接关系可用图表示，称为网络链接图。

顶点 网页 $\nu_1, \nu_2, \dots, \nu_n$

弧 网页间的链接关系，即若网页 ν_i 上有链接指向网页 ν_j ，则网络链接图中有一条以 ν_i 为起点， ν_j 为终点的弧

出度 以某顶点为起点的弧的总数，即该网页链接的网页数量

网页重要度的矩阵表示

网页 ν_i 的重要度记为 x_i 出度记为 q_i

传递性 网页 ν_i 对其它网页重要度贡献之和为 x_i

等效性 网页 ν_i 对它链接的 q_i 个网页中的任一个的重要度贡献为 $\frac{x_i}{q_i}$

叠加性 若链接到网页 ν_j 的网页有 $\nu_{j_1}, \nu_{j_2}, \dots, \nu_{j_k}$, 则

$$x_j = \frac{x_{j_1}}{q_{j_1}} + \frac{x_{j_2}}{q_{j_2}} + \dots + \frac{x_{j_k}}{q_{j_k}}$$

记 p_{ij} 为网页 v_i 到 v_j 的链接概率, 即 v_i 链接到 v_j 的概率, 有

$$p_{ij} = \begin{cases} \frac{1}{q_j}, & \text{若 } v_j \text{ 链接到 } v_i \\ 0, & \text{若 } v_j \text{ 不链接到 } v_i \end{cases}$$

所以, 上式改写为

$$x_i = \sum_{j=1}^n p_{ij} x_j$$

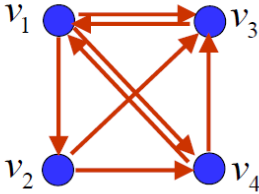
记矩阵 $\mathbf{P} = (p_{ij})_{n \times n}$ 为初始链接矩阵 (网页 v_j 的出度列向量 $\mathbf{p}_j = (p_{1j}, p_{2j}, \dots, p_{nj})^T$, $\mathbf{x} = (x_1, x_2, \dots, x_n)^T$ 为网页重要度向量, 则 \mathbf{x} 为线性方程 $\mathbf{x} = \mathbf{P}\mathbf{x}$ 的解。

$$\mathbf{x} = \mathbf{P}\mathbf{x} \quad (2.1)$$

(1) \mathbf{x} 是 \mathbf{P} 的特征向量, 对应的特征值为 1。

(2) $\text{Rank}(\mathbf{I} - \mathbf{P}) < n$ 由于 $\mathbf{1}^T(\mathbf{I} - \mathbf{P}) = \mathbf{0}$, 即说明其行向量线性相关, 因此方程 (2.1) 有非零解

(3) 方程 (2.1) 一定有非零解吗, 即重要度向量 \mathbf{x} 一定存在吗, 以及存在一定唯一吗, 这个问题之后分析。

$$\begin{cases} x_1 = & x_3 + \frac{1}{2}x_4 \\ x_2 = \frac{1}{3}x_1 \\ x_3 = \frac{1}{3}x_1 + \frac{1}{2}x_2 & + \frac{1}{2}x_4 \\ x_4 = \frac{1}{3}x_1 + \frac{1}{2}x_2 \end{cases}$$


$$\mathbf{P} = \begin{pmatrix} 0 & 0 & 1 & 1/2 \\ 1/3 & 0 & 0 & 0 \\ 1/3 & 1/2 & 0 & 1/2 \\ 1/3 & 1/2 & 0 & 0 \end{pmatrix}$$

| | 1 | 2 | 3 | 4 |
|----|----------------|----------------|----------------|----------------|
| 1 | | | $\sqrt{\quad}$ | |
| 2 | $\sqrt{\quad}$ | | | |
| 3 | $\sqrt{\quad}$ | $\sqrt{\quad}$ | | $\sqrt{\quad}$ |
| 4 | $\sqrt{\quad}$ | $\sqrt{\quad}$ | | $\sqrt{\quad}$ |
| 出度 | 3 | 2 | 1 | 4 |

$$\mathbf{I} - \mathbf{P} = \begin{pmatrix} 1 & 0 & -1 & -1/2 \\ -1/3 & 1 & 0 & 0 \\ -1/3 & -1/2 & 1 & -1/2 \\ -1/3 & -1/2 & 0 & 1 \end{pmatrix}$$

$$x_1 = \frac{12}{31}, x_2 = \frac{4}{31}, x_3 = \frac{9}{31}, x_4 = \frac{6}{31}$$

例 2.1.2 (链接矩阵与重要度向量的求解).

