计数, 容斥原理

参考答案

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.

   解 $R_0 = \sum_{k\geq 0} 2^{-k} = 1$.

$$\begin{aligned} R_n &= \sum_{k\geq 0} \binom{n+k}{k} 2^{-k} \\ &= \sum_{k\geq 0} \binom{n+k-1}{k-1} 2^{-k} + \sum_{k\geq 0} \binom{n+k-1}{k} 2^{-k} \\ &= \sum_{k\geq 0} \binom{n+k}{k} 2^{-k-1} + R_{n-1} \\ &= \frac{1}{2} R_n + R_{n-1}. \end{aligned}$$

   因此 $R_n = 2R_{n-1} = 2^{n+1}$.

   另一种解法: 不停扔均匀硬币, 直到扔出 $n+1$ 个反面才停止. 停止前扔出了 k 个正面的概率是 $\binom{n+k}{k}/2^{n+k+1}$. 因此 $\sum_k \binom{n+k}{k}/2^{n+k+1} = R_n/2^{n+1} = 1$.

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.

   解 $R_0 = R_1 = 1$.

$$\begin{aligned} R_n = \sum_k \binom{n-k}{k} (-1)^k &= \sum_k \binom{n-k-1}{k} (-1)^k + \sum_k \binom{n-k-1}{k-1} (-1)^k \\ &= \sum_k \binom{n-k-1}{k} (-1)^k + \sum_k \binom{n-k-2}{k} (-1)^{k+1} = R_{n-1} - R_{n-2}. \end{aligned}$$

   根据递推公式, 不难验证, 数列是 $1, 1, 0, -1, -1, 0$ 的循环.

$$R_i = \begin{cases} 1, & \text{if } i = 0, 1 \mod 6 \\ 0, & \text{if } i = 2, 5 \mod 6 \\ -1, & \text{if } i = 3, 4 \mod 6 \end{cases}$$

3. (10 分) 每一个置换 $g \in \mathrm{Sym}(n)$ 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 $g \in \mathrm{Sym}(n)$ 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.

注. *(这往往会被包装为以下问题.)* 监狱中有 n 位囚犯. 现在让他们进行如下游戏. 在房间里布置标号 $1,\ldots,n$ 的 n 个柜子, 其中分别写有 n 个囚犯的名字. 每个囚犯分别被带到房间中, 允许打开其中至多 αn 个柜子. 如果所有囚犯都找到了包含自己名字的柜子, 那么所有囚犯都被释放. 否则, 所有囚犯都被处死. 游戏开始后囚犯之间不能交流. 请问囚犯应该采取怎样的策略.

解

(1) 对置换 g 和元素 i, 要求 g 包含一个长度为 k 的轮换且 i 在轮换中. 这样的 (g,i) 对有

$$\underbrace{n}_{i\text{ 的选择}}\cdot\underbrace{(n-1)^{\underline{k-1}}}_{i\text{ 所在的轮换}}\cdot\underbrace{(n-k)!}_{\text{剩下 }n-k\text{ 元素的置换}}=n!\text{ 个.}$$

每个包含 k 轮换的置换对应了 k 个 (g,i) 对, 因此数目为 $n!/k$.

(2) 概率为

$$\sum_{k\in[\alpha n,n]}\frac{n!/k}{n!}=\sum_{k\in[\alpha n,n]}\frac{1}{k}=H_n-H_{\alpha n}\approx\ln(1/\alpha).$$

4. (10 分) 给定一个函数 $f:2^{[n]}\to\mathbb{R}$. 证明如果定义 $\tilde{f}(S)=\sum_{T\supseteq S}f(T)$, 那么

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

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

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

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

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

解

$$\begin{aligned}\sum_{T\supseteq S}(-1)^{|T\setminus S|}\tilde{f}(T)&=\sum_{T\supseteq S}(-1)^{|T\setminus S|}\sum_{U\supseteq T}f(U)\\&=\sum_{U\supseteq S}f(U)\sum_{T\text{ s.t. }U\supseteq T\supseteq S}(-1)^{|T\setminus S|}\\&=\sum_{U\supseteq S}f(U)\sum_{T\subseteq U\setminus S}(-1)^{|T|}\\&=\sum_{U\supseteq S}f(U)\begin{cases}1,&\text{if }U=S,\\0,&\text{if }U\supsetneq S.\end{cases}\\&=f(S).\end{aligned}$$

5. (10 分) 令 $M \in \mathrm{Mat}_{n,n}(\mathbb{F})$ 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 $(y_1, \ldots, y_n) = M(x_1, \ldots, x_n)$，任意固定 $x_1, \ldots, x_n, y_1, \ldots, y_n$ 中的 n 个变量，方程仍有解；

   f. 考虑方程 $(y_1, \ldots, y_n) = M(x_1, \ldots, x_n)$，任意固定 $x_1, \ldots, x_n, y_1, \ldots, y_n$ 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 $M \in \mathrm{Mat}_{n,n}(\mathbb{F})$ 是一个 MDS 矩阵，求出满足 $(x_{n+1}, \ldots, x_{2n}) = M(x_1, \ldots, x_n)$ 且 $x_1, \ldots, x_{2n}$ 均不为 0 的解的个数.

