

高级算法设计与分析

零知识证明

夏盟佶

Xia, Mingji

中科院软件所
计算机科学国家重点实验室

2016.6

NP里的语言

- 一个语言 $L : \Sigma^* \rightarrow \{0, 1\}$ 在NP中,
- 存在多项式时间可以判定的二元关系 R 和常数 k ,
使得 $x \in L$, 当且仅当存在 y , $|y| = |x|^k$ 并且 $R(x, y) = 1$ 。

多项式时间随机算法 P 、 V 是 L 的零知识证明

$\langle P(x, u), V(x) \rangle$ 表示证明者 P 得到输入 x, u ，验证者 V 得到输入 x 时，他们之间的交互证明。

如果以下三条成立：

- **Completeness:**
对任意的 $x \in L$ 以及 x 的一个证据 u （即 $R(x, u) = 1$ ）， V 接受 $\langle P(x, u), V(x) \rangle$ 的概率大于 $2/3$ 。
- **Soundness:** 如果 $x \notin L$ ，对于任何的 P^* 和 u ， V 接受 $\langle P^*(x, u), V(x) \rangle$ 的概率小于 $1/3$ 。
- **Perfect Zero Knowledge:** 对任何随机多项式时间的交互策略算法 V^* ，存在一个多项式期望时间的随机算法 S^* ，使得对任意的 $x \in L$ 以及 x 的一个证据 u ， $\langle P(x, u), V^*(x) \rangle$ 和 $S^*(x)$ 的概率分布相同。
 S^* 叫做 V^* 的模拟者。

图同构问题的零知识证明

- 图 $G_0(V_0, E_0)$ 和 $G_1(V_1, E_1)$ 是同构的，如果存在从 V_0 到 V_1 的一一对应 π ，使得 $(u, v) \in E$ 当且仅当 $(\pi(u), \pi(v)) \in E_1$ 。
- 不严格的直观： P 知道怎么从甲地到乙地，它要 V 相信它知道，但又不告诉 V 甲到乙的路。
- P 选取一个和甲乙都连通的丙地，让 V 随机问甲到丙或者乙到丙的路，然后告诉 V 这条路。

图同构问题的零知识证明

- V: G_0, G_1
P: G_0, G_1, π , 如果同构, $\pi(G_0) = G_1$
- P: 随机选取置换 π_1 , 把 $H = \pi_1(G_1)$ 送给 V。 (V 没得到 π_1 。)
- V: 随机选取 $b \in_R \{0, 1\}$, 送给 V。
- P: 如果 $b = 1$, 送 π_1 给 V; 如果 $b = 0$, 送 $\pi_1 \circ \pi$ 给 V。
- V: 刚收到的置换记为 π' , 接受, 如果 $H = \pi'(G_b)$ 。

$$G_0 \xrightarrow{\pi} G_1 \xrightarrow{\pi_1} H$$

零知识

- 用一个没知识 π 的模拟者 S^* ，模拟任何 V^* 和 P 的交互。
- S^* 猜一个 $b' \in \{0, 1\}$ 。随机选取置换 π_1 ，用 $\pi_1(G_{b'})$ 作为 P 给 V 的第一条信息。
- 随后模拟 P 和 V 的行为。猜对了，即 $b' = b$ ，就模拟成功，最后一条 P 发送的信息是 π_1 ；猜错了就从头再来。

参考文献

- Sanjeev Arora, Boaz Barak: Computational complexity, a modern approach 第九章密码学