2.2 随机矩阵

定义 2.2.1. 各行 (列) 元素之和均为 1 的非负方阵称为行 (列) 随机矩阵 (row(column) stochastic matrix)

各行与各列元素之和均为 1 的非负方阵称为双随机矩阵 (doubly stochastic matrix)

命题 2.2.2. 随机矩阵一定存在特征值为 1 对应的特征向量

证明. 上文已经简单地从行秩的角度说明了 $(\mathbf{P} - \mathbf{I})\mathbf{x} = 0$ 有非零解, 下面以列随机矩阵从行列式的角度证明 $\det(\mathbf{P} - \mathbf{I}) = 0$, 从而证明行列式有非零解。

$$\begin{aligned}
\det(\mathbf{P} - \mathbf{I}) &= \begin{vmatrix} p_{11} - 1 & p_{12} & \cdots & p_{1n} \\ p_{21} & p_{22} - 1 & \cdots & p_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n1} & p_{n2} & \cdots & p_{nn} - 1 \end{vmatrix} \\
&= \begin{vmatrix} \sum_{i=1}^n p_{i1} - 1 & \sum_{i=1}^n p_{i2} & \cdots & \sum_{i=1}^n p_{in} \\ p_{21} & p_{22} - 1 & \cdots & p_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n1} & p_{n2} & \cdots & p_{nn} - 1 \end{vmatrix} = \begin{vmatrix} 0 & 0 & \cdots & 0 \\ p_{21} & p_{22} - 1 & \cdots & p_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n1} & p_{n2} & \cdots & p_{nn} - 1 \end{vmatrix} = 0
\end{aligned}$$

□

定理 2.2.3 (随机矩阵的模最大特征值). 任一随机矩阵的模最大特征值为 1

证明. 设 λ 是行随机矩阵 $\mathbf{P} = (p_{ij})_{n \times n}$ 的特征值, 非零向量 $\mathbf{X} = (x_1, \dots, x_n)^T$ 为属于特征值 λ 的特征向量。设 $|x_i| = \max_{1 \leq j \leq n} |x_j| > 0$

由 $\mathbf{P}\mathbf{X} = \lambda\mathbf{X}$, 可得 $\lambda x_i = \sum_{j=1}^n p_{ij} x_j$ 。两边取模, $|\lambda| |x_i| = |\lambda x_i| = |\sum_{j=1}^n p_{ij} x_j| \leq \sum_{j=1}^n |p_{ij}| |x_j| \leq |x_i| \sum_{j=1}^n |p_{ij}| = |x_i|$, 即 $|\lambda| \leq 1$ □

2.3 链接矩阵

链接矩阵的基本性质

- (1) 链接矩阵 \mathbf{P} 的每列元素之和为 1, 为列随机矩阵
- (2) 链接矩阵 \mathbf{P} 一定存在特征值为 1 的非零特征向量
- (3) $\mathbf{1}^T \mathbf{P} = \mathbf{1}^T$

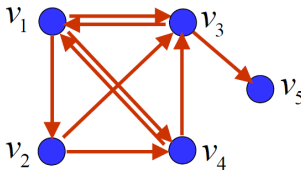
2.3.1 悬挂网页修正

悬挂网页 (dangling link): 若某网页不链接任意其它网页

悬挂网页修正: 将链接矩阵 \mathbf{P} 中对应列的所有元素由 0 修改为 $\frac{1}{n}$, 得到修正链接矩阵 $\bar{\mathbf{P}}$

