The Knowledge Complexity of Interactive Proof System

Abstract

通常来说, 一个证明会包含超过仅仅证明命题正确所需要的知识. 比如, 去证明一个图中包含哈密顿回路. 然而, 这个证明显然包含的知识要超过是/否这个 1 位的答案.

在这篇论文当中讨论发展了关于"知识"的计算复杂度理论. 零知识证明被定义为除了命题正确性外不传递任何额外知识的证明. 二次剩余 (quadratic residuosity) 和二次非剩余 (quadratic nonresiduosity) 问题是零知识证明系统的例子. 他们是第一个零知识证明的例子但其形式语言还并未被充分认识

Introduction

通常说一个语言 L 是 NP 的等价于对 L 存在一个多项式时间的"证明系统", 其给定一个输入 x, 一个证明者 (prover) 生成一个字符串 α, 验证者 (verifier) 利用 x 和 α 在多项式时间内计算给定的 x 的二进制表示属于 L. 问是否有更通用,(可能) 更自然的多项式时间内的证明系统是很合理的, 本文提出了一个这样的概念

我们仍然允许验证者只使用多项式时间，而证明者是任意的计算能力，但现在将允许双方翻转无偏见的硬币。结果是 NP 的概率版本，其中允许小概率的错误。然而，为了获得这个猜想的完全一般性，我们还必须允许证明者和验证者进行交互（即来回交谈）并保密他们的硬币抛掷。我们将这些证明系统称为"交互式证明系统"。这个概念正式在第 2 节中定义，我们还定义了语言具有交互性证明系统的含义。

如何使用这种交互证明的力量还远不清楚。带有非确定性多项式时间算法或概率多项式时间算法的语言具有很少或没有交互的证明系统。因此，期望例子是没有非确定性也没有概率多项式时间算法的语言，但具有交互式证明系统。虽然我们这里没有提供任何这样的例子，现有文献中有例子。使用这篇轮文最初版本的想法 [GMR] Goldreich、Micali 和 Wigderson[GMW] 表明"非同构图"语言具有交互式证明系统

...

不管怎么样, 已有工作表明: 一个语言拥有交互式证明系统等价于其含有 Arthur-Merlin 证明系统

然而，我们的交互式证明系统的概念可以概括为解决新问题的正确方法。这篇论文的主要目的，在事实上，就是使用交互式证明系统来研究一个自然的问题；多少知识在 L 语言的交互

式证明系统中传输给验证者？例如，考虑 SAT 问题，满足命题演算的句子的 NPC 语言。在明显的证明系统中，为了证明 F⊆ SAT，证明者给出满足公式 F 的赋值，然后验证者可在多项式时间检查验证。这些赋值给了验证者更多的知识，而不仅仅是事实 F⊆ SAT；它也给出了令人满意的赋值。在另一个极端，每一种语言可以在概率多项式时间内被接受的有一个证明系统，其中证明者什么都不做，因此不向验证者提供任何知识。

我们说 L 的交互式证明系统是零知识的，如果对于每个 $x \subseteq L$，证明者除了 $x \subseteq L$ 之外，基本上什么都不告诉验证者；即使验证者选择不遵循证明系统而是尝试（在多项式时间内）欺骗证明者揭示某些东西，情况也应该如此。零知识的概念在第 3 节中正式定义。这个定义是本文的重要贡献。

自从这些结果首次出现以来，最重要的发展是 Goldreich、Micali 和 Wigderson [GMW] 的证明，即根据共同的复杂性理论假设，每个 NP 语言都有一个零知识交互式证明系统。这些 NP 语言的证明系统似乎在几乎所有协议问题中都有应用。几乎可以肯定，这些结果将在未来极大地简化分布式密码协议设计，正如 [GMW2] 的强大结果所证明的那样。

Interactive proof system

交互式图灵机和协议

交互式证明系统

定义: 让 L 成为 $\{0,1\}^*$ 之上的语言。让 (A,B) 成为交互式协议。如果我们有以下条件，我们说 (A, B) 是 L 的交互式证明系统：

(1) 对于每个 k，对于作为 (A, B) 的输入且 L 中足够大的 x，B 以至少 $1-|x|^{-k}$ 的概率停止并接受。（这里的概率取自 A 和 B 的抛硬币。）

