

随机算法

岳锴

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

Chebyshev's Inequality

对于随机变量 X 和 $\varepsilon > 0$,

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

概率不等式

Chernoff/Hoeffding Bounds

设 X_1, X_2, \dots, 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

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

(2) 对 $\beta > 0$, 有

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

(3) 对 $\lambda > 0$, 有

$$\frac{\Pr[X \geq \mu + \lambda]}{\Pr[X \leq \mu - \lambda]} \leq \exp\left(-\frac{2\lambda^2}{n}\right)$$

复杂性类

ZPP (zero-error probabilistic polynomial time)

称语言（问题） $L \in \text{ZPP}$ ，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) $L \in \text{RP}$, 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) $x \in L \implies \Pr[A(x) = \text{acc}] \geq 1/2$
- (2) $x \notin L \implies A(x) = \text{rej}$

- ▶ “弃真”型蒙特卡洛算法
- ▶ 例子: 合数

coRP

称语言(问题) $L \in \text{coRP}$, 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) $x \in L \implies A(x) = \text{acc}$
- (2) $x \notin L \implies \Pr[A(x) = \text{rej}] \geq 1/2$

- ▶ “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） $L \in \text{BPP}$ ，若存在多项式时间的随机算法 A ，使得对任意实例 $x \in \{0, 1\}^*$ ，

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

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

复杂性类

$$P \subseteq ZPP = RP \cap \text{co}RP \subseteq RP \subseteq BPP$$

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 $1/n$

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， $S = \{x_1, x_2, \dots, x_t\}$
- ▶ 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， $S = \{x_1, x_2, \dots, x_t\}$
- ▶ 令 $x^* = \text{median}(S)$
- ▶ 错误概率？

Amplification

已知弃真型算法 A

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

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

构造弃真型算法 A'

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

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

Amplification

已知弃真型算法 A

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

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

构造弃真型算法 A'

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

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

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

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

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

构造双侧错误算法 A'

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

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

Amplification

已知双侧错误算法 A

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

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

构造双侧错误算法 A'

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

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

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 α 和 rej 的次数 β ($\alpha + \beta = t$)
3. 若 $\alpha \geq \beta$, 则返回 acc
4. 若 $\alpha < \beta$, 则返回 rej

例题

证明: $\text{ZPP} = \text{RP} \cap \text{coRP}$

例题

证明: $ZPP = RP \cap coRP$

称语言（问题） $L \in ZPP$ ，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） $L \in RP$ ，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) $x \in L \implies \Pr[A(x) = \text{acc}] \geq 1/2$

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

称语言（问题） $L \in coRP$ ，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) $x \in L \implies A(x) = \text{acc}$

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

例题

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

- ▶ 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) $ZPP \subseteq RP \cap coRP$

- ▶ 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 τ ，超时则强行停止，输出 rej

例题

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

- ▶ 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) $\text{RP} \cap \text{coRP} \subseteq \text{ZPP}$

- ▶ 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) $\text{RP} \cap \text{coRP} \subseteq \text{ZPP}$

- ▶ 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