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$L : \Sigma^* \to \{0, 1\}$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

$< P(x,u), V(x) >$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$< P(x,u), V(x) >$的概率大于$2/3$。

多项式时间随机算法P、V是L的零知识证明

$< P(x,u), V(x) >$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$< P(x,u), V(x) >$的概率大于$2/3$。
- Soundness：如果$x \notin L$，对于任何的P^*和u，V接受$< P^*(x,u), V(x) >$的概率小于$1/3$。

多项式时间随机算法P、V是L的零知识证明

$< P(x,u), V(x) >$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$< P(x,u), V(x) >$的概率大于$2/3$。
- Soundness：如果$x \notin L$，对于任何的P^*和u，V接受$< P^*(x,u), V(x) >$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，$< P(x,u), V^*(x) >$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$(\pi(u), \pi(v)) \in E_1$。

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。

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，$\pi(G_0) = G_1$

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。）

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。

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。

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$H = \pi'(G_b)$。

$$G_0 \longrightarrow^{\pi} G_1 \longrightarrow^{\pi_1} H$$

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。

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。

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