$$\bar{\mathbf{P}} = \mathbf{P} + \frac{1}{n} \mathbf{1} \mathbf{d}^T$$

其中 $\mathbf{1}$ 为分量全为 0 的列向量。



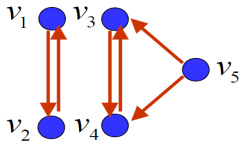
$$\mathbf{P} = \begin{pmatrix} 0 & 0 & 1/2 & 1/2 & 0 \\ 1/3 & 0 & 0 & 0 & 0 \\ 1/3 & 1/2 & 0 & 1/2 & 0 \\ 1/3 & 1/2 & 0 & 0 & 0 \\ 0 & 0 & 1/2 & 0 & 0 \end{pmatrix}$$

$$\bar{\mathbf{P}} = \begin{pmatrix} 0 & 0 & \frac{1}{2} & \frac{1}{2} & \frac{1}{5} \\ \frac{1}{3} & 0 & 0 & 0 & \frac{1}{5} \\ \frac{1}{3} & \frac{1}{2} & 0 & \frac{1}{2} & \frac{1}{5} \\ \frac{1}{3} & \frac{1}{2} & 0 & 0 & \frac{1}{5} \\ 0 & 0 & \frac{1}{2} & 0 & \frac{1}{5} \end{pmatrix} = \begin{pmatrix} 0 & 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{3} & 0 & 0 & 0 & 0 \\ \frac{1}{3} & \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ \frac{1}{3} & \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 & \frac{1}{5} \\ 0 & 0 & 0 & 0 & \frac{1}{5} \\ 0 & 0 & 0 & 0 & \frac{1}{5} \\ 0 & 0 & 0 & 0 & \frac{1}{5} \\ 0 & 0 & 0 & 0 & \frac{1}{5} \end{pmatrix} = \mathbf{P} + \frac{1}{5} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

例 2.3.1 (悬挂网页修正).

2.3.2 多解修正

若 \mathbf{P} 有两个属于特征值 1 的线性无关的特征向量重要度向量排序不唯一



$$\mathbf{P} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1/2 \\ 0 & 0 & 1 & 0 & 1/2 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

图 2.1: 修正矩阵 $\bar{\mathbf{P}}$ 具有两个特征值为一的特征向量 (重要度向量)

将 $\bar{\mathbf{P}}$ 修改为最终的链接矩阵, 修正方法:

$$\bar{\bar{\mathbf{P}}} = \alpha \bar{\mathbf{P}} + (1 - \alpha) \frac{1}{n} \mathbf{1} \mathbf{1}^T$$

其中参数 $\alpha = 0.85$

$\bar{\bar{\mathbf{P}}}$ 为完全正矩阵 (totally positive matrix) 与列随机矩阵:

$$\mathbf{1}^T \bar{\bar{\mathbf{P}}} = \alpha \mathbf{1}^T \bar{\mathbf{P}} + (1 - \alpha) \mathbf{1}^T \mathbf{1} \mathbf{1}^T = \alpha \mathbf{1}^T + (1 - \alpha) \mathbf{1}^T = \mathbf{1}^T$$

$$\bar{\mathbf{P}} = 0.85 \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0.5 \\ 0 & 0 & 1 & 0 & 0.5 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} + 0.15 \cdot \frac{1}{5} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 0.03 & 0.88 & 0.03 & 0.03 & 0.03 \\ 0.88 & 0.03 & 0.03 & 0.03 & 0.03 \\ 0.03 & 0.03 & 0.03 & 0.88 & 0.455 \\ 0.03 & 0.03 & 0.88 & 0.03 & 0.455 \\ 0.03 & 0.03 & 0.03 & 0.03 & 0.03 \end{pmatrix}$$

图 2.2: 多解修正

2.3.3 重要度向量的存在唯一性

根据随机矩阵存在特征值为 1 的特征向量，因此链接矩阵的重要度向量一定存在。下证它的唯一性。

引理 2.3.2. 完全正、列随机矩阵属于特征值的特征向量分量之和不为 0。

证明. 设 \mathbf{x} 是完全正、列随机矩阵 \mathbf{P} 的属于特征值 1 的特征向量，则 $x_i = \sum_{j=1}^n \bar{p}_{ij} x_j$