(2) 对于每个 k，对于不在 L 中的足够大的 x，对于任何交互式图灵机 A'，在 (A', B) 的输入 x 上，B 以最多 $|x|^{-k}$ 的概率接受。（这里的概率来自于 A' 和 B 的抛硬币。）

备注 1. 通过多次重复协议并选择以多数票接受的标准技术，可以将上述错误概率降低到小于 $2^{-|x|}$。

我们现在讨论，这个定义从一个有效的证明系统中捕获了我们直观地想要的东西。条件（1）

本质上说，如果 $x \subseteq \mathbf{L}$，B 将以压倒性的概率接受。条件 (2) 表明，如果 x 不在 L 中，则不存在以不可忽略的概率成功说服 B 接受的策略。事实上，B 不需要信任（或知道它的程序）与之交互的机器。B 相信自己抛硬币的随机性就足够了。

zero-knowledge

我们将给出一个更一般的定义，而不是只为交互式证明系统给出零知识的定义。我们将定义任何交互式协议 (A, B) 对语言 L 的零知识的含义，无论 (A, B) 是否是 L 的证明系统。实际上这个定义根本不依赖于 B ; 正如我们将看到的，它表示对于每个多项式时间 B'，当与输入 $x \subseteq \mathbf{L}$ 交互时，B'"看到"的分布与可以在多项式时间内从 x 计算的分布"无法区分"。因此，我们首先关注随机变量不可区分的概念。

The quadratic residuosity problem

让 **N** 表示正整数集合,$x \subseteq \mathbf{N}$ 并且 $\mathbf{Z}_{\mathbf{x}}^* = \{y \mid 1 \leq y < x, gcd(x, y) = 1\}$, 如果 $\exists w \subseteq \mathbf{Z}_{\mathbf{x}}^*$ 使得

$$w^2 \equiv y \bmod x$$

我们称 y 在 $\mathbf{Z}_{\mathbf{x}}^*$ 中是 x 的二次剩余, 不然, 我们称 y 为 x 的二次非剩余

事实 1 *y 是 x 的二次剩余等价于 y 是 x 所有素因子的二次剩余*

定义二次剩余的判别函数如下:

$$Q_x(y) = \begin{cases} 0 & \text{如果 y 是 x 的二次剩余} \\ 1 & \text{反之} \end{cases}$$

因此有接下来的事实.

事实 2 *对于给定的 y 和 x 的素分解, $Q_x(y)$ 能够在多项式时间 $|x|$ 内被计算*

让 $y \subseteq \mathbf{Z}_x^*$ 和 x 的素分解为 $\prod_{i=1}^k p_i^{\alpha_i}$. 那么雅可比符号定义为

$$(y/x) = \prod_{i=1}^k (y/p_i)^{\alpha_i}$$

当 y 是 p_i

的二次剩余, 则有 $(y/p_i) = 1$, 否则为-1

事实 3 *对给定的 $x \subseteq \mathbf{N}$ 和 $y \subseteq \mathbf{Z}_x^*$, (y/x) 能够在多项式时间 $|x|$ 内被计算*

$y \bmod x$ 的 Jacobi 符号给出了一些关于 y 是否是 x 二次非剩余的信息。如果 $(y/x) = —1$ ，则 y 是 x 的二次非剩余且 $Q_x(y) = 1$。然而，当 $(y/x) = 1$ 时，没有已知有效的（概率或确定性多项式时间)解决方案可正确计算 $Q_x(y)$,且概率明显高于 1/2. 这导致了二次剩余问题的公式化。

定义 1 *我们将二次剩余问题定义为在输入 x 和 y 上计算 $Q_x(y)$ 的问题，其中 y 在 $\mathbf{Z}_x^*$ 且 $(y/x) = 1$*

当前计算 $Q_x(y)$ 的最佳算法是首先考虑 x 的分解和然后计算 $Q_x(y)$ 。实际上，因式分解整数和计算 Q_x 已被推测为具有相同的时间复杂度[1]。二次剩余问题的难度已被用作设计几种密码协议的基础 [GM]、[LMR]、[B1]。

