# 随机算法

岳镝

2025 年 5 月 30 日

# 随机算法

欢迎大家选修孔雨晴老师的《随机算法》课程（春季学期）

# 概率不等式

## Union Bound

对事件 $A, B$，有 $\Pr[A \cup B] \leq \Pr[A] + \Pr[B]$

# 概率不等式

## Markov's Inequality

对非负随机变量 $X$ 和 $a > 0$，有 $\Pr[X \geq a] \leq \frac{\mathbb{E}[X]}{a}$

# 概率不等式

$$\Pr\left[e^{\lambda|X-\mathbb{E}[X]|} \geq e^{\lambda\varepsilon}\right]$$

## Chebyshev's Inequality

对于随机变量 $X$ 和 $\varepsilon > 0$,

$$\Pr[|X - \mathbb{E}[X]|^2 \geq \varepsilon^2] \leq \frac{\mathrm{Var}[X]}{\varepsilon^2}$$

$$\Pr\left[|X-\mathbb{E}[X]|^4 \geq \varepsilon^4\right]$$

$$\Pr\left[|X-\mathbb{E}[X]|^6 \geq \varepsilon^6\right]$$

# 概率不等式

## Chernoff/Hoeffding Bounds

设 $X_1, X_2, \ldots, X_n$ 是独立的 0-1 随机变量。记 $X = \sum_{i=1}^{n} X_i$，$\mu = \mathbb{E}[X]$。

(1) 对 $\beta \in (0,1)$，有

$$\Pr[X \le (1-\beta)\mu] \le \exp\left(-\frac{\beta^2\mu}{2}\right)$$

(2) 对 $\beta > 0$，有

$$\Pr[X \ge (1+\beta)\mu] \le \begin{cases} \exp\left(-\frac{\beta^2\mu}{2+\beta}\right), & \beta > 0, \\ \exp\left(-\frac{\beta^2\mu}{3}\right), & \beta \in (0,1] \end{cases}$$

(3) 对 $\lambda > 0$，有

$$\left.\begin{matrix} \Pr[X \ge \mu + \lambda] \\ \Pr[X \le \mu - \lambda] \end{matrix}\right\} \le \exp\left(-\frac{2\lambda^2}{n}\right)$$

# 复杂性类

ZPP (zero-error probabilistic polynomial time)

