期末试题

试卷共 3 页, 共 13 题, 满分 30 分.

判断/选择题：无需写出证明.

1. (1 分) 对任意 $n \in \mathbb{N}$, $\binom{2n}{n}$ 都是偶数.
2. (1 分) 两个 (不独立的) 随机变量 X, Y 满足 $0 \le X \le Y$ 恒成立. 那么 $\mathrm{Var}[X] \le \mathrm{Var}[Y]$.
3. (1 分) 如果一个平面图是简单图, 那么它的对偶 (dual graph) 也是简单图.
4. (1 分) 对任意 $\delta > 0$, 存在 $\varepsilon > 0$, 使得对于任何有限空间中的分布 P, Q,

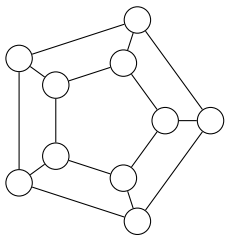
$$\Delta_{\mathrm{TV}}(P, Q) \le \varepsilon \implies D_{\mathrm{KL}}(P \| Q) \le \delta.$$

填空题：无需写出证明.

5. (2 分) $S_n = \{\mathbf{v} \in \{0,1,2\}^n \mid \sum v_i = n\}$. 估算 $|S_n|$, 要求误差不超过 $n^{O(1)}$.
6. (2 分) 有 n 张互异的扑克牌, 摞成一堆. 用以下方式洗牌: 每次随机抽取一张扑克牌, 再放回牌堆顶部. 请估算洗牌时间.

   具体来说, 这个过程可以视为一个马尔可夫链, 其稳态分布是均匀分布 (洗匀的牌堆). 请估计混合时间 $t_{\mathrm{mix}}(1/100)$. 允许有常数误差.
7. (2 分) 考虑一个 10 个珠子构成的双层项链, 用两种颜色对珠子染色, 有多少种不同的染色方案.

   只要存在图同构都视为相同染色. 包括旋转、内外层交换、镜像.



解答题：请选择 4 道作答.

8. (5 分) 用 C 种颜色对满二叉树中的点进行染色. 两个染色方案等价, 当且仅当其中一种方案可以经过一系列左右子树的交换转化为另一种方案.

   (1) 高度为 2 的满二叉树 (共有 3 个点) 有多少种不同的染色方案?

   (2) 高度为 3 的满二叉树 (共有 7 个点) 有多少种不同的染色方案?

   (3) 高度为 4 的满二叉树 (共有 15 个点) 有多少种不同的染色方案?

   不强制要求把结果完全展开, 但请表述为清晰便于验证的形式.
9. (5 分) 每个置换 $f \in \mathrm{Sym}(n)$ 都可以拆成若干不交的轮换 (cycle). 不动点就是一个长度为 1 的轮换.

   (1) 求 $\mathrm{Sym}(2n)$ 中只包含偶数长度轮换的置换个数 a_{2n}, 并证明.

(2) 求 $\mathrm{Sym}(2n)$ 中只包含奇数长度轮换的置换个数 b_{2n}, 并证明.

举例来说, $(1)(2)(34) \in \mathrm{Sym}(4)$ 包含了奇长度轮换 (1), 所以不在第一问的计数范围; 同时包含了偶长度轮换 (34), 所以也不在第二问的计数范围.

10. (5 分) 有 n 对情侣, 随机将他们分为 n 组, 每组两人. 有多少对情侣被分到同组中?

    (1) 当 n 充分大时, 所有情侣都没有分入同组的概率是多少. 证明你的结果.

    (2) 用 $P_{n,k}$ 表示其中恰好有 k 对情侣分到同组的概率. 对于任意常数 k, 请计算 $\lim_{n\to\infty} P_{n,k}$ 并证明你的结果.

11. (5 分) 这里我们设计一种高效纠错码.

    (1) 考虑压缩函数 $f : \{0,1\}^n \to \{0,1\}^m$ 和解压缩函数 $g : \{0,1\}^m \to \{0,1\}^n$. 固定一个常数概率 $p < 1/2$, 求出

$$\alpha^* = \inf\left\{ \alpha \middle| \begin{array}{c} \exists f : \{0,1\}^n \to \{0,1\}^{\alpha n}, g : \{0,1\}^{\alpha n} \to \{0,1\}^n \\ \Pr_{\mathbf{x}\sim \mathrm{Bern}(p)^n}[g(f(\mathbf{x})) = \mathbf{x}] = 1 - 2^{\Theta(n)} \end{array} \right\}$$

    不需写出证明和计算过程.

    (2) 如果额外限制 f 为 $\mathbb{F}_2$ 上的线性函数, 那么 α^* 将如何变化? 证明你的结论.