   提示：对每个集合 $S \subseteq [2n]$，计算满足 $(x_{n+1}, \ldots, x_{2n}) = M(x_1, \ldots, x_n)$ 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

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

解

(1) 对每个集合 $S \subseteq [2n]$，定义 $f(S)$ 为计算满足 $(x_{n+1}, \ldots, x_{2n}) = M(x_1, \ldots, x_n)$ 且 $x_i = 0 \iff i \in S$ 的解的个数. 定义 $\tilde{f}(S) = \sum_{T \supseteq S} f(T)$，那么 $\tilde{f}(S)$ 就是满足 $(x_{n+1}, \ldots, x_{2n}) = M(x_1, \ldots, x_n)$ 且 $i \in S \implies x_i = 0$ 的解的个数. 注意到，$\tilde{f}(S)$ 就是线性空间

$$V_S := \left\{ (x_1, \ldots, x_{2n}) \;\middle|\; (x_{n+1}, \ldots, x_{2n}) = M(x_1, \ldots, x_n), \forall i \in S, x_i = 0 \right\}$$

的大小. 计算线性空间的大小，只需计算其维度即可. $V_\varnothing$ 的维度是 n. S 中的每增加一个元素，代表增加了一个线性条件，维度最多减少 1. 也就是说

$$\dim V_S \geq \dim V_{S \cup \{i\}} \geq \dim V_S - 1.$$

另一方面，根据 M 是 MDS 的性质 e，我们知道，当 $|S| \geq n$ 时，V_S 的维度等于 0. 综合 $V_\varnothing$ 和 $V_S, |S| \geq 0$ 的情况，我们有

$$\dim V_S = \begin{cases} n - |S| & \text{if } |S| < n \\ 0 & \text{if } |S| \geq n \end{cases} \qquad \tilde{f}(S) = \begin{cases} |\mathbb{F}|^{n-|S|} & \text{if } |S| < n \\ 1 & \text{if } |S| \geq n \end{cases} = |\mathbb{F}|^{\max(n-|S|,0)}.$$

第一问要求的就是 $f(\varnothing)$ 的值. 根据第 4 题的结论,

$$f(\varnothing)=\sum_S(-1)^S\tilde{f}(S)=\sum_S(-1)^S|\mathbb{F}|^{\max(n-|S|,0)}=\sum_{i=0}^{2n}(-1)^i|\mathbb{F}|^{\max(n-i,0)}\binom{2n}{i}.$$

(2) 定义函数 $\tilde{g}$

$$\tilde{g}(S):=|\mathbb{F}|^{n-|S|}.$$

这里 $\tilde{g}$ 的定义使得 $|\tilde{g}(S)-\tilde{f}(S)|\le 1$ 对任何 S 都成立; 而 g 由 $g(S)=\sum_{T\supseteq S}(-1)^{|T\setminus S|}\tilde{g}(T)$ 自然地诱导出:

$$g(S):=(|\mathbb{F}|-1)^{2n-|S|}/|\mathbb{F}|^n,$$

这样

$$|f(S)-g(S)|=\left|\sum_{T\supseteq S}(-1)^{|T\setminus S|}(\tilde{f}-\tilde{g})(T)\right|\le\sum_{T\supseteq S}\left|(-1)^{|T\setminus S|}(\tilde{f}-\tilde{g})(T)\right|=\sum_{T\supseteq S}1=2^{2n-|S|}.$$

特别地, 当选取 $S=\varnothing$ 时,

$$\left|L-\frac{(|\mathbb{F}|-1)^{2n}}{|\mathbb{F}|^n}\right|=|f(\varnothing)-g(\varnothing)|\le 2^{2n}.$$

6. (10 分) 设 $k\ge 1$ 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 $f(x_1,\dots,x_n)$

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

提示: 先考虑 $n=2^k-1$ 的情况.

解 $d=2^k-1$.

因为输入只有 0 或 1, 对任意 $k>1$ 都有 $x_i^k=x_i$. 所以不妨令 f 对于每位输入的次数都不超过 1.

先考虑 $n=2^k-1$ 的情况. 这时唯一满足要求的多项式是 $f=x_1x_2\dots x_n$.

对一般的情况, 可以知道 f 中没有次数小于 2^k-1 的项, 同时含有所有次数为 2^k-1 的项. 尝试

$$f(x_1,\dots,x_n)=\sum_{\text{size-}(2^k-1)\ S\subseteq[n]}\prod_{i\in S}x_i.$$

当输入中有 m 个 1 时,

$$f(x_1,\dots,x_n)=\binom{m}{2^k-1}\bmod 2=\frac{(m-2^k+2)\cdots(m-1)m}{1\cdot 2\cdot\cdots\cdot(2^k-1)}\bmod 2.$$

我们关心分子分母中 2 的次数.

- 如果 $m=2^kq+2^k-1$, 那么可以将分子分母中的项一一对应, i 与 2^kq+i 对应. 对应的两项中 2 的次数相同, 因此上下次数相同.

- 如果 $m = 2^k q + r$ 且 $r \in \{0, \ldots, 2^k - 2\}$, 那么仍然可以分子分母中的项按照 $\bmod 2^k$ 的值一一对应. 只有分子中的 $2^k q$ 和分母中的 $r+1$ 没有对应. 这里 $2^k q$ 中 2 的次数比 $r+1$ 中 2 的次数多.