称语言（问题） $L \in \mathrm{ZPP}$，若存在期望运行时间为多项式的随机算法判定 $L$

- 判定算法是拉斯维加斯型
- 例子：排序问题

# 复杂性类

## RP (randomized polynomial time)

称语言（问题） $L \in \mathrm{RP}$，若存在多项式时间的随机算法 $A$，使得对任意实例 $x \in \{0,1\}^*$，

(1) $x \in L \Longrightarrow \Pr[A(x) = \mathrm{acc}] \geq 1/2$

(2) $x \notin L \Longrightarrow A(x) = \mathrm{rej}$

- “弃真”型蒙特卡洛算法
- 例子：合数

## coRP

称语言（问题） $L \in \mathrm{coRP}$，若存在多项式时间的随机算法 $A$，使得对任意实例 $x \in \{0,1\}^*$，

(1) $x \in L \Longrightarrow A(x) = \mathrm{acc}$

(2) $x \notin L \Longrightarrow \Pr[A(x) = \mathrm{rej}] \geq 1/2$

- “取伪”型蒙特卡洛算法
- 例子：素数、串相等

# 复杂性类

## BPP (bounded-error probabilistic polynomial time)

称语言（问题） $L \in \mathrm{BPP}$，若存在多项式时间的随机算法 $A$，使得对任意实例 $x \in \{0,1\}^*$，

(1) $x \in L \Longrightarrow \Pr[A(x) = \mathrm{acc}] \geq 2/3$

(2) $x \notin L \Longrightarrow \Pr[A(x) = \mathrm{rej}] \geq 2/3$

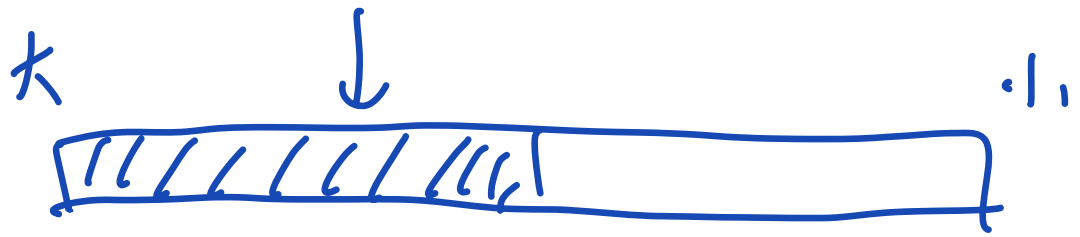
# 复杂性类

$$\mathrm{P} \subseteq \mathrm{ZPP} = \mathrm{RP} \cap \mathrm{coRP} \subseteq \mathrm{RP} \subseteq \mathrm{BPP}$$

# 作业题

给定 $n$ 个数的集合 $X$，找出 $X$ 中一个至少第 $\lfloor n/2 \rfloor$ 大的数。要求错误概率不超过 $1/n$

确定型：$\lceil \frac{n}{2} \rceil$




任取 $\lceil \frac{n}{2} \rceil + 1$ 个 S

$\max(S)$

Complexity $= |S| - 1 = \lceil \frac{n}{2} \rceil$

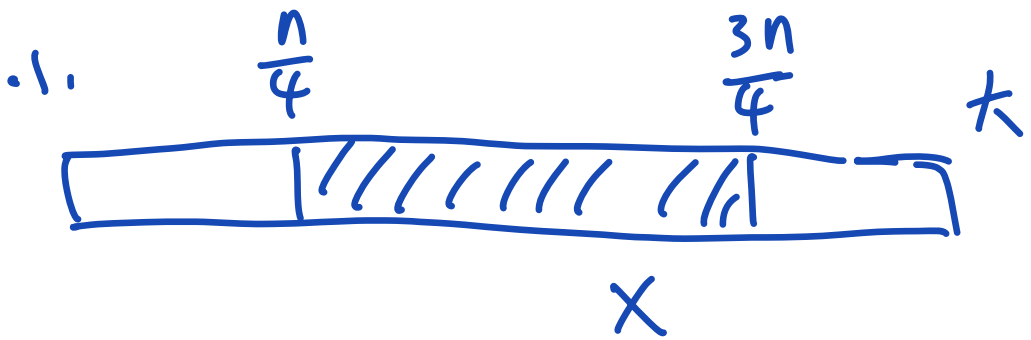
# 作业题

给定 $n$ 个数的集合 $X$，找出 $X$ 中一个至少第 $n/2$ 大的数。要求错误概率不超过 $1/n$

- 随机取 $x \sim X$，则 $x$ 是至少第 $n/2$ 大的概率为 $1/2$
- 独立重复 $t = O(\log n)$ 次，$S = \{x_1, x_2, \ldots, x_t\}$
- 令 $x^* = \max(S)$

# 作业题

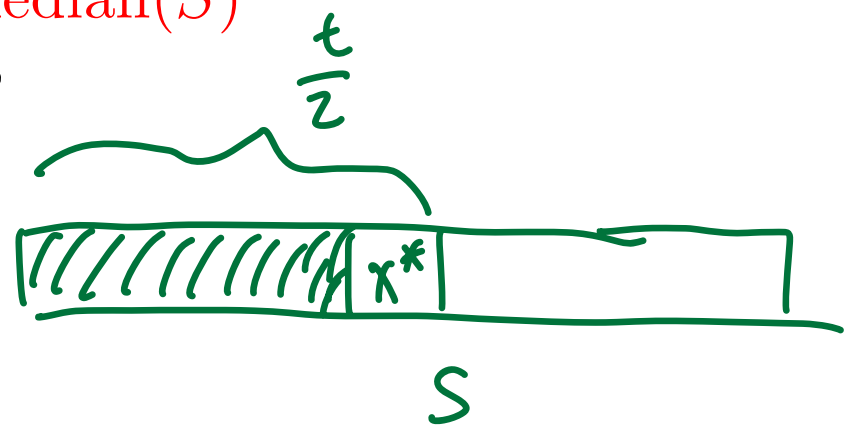
给定 $n$ 个数的集合 $X$，找出 $X$ 中一个排名在 $[n/4, 3n/4]$ 之间的数。要求错误概率不超过 $1/n$