    (3) 符合前一问的压缩和解压缩函数可以非常高效 ($O(n \log n)$ 电路大小). 据此设计用于 $\mathrm{BSC}(p)$ 信道的高效编码 $E : \{0,1\}^n \to \{0,1\}^\ell, D : \{0,1\}^\ell \to \{0,1\}^n$. 要求对任意消息 $\mathbf{w} \in \{0,1\}^n$,

$$\Pr_{Y\sim (P_{Y|X})^\ell(\cdot|E(\mathbf{w}))}[D(Y) = \mathbf{w}] \geq 1 - \exp(-\Theta(n)).$$

    在这样的要求下, 码率 n/ℓ 可以达到多少? 请写出 E, D 的构造并证明结论.

    $\mathrm{BSC}(p)$ 的定义: $P_{Y|X}(0|0) = P_{Y|X}(1|1) = 1 - p$, $P_{Y|X}(0|1) = P_{Y|X}(1|0) = p$.

12. (6 分) 给定一个奇素数 p, 我们将 $x \in \mathbb{Z}_p^*$ 分为两类: 如果 $\exists y \in \mathbb{Z}_p^*$, $x = y^2$, 那么称 x 为二次剩余, 否则称 x 为二次非剩余. 不难说明 $\mathbb{Z}_p^*$ 中恰好有一半是二次剩余. 判断一个元素是否为二次剩余可以使用勒让德符号 (Legendre symbol)

$$\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}} = \begin{cases} +1, & \text{if } x \text{ 是二次剩余} \\ -1, & \text{if } x \text{ 是二次非剩余} \\ 0, & \text{if } x = 0 \end{cases}$$

    不难说明, $x \mapsto (\frac{x}{p})$ 是一个 $\mathbb{Z}_p^*$ 到 $\{-1, 1\}$ 的群同态.

    请证明存在常数 C_0, C_1 使得, 对于任何 $n \in \mathbb{N}$, 任何素数 $p > 2^{C_0 n + C_1}$ 和任何 $(b_1, \ldots, b_n) \in \{0,1\}^n$, 存在 $x \in \mathbb{Z}_p$ 满足

$$\left(\frac{x+1}{p}\right) = (-1)^{b_1}, \left(\frac{x+2}{p}\right) = (-1)^{b_2}, \ldots, \left(\frac{x+n}{p}\right) = (-1)^{b_n}.$$

Weil bound 的大意为: $\mathbb{F}_p$ 上的"简单"曲线经过大约 p 个点. 特别地, 证明需要 Weil bound 的以下推论: 如果 $f \in \mathbb{F}_p[x]$ 满足 $\deg f = d > 0$ 且无平方 (square-free, 等价于在任何扩域中无重根), 那么

$$\left|\left\{(x,y) \in \mathbb{Z}_p^2 \;\middle|\; f(x) = y^2\right\}\right| \in (p - d\sqrt{p}, p + d\sqrt{p}).$$

证明也可以使用这个推论的以下等价表述, 等价性只需注意到 $(\frac{x}{p}) = |\{y \mid y^2 = x\}| - 1$,

$$\sum_{x \in \mathbb{Z}_p} \left(\frac{f(x)}{p}\right) \in (-d\sqrt{p}, d\sqrt{p}).$$

提示: 对任意非空子集 $\Theta \subseteq \mathbb{F}_p$, 考虑函数 $x \mapsto \prod_{i \in \Theta}(x - i)$.

13. (5 分) 对于随机图上的单调性质, 课上讨论了阈值 (threshold) 与 sharp threshold.

    (1) 存在 K_4 (4-clique) 是图的一个单调性质, 因此一定存在阈值. 请找出一个阈值并证明.

    (2) 这个性质是否存在 sharp threshold? 请证明你的结论.

    本题中请使用 $G(n,p)$ 模型. 阈值和 sharp threshold 的定义分别为.

    - $p^* : \mathbb{N} \to \mathbb{R}$ 是性质 $\mathcal{P}$ 的阈值, 如果对任意 $p(n) = o(p^*(n))$, $p'(n) = \omega(p^*(n))$

      $$\lim_{n\to\infty} \Pr[G(n,p(n)) \in \mathcal{P}] = 0, \qquad \lim_{n\to\infty} \Pr[G(n,p'(n)) \in \mathcal{P}] = 1.$$

    - $p^* : \mathbb{N} \to \mathbb{R}$ 是性质 $\mathcal{P}$ 的 sharp threshold, 如果对任意 $\varepsilon > 0$

      $$\lim_{n\to\infty} \Pr[G(n,(1-\varepsilon)p^*(n)) \in \mathcal{P}] = 0, \qquad \lim_{n\to\infty} \Pr[G(n,(1+\varepsilon)p^*(n)) \in \mathcal{P}] = 1.$$