若 $\sum_{i=1}^n x_i = 0$ ，则 \mathbf{x} 的分量有正有负，故

$$|x_i| = \left| \sum_{j=1}^n \bar{p}_{ij} x_j \right| < \sum_{j=1}^n \bar{p}_{ij} |x_j|$$

故而

$$\sum_{i=1}^n |x_i| < \sum_{i=1}^n \sum_{j=1}^n \bar{p}_{ij} |x_j| = \sum_{j=1}^n \sum_{i=1}^n \bar{p}_{ij} |x_j| = \sum_{j=1}^n (|x_j| \sum_{i=1}^n \bar{p}_{ij}) = \sum_{j=1}^n |x_j|$$

矛盾。 □

命题 2.3.3. 完全正、列随机矩阵仅有 1 个属于特征值 1 的线性无关的特征向量。

证明. 设 $\mathbf{v} = (v_1, v_2, \dots, v_n)^T$, $\mathbf{w} = (w_1, w_2, \dots, w_n)^T$ 是完全正、列随机矩阵 \mathbf{P} 的两个属于特征值 1 的线性无关的特征向量。令 $x_i = -\frac{W}{V}v_i + w_i, i = 1, 2, \dots, n$ ，其中 $W = \sum_{i=1}^n w_i, V = \sum_{i=1}^n v_i \neq 0$ 。

首先若向量 $\mathbf{x} = (x_1, x_2, \dots, x_n)$ 是 \mathbf{P} 的特征值为 λ 的特征向量 $\Leftrightarrow \forall i, \sum_{j=1}^n p_{ij} x_j = \lambda x_i$ ，根据特征向量的定义即可证得。

由 \mathbf{v} 和 \mathbf{w} 线性无关，且

$$\sum_{j=1}^n p_{ij} x_j = \sum_{j=1}^n p_{ij} \left(-\frac{W}{V}v_j + w_j \right) = -\frac{W}{V}p_{ij}v_j + \sum_{j=i}^n p_{ij}w_j = -\frac{W}{V}v_i + w_i = x_i$$

可知 $\mathbf{x} = (x_1, \dots, x_n)$ 为 \mathbf{P} 的属于特征值 1 的特征向量

又有

$$\sum_{i=1}^n x_i = \sum_{i=1}^n \left(-\frac{W}{V} v_i + w_i\right) = -\frac{W}{V} \sum_{i=1}^n v_i + \sum_{i=1}^n w_i = -\frac{W}{V} V + W = 0$$

即 \mathbf{x} 的分量之和为零。

从而与上面的结论矛盾。

□

Perron—Frobenius 定理

Perron 定理

若矩阵 \mathbf{A} 是完全正矩阵，则

- (1) \mathbf{A} 的模最大特征值唯一，且为正实数
- (2) 该特征值代数重数为 1
- (3) 存在该特征值的一个特征向量，其分量全为正

Perron—Frobenius 定理

若矩阵 \mathbf{A} 是非负不可约 (irreducible) 矩阵，则

- (1) \mathbf{A} 的模最大特征值为正实数
- (2) 该特征值代数重数为 1
- (3) 存在该特征值的一个特征向量，其分量全为正

• 不可约矩阵

- 若干个初等对换矩阵的乘积称为置换矩阵 (permutation matrix)
 - 置换矩阵每行和每列都恰有一个元素为 1，其余元素都为 0
- 若存在置换矩阵 \mathbf{Q} ，使得 $\mathbf{Q}^T \mathbf{A} \mathbf{Q} = \begin{pmatrix} \mathbf{X} & \mathbf{0} \\ \mathbf{Y} & \mathbf{Z} \end{pmatrix}$ ，其中 \mathbf{X} 和 \mathbf{Z} 均为方阵，则称 \mathbf{A} 为可约矩阵 (reducible matrix)，否则 \mathbf{A} 为不可约矩阵