# 作业题

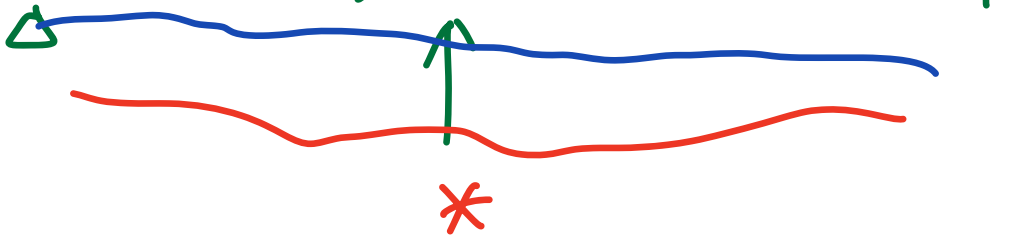
给定 $n$ 个数的集合 $X$，找出 $X$ 中一个排名在 $[n/4, 3n/4]$ 之间的数。要求错误概率不超过 $1/n$

- 随机取 $x \sim X$，则 $x$ 排名在 $[n/4, 3n/4]$ 之间的概率为 $1/2$
- 独立重复 $t = O(\log n)$ 次，$S = \{x_1, x_2, \ldots, x_t\}$
- 令 $x^* = \text{median}(S)$
- 错误概率？




(1) $x^*$ 排名 $< \frac{n}{4}$ $\Rightarrow$ S 中有至少 $\frac{t}{2}$ 个数排名 $< \frac{n}{4}$

$\Pr[\downarrow] \le \frac{1}{\text{poly}(n)}$



$$I_i = \begin{cases} 1, & \text{若 } x_i \text{ 的排名} < \frac{n}{4} \\ 0, & \text{o.w.} \end{cases}$$

$1 \le i \le t$

$$\Pr[I_i = 1] \le \frac{1}{4}$$

$$I = \sum_{i=1}^{t} I_i \qquad \mathbb{E}[I] \le \frac{t}{4}$$

---

$$\Pr[*] = \Pr\left[I \ge \frac{t}{2}\right] \le \Pr\left[I \ge \mathbb{E}[I] + \frac{t}{4}\right]$$

Chernoff Bound

$$\le \exp\left(-\frac{2\cdot\left(\frac{t}{4}\right)^2}{t}\right) = \exp\left(-\frac{t}{8}\right) \le \frac{1}{\text{poly}(n)}$$

# Amplification

已知弃真型算法 $A$

(1) $x \in L \Longrightarrow \Pr[A(x) = \text{acc}] \geq 1/2$

(2) $x \notin L \Longrightarrow A(x) = \text{rej}$

构造弃真型算法 $A'$

(1) $x \in L \Longrightarrow \Pr[A'(x) = \text{acc}] \geq 1 - 1/\text{poly}(n)$

(2) $x \notin L \Longrightarrow A'(x) = \text{rej}$

# Amplification

已知弃真型算法 $A$

(1) $x \in L \Longrightarrow \Pr[A(x) = \text{acc}] \geq 1/2$

(2) $x \notin L \Longrightarrow A(x) = \text{rej}$

构造弃真型算法 $A'$

(1) $x \in L \Longrightarrow \Pr[A'(x) = \text{acc}] \geq 1 - 1/\text{poly}(n)$

(2) $x \notin L \Longrightarrow A'(x) = \text{rej}$

算法 $A'$:

1. 独立重复运行 $t = O(\log n)$ 次算法 $A$
2. 若某次结果为 acc, 则返回 acc
3. 若每次结果均为 rej, 则返回 rej

# Amplification

已知双侧错误算法 $A$

(1) $x \in L \Longrightarrow \Pr[A(x) = \text{acc}] \geq 2/3$

(2) $x \notin L \Longrightarrow \Pr[A(x) = \text{rej}] \geq 2/3$

构造双侧错误算法 $A'$

(1) $x \in L \Longrightarrow \Pr[A'(x) = \text{acc}] \geq 1 - 1/\text{poly}(n)$

(2) $x \notin L \Longrightarrow \Pr[A'(x) = \text{rej}] \geq 1 - 1/\text{poly}(n)$

# Amplification

已知双侧错误算法 $A$

(1) $x \in L \Longrightarrow \Pr[A(x) = \text{acc}] \geq 2/3$

(2) $x \notin L \Longrightarrow \Pr[A(x) = \text{rej}] \geq 2/3$

构造双侧错误算法 $A'$

(1) $x \in L \Longrightarrow \Pr[A'(x) = \text{acc}] \geq 1 - 1/\text{poly}(n)$

(2) $x \notin L \Longrightarrow \Pr[A'(x) = \text{rej}] \geq 1 - 1/\text{poly}(n)$

算法 $A'$:

1. 独立重复运行 $t = O(\log n)$ 次算法 $A$
2. 统计 acc 的次数 $\alpha$ 和 rej 的次数 $\beta$ $(\alpha + \beta = t)$
3. 若 $\alpha \geq \beta$, 则返回 acc
4. 若 $\alpha < \beta$, 则返回 rej

# 例题

**证明：** $\mathrm{ZPP} = \mathrm{RP} \cap \mathrm{coRP}$

# 例题

## 证明：$\mathrm{ZPP} = \mathrm{RP} \cap \mathrm{coRP}$

称语言（问题） $L \in \mathrm{ZPP}$，若存在期望运行时间为多项式的随机算法判定 $L$

称语言（问题） $L \in \mathrm{RP}$，若存在多项式时间的随机算法 $A$，使得对任意实例 $x \in \{0,1\}^*$，

(1) $x \in L \Longrightarrow \Pr[A(x) = \mathrm{acc}] \geq 1/2$

(2) $x \notin L \Longrightarrow A(x) = \mathrm{rej}$

称语言（问题） $L \in \mathrm{coRP}$，若存在多项式时间的随机算法 $A$，使得对任意实例 $x \in \{0,1\}^*$，

(1) $x \in L \Longrightarrow A(x) = \mathrm{acc}$

(2) $x \notin L \Longrightarrow \Pr[A(x) = \mathrm{rej}] \geq 1/2$

# 例题

(1) $\mathrm{ZPP} \subseteq \mathrm{RP} \cap \mathrm{coRP}$

- 目标：给定问题 $L$ 的期望多项式时间判定算法 $M$，改造成单侧错误随机算法 $A$

# 例题

(1) $\mathrm{ZPP} \subseteq \mathrm{RP} \cap \mathrm{coRP}$

- 目标：给定问题 $L$ 的期望多项式时间判定算法 $M$，改造成单侧错误随机算法 $A$
- 给 $M$ 一个运行时间上限 $\tau$，超时则强行停止，输出 rej

# 例题

(2) $\mathrm{RP} \cap \mathrm{coRP} \subseteq \mathrm{ZPP}$

- 目标：给定问题 $L$ 的弃真型算法 $A$ 和取伪型算法 $B$，构造期望多项式时间算法 $M$

# 例题

(2) $\mathrm{RP} \cap \mathrm{coRP} \subseteq \mathrm{ZPP}$

- 目标：给定问题 $L$ 的弃真型算法 $A$ 和取伪型算法 $B$，构造期望多项式时间算法 $M$
- 反复运行 $A(x), B(x)$，直到它们给出相同结果

# 例题

(2) $\mathrm{RP} \cap \mathrm{coRP} \subseteq \mathrm{ZPP}$

- 目标：给定问题 $L$ 的弃真型算法 $A$ 和取伪型算法 $B$，构造期望多项式时间算法 $M$
- 反复运行 $A(x)$, $B(x)$，直到它们给出相同结果

算法 $M(x)$:

1. 重复独立运行 $A(x), B(x)$
2. 若 $A(x) = B(x)$，输出 $A(x)$；否则转 1