定义如下两个语言

$$\mathbf{QR} = \{(x, y) | x \subseteq \mathbf{N}, y \subseteq \mathbf{Z}_x^*,\ Q_x(y) = 0\},$$
$$\mathbf{QNR} = \{(x, y) | x \subseteq \mathbf{N}, y \subseteq \mathbf{Z}_x^*, (y/x) = 1\ Q_x(y) = 1\}$$

x 和 y 都用二进制表示

显然，根据事实 1 和 2，QR 和 QNR 都在 CO-NP 和 NP 问题的交集处。然而，没有已知的概率多项式时间算法可以接受这些语言，因此它们不是平凡的零知识。在第 5 节中，我们展示了 QR 的完美零知识证明系统，在第 6 节中，我们展示了 QNR 的统计零知识证明系统。以下事实在第 5 节和第 6 节的零知识证明中很有用。

事实 4 *设 $x \subseteq \mathbf{N}$。然后，对于任意 y 满足 $Q_x(y) = 0$ ，$w \subseteq \mathbf{Z}_x^*$。满足 $w^2 \equiv y \bmod x$ 解的数量是相同的（与 y 无关.)。*

事实 5 *设 $x \subseteq \mathbf{N}$, $y, z \subseteq \mathbf{Z}_x^*$。那么我们有以下内容:*
(a) 如果 $Q_x(y) = Q_x(z) = 0$，则 $Q_x(yz) = 0$
(b) $Q_x(y) \neq Q_x(z)$，则 $Q_x(yz) = 1$.

事实 6 *给定 x, y，欧几里得算法 (求最大公约数) 多项式时间内计算完成, 无论 $y \subseteq \mathbf{Z}_x^*$*

[1]整数分解是复杂的的非多项式时间内可求解的问题,Prover 的计算能力无法完成求解

Zero-knowledge proofs of quadratic residuosity

我们将首先非正式地描述我们针对 QR 的零知识交互证明系统，然后更严格地描述它。假定 A 和 B 被给定 (x,y),|x|=m, 进入如下的操作 m 次:

$i \leftarrow m$;
while *i != 0* **do**
  A 向 B 发送一个随机 x 的二次剩余 u ;
  B 向 A 发送一个随机位 bit。;
  if $bit = 0$ **then**
    • 则 A 向 B 随机发送方程 ($w^2 \equiv u \bmod x$) 的一个解 w ， 如果 bit = 1,
  else
    A 向 B 随机发送方程 ($w^2 \equiv uy \bmod x$) 的一个解 w。
  end
  • B 检查 [bit = 0 且 $w^2 \bmod x \equiv u$]^2 or [bit = 1 且 $w^2 \bmod x = (uy) \bmod x$] ;
  $i--$;
end

Algorithm 1: 交互式证明过程

证明解答: A 向 B 证明 $Q_x(y) = 0$, 但要求保持零知识性, 不管 B 采用什么策略，也无法从 A 这里得到“y 是模 x 的二次剩余”外的任何信息, 如果 A 向 B 展示了 x 的素分解或任意随机解 w, 显然是不符合零知识的要求的, 因为 A 的计算能力是 arbitrary 的,A 可以随意获得一个随机的 x 的二次剩余 u, 并且 A 可以随时构造下面两个等式

$$Q_x(u) = 0$$
$$Q_x(uy) = 0$$

考虑下面三个因素:

- **completeness**： 只要正确皆可通过验证, 如果 $Q_x(y) = 0$ 成立, 以 A 的计算能力, 上述两个等式显然不管 B 如果构造随机 bit, 其都是成立的

- **soundness**： 只要错误皆无法通过验证, 如果 $Q_x(y)! = 0$, 由于 A 不知道随机 bit, 当 B 发送 0,A 可以蒙混过关, 但 B 发送 1,A 此时无论如何也无法满足 $Q_x(uy) = 0$ 的, 因为这违背了上述提到的事实 5, 但 B 可以在多项式时间内检查这个等式, 即多次试验后,A 被暴露的概率为 $1 - \frac{1}{2^m}$

- **zero knowledge**： proof 的信息不增加解密能力, 这里需要用到关于模拟的数学语言的严格证明, 原论文中含有该证明