• 不可约矩阵与有向图

- 若对有向图中任意顶点对 v_i, v_j ，既存在一条从 v_i 到 v_j 的有向路，也存在一条从 v_j 到 v_i 的有向路，则称有向图是强联通 (strongly connected) 的
- 给定非负矩阵 $\mathbf{A} = (a_{ij})_{n \times n}$ ，构造有向图 $G(\mathbf{A}) = (V, A)$ ，其中 $V = \{v_1, v_2, \dots, v_n\}$ ，弧 $(v_i, v_j) \in A$ 当且仅当 $a_{ij} > 0$
- \mathbf{A} 是不可约矩阵当且仅当 $G(\mathbf{A})$ 是强联通的

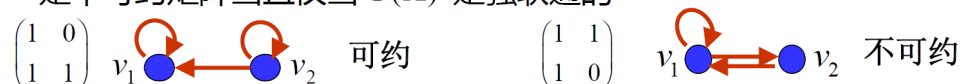


图 2.3: 不可约矩阵简单介绍

链接矩阵与重要度向量

链接矩阵为完全正、列随机矩阵，模最大特征值为 1，重要度向量唯一且分量全为正。

2.4 矩阵计算

2.4.1 幂法迭代

幂法是计算矩阵模最大特征值和对应的特征向量的一种迭代算法

任取初始向量 $\mathbf{x}^{(0)} > 0$ ，且 $\sum_{i=1}^n x_i^{(0)} = 1$ ，

迭代计算 $\mathbf{x}^{(k)} = \bar{\bar{\mathbf{P}}} \mathbf{x}^{(k-1)}$ ，直到 $\mathbf{x}^{(k)}$ 收敛

迭代后的向量仍然向量之和为 1:

$$\mathbf{1}^T \mathbf{x}^{(k)} = \mathbf{1}^T \bar{\bar{\mathbf{P}}} \mathbf{x}^{(k-1)} = \mathbf{1}^T \mathbf{x}^{(k-1)} = 1$$

将 $\bar{\mathbf{P}} = \mathbf{P} + \frac{1}{n} \mathbf{1} \mathbf{d}^T$ ， $\bar{\bar{\mathbf{P}}} = \alpha \bar{\mathbf{P}} + (1 - \alpha) \frac{1}{n} \mathbf{1} \mathbf{1}^T$ 两式带入迭代计算式中

$$\begin{aligned} \mathbf{x}^{(k)} &= \bar{\bar{\mathbf{P}}} \mathbf{x}^{(k-1)} \\ &= \alpha \bar{\mathbf{P}} \mathbf{x}^{(k-1)} + (1 - \alpha) \frac{1}{n} \mathbf{1} \mathbf{1}^T \mathbf{x}^{(k-1)} \\ &= \alpha \bar{\mathbf{P}} \mathbf{x}^{(k-1)} + (1 - \alpha) \frac{1}{n} \mathbf{1} \\ &= \alpha \left(\mathbf{P} + \frac{1}{n} \mathbf{1} \mathbf{d}^T \right) \mathbf{x}^{(k-1)} + (1 - \alpha) \frac{1}{n} \mathbf{1} \\ &= \alpha \mathbf{P} \mathbf{x}^{(k-1)} + \alpha \frac{1}{n} \mathbf{1} \mathbf{d}^T \mathbf{x}^{(k-1)} + (1 - \alpha) \frac{1}{n} \mathbf{1} \end{aligned}$$

2.4.2 完全正、列随机矩阵的幂法收敛性

证明. 记 \mathbf{V} 为满足 $\mathbf{1}^T \mathbf{v} = 0$ 的 n 维列向量 $\mathbf{v} = \{v_1, v_2, \dots, v_n\}$ 全体组成的集合。记

$$\|\mathbf{v}\|_1 = \sum_{i=1}^n |v_i| \text{ (范数)}$$

对任意的 $\mathbf{v} \in \mathbf{V}$ ，取 $\mathbf{w} = \mathbf{P} \mathbf{v}$ ，下证： $\|\mathbf{w}\|_1 \leq c \|\mathbf{v}\|_1$ ，其中 $c < 1$

