

计数, 容斥原理

请在 11 月 13 日课前提交纸质作业.

1. (5 分) 定义 $R_n = \sum_{k \geq 0} \binom{n+k}{k} 2^{-k}$. 化简 R_n 的表达式.
2. (5 分) 定义 $R_n = \sum_{k \leq n} \binom{n-k}{k} (-1)^k$. 化简 R_n 的表达式.
3. (10 分) 每一个置换 $g \in \text{Sym}(n)$ 都可以写成若干不交的轮换.
 - (1) 对任意 $k > n/2$, 问有多少个置换包含一个长度恰好为 k 的轮换.
 - (2) 对任意 $\alpha > 1/2$, 对一个随机的置换 $g \in \text{Sym}(n)$ 包含一个长度至少为 αn 的轮换的概率大概是多少. 这里假设 n 充分大.
4. (10 分) 给定一个函数 $f : 2^{[n]} \rightarrow \mathbb{R}$. 证明如果定义 $\tilde{f}(S) = \sum_{T \supseteq S} f(T)$, 那么

$$f(S) = \sum_{T \supsetneq S} (-1)^{|T \setminus S|} \tilde{f}(T).$$

Remark: 对于一组有限集 A_1, \dots, A_n 和 $\Omega = A_1 \cup A_2 \cup \dots \cup A_n$. 如果定义

$$f(S) = |\{x \in \Omega \mid \forall i \in [n], x \in A_i \iff i \in S\}|,$$

那么题目结论可以推出容斥原理.

Remark: 对称地, 如果定义 $\hat{f}(S) = \sum_{T \subseteq S} f(T)$, 那么

$$f(S) = \sum_{T \subseteq S} (-1)^{|S \setminus T|} \hat{f}(T).$$

5. (10 分) 令 $M \in \text{Mat}_{n,n}(\mathbb{F})$ 是一个有限域 \mathbb{F} 上的 $n \times n$ 矩阵. 定义 M 是一个 MDS (maximum distance separable) 矩阵, 当且仅当对任何不同的 $x, x' \in \mathbb{F}^n$, (Mx, x) 和 (Mx', x') 至少在 $n+1$ 个位置不同. 不难证明以下命题等价,

- a. M 是 MDS 矩阵;
- b. M 可逆, 且 M^{-1} 是 MDS 矩阵;
- c. M 的任何子矩阵满秩;
- d. 对任何非零 $x \in \mathbb{F}^n$, (Mx, x) 至少在 $n+1$ 个位置非零.

- e. 考虑方程 $(y_1, \dots, y_n) = M(x_1, \dots, x_n)$, 任意固定 $x_1, \dots, x_n, y_1, \dots, y_n$ 中的 n 个变量, 方程仍有解;
- f. 考虑方程 $(y_1, \dots, y_n) = M(x_1, \dots, x_n)$, 任意固定 $x_1, \dots, x_n, y_1, \dots, y_n$ 中的 n 个变量, 方程有唯一解.

由等价命题 c 可以看出, 当 $|\mathbb{F}|$ 足够大时, 大部分矩阵都是 MDS 矩阵. 因此, 可以说 MDS 刻画了“一般的”矩阵.

- (1) 若 $M \in \text{Mat}_{n,n}(\mathbb{F})$ 是一个 MDS 矩阵, 求出满足 $(x_{n+1}, \dots, x_{2n}) = M(x_1, \dots, x_n)$ 且 x_1, \dots, x_{2n} 均不为 0 的解的个数.

提示: 对每个集合 $S \subseteq [2n]$, 计算满足 $(x_{n+1}, \dots, x_{2n}) = M(x_1, \dots, x_n)$ 且 $x_i = 0 \iff i \in S$ 的解的个数.

- (2) 记上问求出的解的个数为 L . 证明

$$\left| L - \frac{(|\mathbb{F}| - 1)^{2n}}{|\mathbb{F}|^n} \right| \leq 2^{2n}.$$

6. (10 分) 设 $k \geq 1$ 是整数, 找到最小的 d , 使得对任意 n , 都存在一个 \mathbb{F}_2 上的次数不超过 d 的多项式 $f(x_1, \dots, x_n)$

$$\forall x_1, \dots, x_n \in \{0, 1\}, f(x_1, \dots, x_n) = \begin{cases} 1, & \text{if } x_1, \dots, x_n \text{ 中 } 1 \text{ 的个数 } \equiv -1 \pmod{2^k} \\ 0, & \text{otherwise} \end{cases}$$

提示: 先考虑 $n = 2^k - 1$ 的情况.