- 教材讨论
  - JH第5章第1、2节

问题1：随机算法的基本概念

- 你能从图灵机的角度分别阐述对于随机算法的这些理解吗？
  - a deterministic algorithm with an additional input that consists of a sequence of random bits
  - a set of deterministic algorithms from which one algorithm is randomly chosen for the given input
  - a nondeterministic algorithm that has a probability distribution for every nondeterministic choice

- 你能从上述这些角度分别解释$Random_A(x)$吗？
- 如果$Random_A(x)$不超过对数，意味着什么？

问题1：随机算法的基本概念 (续)

- 你能解释这两种时间复杂度的计算方式吗？
- 它们分别存在什么问题？怎么解决？

$$\textbf{\textit{Exp-Time}}_A(\boldsymbol{x}) = E[\textit{Time}] = \sum_C \textit{Prob}_{A,x}(C) \cdot \textit{Time}(C)$$

$$\textbf{\textit{Exp-Time}}_A(\boldsymbol{n}) = \max\{\textit{Exp-Time}_A(x) \mid x \text{ is an input of size } n\}$$

$$\textbf{\textit{Time}}_A(\boldsymbol{x}) = \max\{\textit{Time}(C) \mid C \text{ is a run of } A \text{ on } x\}$$

$$\textbf{\textit{Time}}_A(\boldsymbol{n}) = \max\{\textit{Time}_A(x) \mid x \text{ is an input of size } n\}$$

问题2：Las Vegas算法

- Las Vegas和Monte Carlo算法的区别是什么？

- 你理解Las Vegas算法的两种定义了吗？

$$Prob(A(x) = F(x)) = 1$$

$$Prob(A(x) = F(x)) \geq \frac{1}{2}$$

$$Prob(A(x) = \text{``?''}) = 1 - Prob(A(x) = F(x)) \leq \frac{1}{2}$$

- 它们分别采用了哪种时间复杂度的计算方式？
- 为什么会有这种区别？

$$\textbf{\textit{Exp-Time}}_A(x) = E[Time] = \sum_C Prob_{A,x}(C) \cdot Time(C)$$

$$\textbf{\textit{Exp-Time}}_A(n) = \max\{Exp\text{-}Time_A(x) \mid x \text{ is an input of size } n\}$$

$$\textbf{\textit{Time}}_A(x) = \max\{Time(C) \mid C \text{ is a run of } A \text{ on } x\}$$

$$\textbf{\textit{Time}}_A(n) = \max\{Time_A(x) \mid x \text{ is an input of size } n\}$$

问题2：Las Vegas算法 (续)

- 你能画个图解释一下one-way communication protocol吗？

- $Choice_n$是F的一个例子，它的直观含义是什么？
- 针对这个例子，P349的Las Vegas算法的思路是什么？
- 和一般的确定性算法相比，该算法优劣分别是什么？
- 该算法符合Las Vegas算法两种定义中的哪一种？

Las Vegas One-Way Protocol (D_I, D_{II})

Input: (x, j), $x = x_1 \ldots x_n \in \{0, 1\}^n$, $j \in \{1, \ldots, n\}$.

Step 1: D_I chooses a random bit $r \in \{0, 1\}$.

Step 2: D_I sends the message $c_1 c_2 \ldots c_{n/2+1} = 0 x_1 \ldots x_{n/2} \in \{0, 1\}^{n/2+1}$ if $r = 0$, and
D_I sends the message $c_1 c_2 \ldots c_{n/2+1} = 1 x_{n/2+1} \ldots x_n \in \{0, 1\}^{n/2+1}$ if $r = 1$.

Step 3: If $r = 0$ and $j \in \{1, 2, \ldots, n/2\}$ then D_{II} outputs $c_{j+1} = x_j$.
If $r = 1$ and $j \in \{n/2 + 1, \ldots, n\}$ then D_{II} outputs $c_{j-n/2+1} = x_j = Choice(x, j)$.
Else, D_{II} outputs "?".

- 你能不能改造这个算法，使它符合另一种定义？
- 改造之后，上述优劣发生了怎样的变化？

问题3：Monte Carlo算法

- 你能解释one/two-sided-error Monte Carlo算法吗？

(i) for every $x \in L$, $Prob(A(x) = 1) \geq 1/2$, and
(ii) for every $x \notin L$, $Prob(A(x) = 0) = 1$.

$$Prob(A(x) = F(x)) \geq \frac{1}{2} + \varepsilon.$$

- 它们在具体应用中分别如何使用？
- 我们为什么没有讨论它们的时间复杂度？转而讨论了什么？

- unbounded-和two-sided error Monte Carlo算法的区别是什么？

$$Prob(A(x) = F(x)) > \frac{1}{2}.$$

- 这种区别造成了什么结果？

1. Generate an $n \times 1$ random 0/1 vector $\vec{r}$.
2. Compute $\vec{P} = A \times (B\vec{r}) - C\vec{r}$.
3. Output "Yes" if $\vec{P} = (0, 0, \ldots, 0)^T$; "No," otherwise.

- Freivalds算法（验证矩阵乘法AXB=C）属于哪一类？

问题4：随机优化算法

- 你理解randomized δ-approximation
  和randomized δ-expected approximation算法了吗？

$(i)\ Prob(A(x) \in \mathcal{M}(x)) = 1,\ and$
$(ii)\ Prob(R_A(x) \le \delta) \ge 1/2$

$(i)\ Prob(A(x) \in \mathcal{M}(x)) = 1,\ and$
$(ii)\ E[R_A(x)] \le \delta$

- 这两种算法之间有什么关系？

- 你理解RPTAS了吗？

$(i)\ Prob(A(x, \delta) \in \mathcal{M}(x)) = 1\ \{for\ every\ random\ choice\ A\ computes\ a\ feasible$
$\quad solution\ of\ U\},$
$(ii)\ Prob(\varepsilon_A(x, \delta) \le \delta) \ge 1/2\ \{a\ feasible\ solution,\ whose\ relative\ error\ is\ at$
$\quad most\ \delta,\ is\ produced\ with\ the\ probability\ at\ least\ 1/2\},\ and$
$(iii)\ Time_A(x, \delta^{-1}) \le p(|x|, \delta^{-1})\ and\ p\ is\ a\ polynomial\ in\ |x|.$

- 它和PTAS的区别是什么？

问题5：随机算法的设计范式

- 你理解这三类设计范式的思想了吗？能不能各举一个例子？
  - Foiling an adversary
  - Abundance of witnesses (& fingerprinting)
  - Random sampling (& relaxation and random rounding)