若 $\mathbf{w} = 0$ ，显然成立。

若 $\mathbf{w} \neq 0$ ，记 $\mathbf{w} = (w_1, w_2, \dots, w_n)^T$ ， $e_i = \text{sgn}(w_i)$ ，则 $c = \max_j |\sum_{i=1}^n p_{ij} e_i| < |\sum_{i=1}^n p_{ij} e_i| < 1$

$$\begin{aligned} \|\mathbf{w}\|_1 &= \sum_{i=1}^n |\mathbf{w}_i| = \sum_{i=1}^n e_i w_i = \sum_{i=1}^n e_i \left(\sum_{j=1}^n p_{ij} v_j \right) = \sum_{j=1}^n v_j \left(\sum_{i=1}^n p_{ij} e_i \right) \\ &\leq \sum_{j=1}^n |v_j| \left| \sum_{i=1}^n p_{ij} e_i \right| \leq c \sum_{j=1}^n |v_j| = c \|\mathbf{v}\|_1 \end{aligned}$$

□

2.5 随机浏览

定义 2.5.1 (随机浏览). 按以下模式浏览互联网的网页

1. 有时从当前网页的链接中随机打开一个网页
2. 有时键入网址新建一个网页
3. 从任一网页开始, 充分长时间后, 访问各网页的概率即为网页重要度

经过统计, 随机打开网页的次数与键入网址新建网页的次数之比约为 5 : 1, 也即 $\alpha = 0.85$ 。

定义 2.5.2 (随机概率). 记事件 $\{X_m = j\}$ 为时刻 m 访问网页 v_j , 则 $P\{X_m = i | X_{m-1} = j\} = p_{ij}$

若 $P\{X_m = j\} = x_j$, 则 $P\{X_m = i\} = \sum_{j=1}^n P\{X_m = i | X_{m-1} = j\} P\{X_{m-1} = j\} = \sum_{j=1}^n p_{ij} x_j$

记 $\mathbf{x}^{(m)} = (P\{X_m = 1\}, P\{X_m = 2\}, \dots, P\{X_m = n\})^T$, 则有 $\mathbf{x}^{(m)} = \bar{\mathbf{P}} \mathbf{x}^{(m-1)}$

定义 2.5.3 (随机过程). 随机过程是描述随机现象随时间推移而演化的一类数学模型。

在一族随机变量 $\{X(t), t \in T\}$ 中 T 为参数集, t 是参数。 $\{X(t), t \in T\}$ 称为参数为 t 的随机变量。 T 为整数集的随机过程称为随机序列。

定义 2.5.4 (Markov 过程). 在已知目前的状态的条件下, 它未来的演变不依赖于它以往的演变。

在随机序列 $\{X(n), n = 0, 1, 2, \dots\}$ 中 (X_n 有限或可列), 对任意的 $n \geq 0$, 有

$$P\{X_{n+1} = j | X_n = i, X_{n-1} = i_{n-1}, \dots, X_0 = i_0\} = P\{X_{n+1} = j | X_n = i\}$$

第三章 数论与组合模型

3.1 Nim Game

现有 n 堆硬币，每堆数量一定。两人轮流取硬币，每次只能从其中一堆中取，且每次取至少一枚。取到最后一枚硬币的一方获胜。

3.1.1 位值制计数法

选定进位制的基底 b ，给定 $0, 1, 2, \dots, b-1$ 共 b 个数码。任何一个自然数 N ，均可用某个以这些数码为系数的 b 的多项式表示出来。

$$N = a_k \cdot b^k + a_{k-1} \cdot b^{k-1} + \dots + a_1 \cdot b + a_0 \\ \Rightarrow (a_k a_{k-1} \dots a_1 a_0)_b, a_0, a_1, \dots, a_k \in \{0, 1, \dots, b-1\}$$

命题 3.1.1. (1) 任意数的 b 进制表示是唯一的

证明. 可以取模证明。 □

(2) 任意两个数的 b 进制表示不同

证明. 根据 (1) 的 b 进制表示是唯一的用反证法证明。 □

3.1.2 Nim Game 的必胜策略

Safe Combination 安全状态

(1) 安全状态：若无论对方如何取均不会获胜，或者无论对方如何取，己方下一次取后均可变为一个安全状态的，称为安全状态。

(2) 不安全状态若对方至少存在一种获胜的取法，己方下一次取无法变为一个安全状态的，称为不安全状态。

必胜策略：己方取法使得下一状态为安全状态。

二进制位和与安全状态

二进制与位和：将每堆硬币数表示为二进制。将所有二进制数的每一位数字分别求和，其尾数称为位和。

Write the number of the counters in each pile in the binary scale of notation, and place these numbers in three horizontal lines so that the units are in the same vertical column. If then the sum of each column is 2 or 0 (i.e. congruent to 0, mod.2), the set of numbers forms a safe combination.

定理 3.1.2 (Basic Property). *If a, b, c form a safe combination any two of the numbers determine the remaining one, that is, the system is closed. So it is for n piles situation.*

推论 3.1.3. (1) 只有一堆硬币时，位和不可能全为 0

(2) 每次从某一堆中取若干枚硬币，该堆硬币的二进制数发生变化，且至少有一位位和发生变化。

位和和安全状态：若所有位和均为 0，则当前状态为安全的，否则为不安全

(1) 若当前状态安全，对任意取法，状态变为不安全

只能从一堆中取，由于当其他 $n-1$ 堆在给定时，能让这 $n-1$ 堆直和第 n 堆变为安全状态的第 n 堆是唯一确定的，就是当前安全状态下要取走的这堆的数目，所以取走该堆的任意个硬币后，都不能达到安全状态。

(2) 若当前状态不安全，存在一种取法，状态变为安全

按自左至右的顺序确定第一个数字之和不为 0 的位，寻找该位数字为 1 的堆，从该堆中取走若干枚使得状态变为安全

Nim Game 必胜情况与先后手的关系

(1) 若初始状态不安全，先手必胜。若初始状态安全，后手必胜

(2) 必胜一方选择适当的取法，使取后状态对己方是安全的

因此先手必胜的概率可以从 Nim Game 随机开局时是否为不安全状态算出，即

$$P_{\text{先手必胜}} = P_{\text{开局为不安全状态}} = \frac{\text{不安全状态个数}}{\text{所有开局可能个数}} \quad (\text{古典概型})$$

3.2 伪币称重问题

伪币辨识 12 枚外观相同的硬币中有一枚是伪币，伪币质量与真币不同（偏轻或者偏重不知），能否用天平称量三次找出伪币，并说明伪币相对真币偏轻或偏重。其中天平一次称量只能比较两端质量大小，不能读出质量数值

3.2.1 自适应方案

硬币真伪的可能性共有 $12 \times 2 = 24$ 种。每一种称量结果对应一种可能性，不同称量结果对应的可能性各不相同

自适应与非自适应

定义 3.2.1. 后一次称量依赖于之前称量结果的方案为自适应 (*adaptive*) 的，否则称为非自适应 (*non-adaptive*) 的。

Type Konwn 伪币称重的自适应方案

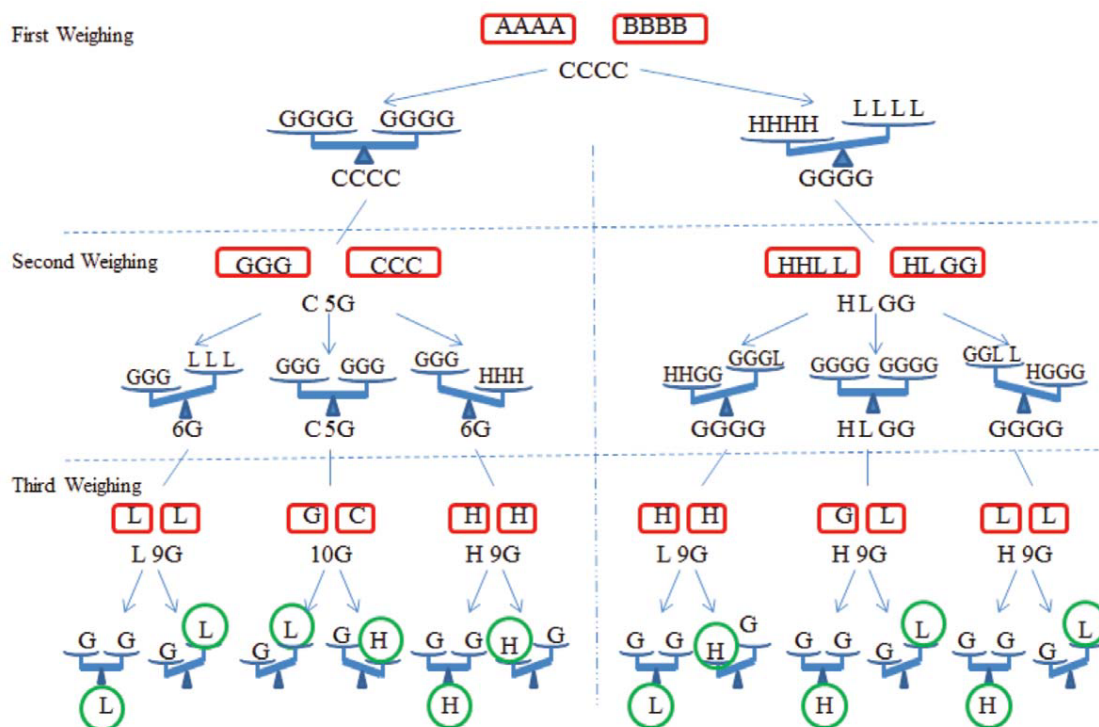


图 3.1: A sequential weighing design for $c = 12$ coins in $w = 3$ weighings with type known

自适应方案的核心在于：在每一次称重后，我们都需要把解答的空间缩小到原来的 $1/3$ 。

3.2.2 非自适应方案

Type Known 自适应最优方案

若 $3 \leq n \leq \frac{3^w-3}{2}$ ，则存在一种非自适应的称量方案，使用 w 次称量可从 n 枚硬币中辨别伪币并确定轻重。

若 $n > \frac{3^w-3}{2}$ ，则不存在自适应的称量方案，用 w 次称量即可从 n 枚硬币中辨别伪币并确定轻重。

第四章 随机模型

4.1 疾病检测

疾病检测性能指标 记 A 为患病, B 为检测结果为阳性, 疾病的发病率为 r

- (1) 灵敏度 (sensitivity) : $p = P(B|A)$: 患病者被检测为阳性 (positive) 的概率
- (2) 特异度 (specificity) : $p = P(\bar{B}|\bar{A})$: 未患病者被检测为阴性 (negative) 的概率
- (3) 被检测出阳性的情况下患病的概率为

$$P(A|B) = \frac{P(B|A)P(A)}{P(B|A)P(A) + P(B|\bar{A})P(\bar{A})} = \frac{pr}{pr + (1-q)(1-r)}$$

4.1.1 概率群试 (group testing)

概率群式: 假定 n 个人相互独立地以概率 p 患病, 如何找出全部的病人, 使平均检测次数尽可能少?

如何选择群式方案? 要考虑平均检测次数、检测阶段数、每人最大检测次数、每组最多样本数、方案的可操作性、检测的灵敏度与特异度等多个因素。

两阶段群试

将 n 人的样本混合后检测。若结果为阴性, 说明这 n 人均未感染。若结果为阳性, 说明这 n 人中至少有一人已感染。此时逐个检测每个人样本。

下求两阶段群试的平均检测次数的数学期望:

- (1) 混合样本阴性概率为 $(1-p)^n$, 总检测次数为 1;
- (2) 混合样本阳性概率为 $1 - (1-p)^n$, 总检测次数为 $n+1$ 。
- (3) 检测次数的数学期望为 $1 \cdot (1-p)^n + (n+1) \cdot (1 - (1-p)^n)$;
- (4) 平均检测次数的数学期望为 $\frac{1 \cdot (1-p)^n + (n+1) \cdot (1 - (1-p)^n)}{n}$

4.2 The Monty Hall Problem