第8卷第7期
1997年7月

软件学报
JOURNAL OF SOFTWARE

Vol. 8, No. 7
Jul. 1997

关于图的非同构问题零知识交互证明协议*

郭宝安　卢开澄

（清华大学计算机系　北京　100084）

摘要　对于图的非同构问题，设计一种交互式零知识的证明协议，许多文章都有讨论，但都是不完善的，本文给出了一个完整的关于图的非同构零知识交互证明协议.

关键词　密码学，复杂性，零知识证明，图同构.

中图法分类号　TP301

Goldreich，Micali 和 Wigderson 在文献[1]中研究了零知识证明协议的设计与密码体制及数论问题之间的关系，通过对图的同构问题和图的非同构问题的零知识证明协议的设计，说明了只要存在难解的问题，都可设计零知识证明协议.

所谓的零知识证明协议是指一个证明者 P 是一个具有无限计算能力的图灵机，向一个仅具有多项式计算能力的图灵机（验证者）V 证明他宣称的一个结论是正确的过程，在此过程中，验证者 V 除了相信 P 的宣称以外，得不到其它额外的信息，允许 P，V 违背协议.

严格地讲，假设 P，V 是 2 个概率图灵机，P 有无限的计算能力，V 的计算能力是多项式的，若一个交互式证明协议满足以下 3 点，就称此协议为一个零知识交互式证明协议：

（1）完备性：如果 P 的声称是真的，则 V 以绝对优势的概率接受 P 的结论.

（2）有效性：如果 P 的声称是假的，则 V 以绝对优势的概率拒绝 P 的结论.

（3）零知识性：无论 V 采取任何手段，当 P 的声称是真的，P 不违背协议时，V 除了接受 P 的结论以外，得不到其它额外的信息.

这里的零知识性是指 V 如果违背协议，并且掌握从其它渠道获得的信息，也无法从 P 那里获得额外知识，V 自己独立运行所输出的随机变量和 V 与 P 交互后所输出的随机变量对 V 而言是不可区分的.

图的同构问题（GI）：

设有 2 个无向图 $G_1=(V_1,E_1)$，$G_2=(V_2,E_2)$，它们的顶点数和边数都相等，问是否存在一个置换 φ，使得对任意的 $(u,w)\in E_1$，一定有 $\varphi(u,w)\in E_2$ 成立？

图的非同构问题（GNI）：

设有 2 个无向图 $G_1=(V_1,E_1)$，$G_2=(V_2,E_2)$，它们的顶点数和边数都相等，问是否不存

---

* 本文研究得到中国博士后基金和中央机要局“八五”密码基金资助. 作者郭宝安，1963 年生，博士后，讲师，主要研究领域为密码学，数学，通信，计算机科学. 卢开澄，1931 年生，教授，主要研究领域为密码学，数学，计算机科学，信息论.

本文通讯联系人：郭宝安，北京 100084，清华大学计算机系

本文 1996-07-21 收到修改稿

在一个置换 φ,使得对任意的 $(u,w)\in E_1$,一定有 $\varphi(u,w)\in E_2$ 成立?

我们总是假定在作置换之前已经对图的顶点作了一定的排序,如字典序.显然图的同构问题(GI)是属于NP的,但是否属于NPC人们还不清楚,人们相信它是不属于NPC的,可关于这些认识,至今都没有一个完整的证明,只是一种想法而已.对图的非同构问题(GNI)也有类似的结论.目前还不知道是否属于NP,一般认为不属于NP类,只能说GNI $\in$ C_o-NP_o.

以下我们总是假设图的同构问题(GI)和图的非同构问题(GNI)都是困难的,在多项式时间是概率图灵机无法解决的问题.所有的协议都是基于这一点.

所以,如果能够设计出图的同构问题(GI)和图的非同构问题(GNI)的零知识证明协议,那么可以肯定地说这2个问题都是属于零知识证明问题类(ZIP)的,用ZIP表示所有可以通过零知识交互证明可解决的问题类.这样,对充分认识图的同构问题(GI)和图的非同构问题(GNI)的性质及其归属是有重要帮助的.

1 GNI问题的零知识证明协议

对于图的同构问题(GI),文献[1]给出了一个完整的零知识证明协议:

假设 P 是一个具有无限计算能力的概率图灵机,称其为证明者,V 是一个多项式规模的概率图灵机,称其为验证者,假设 P 知道2个无向图 G_1,G_2,是同构的,同构置换为 φ,即 $G_1=\varphi G_2$,P 在不向 V 透露任何关于 φ 的信息的情况下向 V 证明 P 知道这样的 φ,由GI问题的特点和 P 具有自己的随机带的特点,P 需要作图的随机置换 π 将图 G_1 的顶点和边作置换.

协议1.1

(1) P 随机选择一置换 π,将 G_1 变换为图 H,$H=\pi G_1$,将 H 发送给 V;

(2) V 随机选择 $\alpha\in\{1,2\}$,发送 α 给 P;

(3) P 判断 α 是否属于 $\{1,2\}$,如果不属于 $\{1,2\}$,则拒绝.

  如果 $\alpha=1$,记 $\theta=\pi$;

  如果 $\alpha=2$,记 $\theta=\pi\varphi^{-1}$;

  P 发送 θ 给 V;

(4) V 验证 H 在 θ 的变换下是否等于 G_α,即 $H=\theta G_\alpha$ 是否成立.若不成立就拒绝接受 P 的宣称,若是,则接受;

这个协议需要重复执行 n 圈,才能使 V 以趋向于1的概率接受 P 的结论.因为执行一圈后,P 对 V 进行欺骗的概率是1/2,V 只能得到图 G_1 或 G_2 的一个随机拷贝,这一点他自己也可独立地完成,所以此协议是零知识的.

此协议不要求 P 有无限的计算能力.

以下我们来看一个图的非同构GNI问题的证明协议.

协议1.2

设有2个无向图 $G_1=(V_1,E_1)$,$G_2=(V_2,E_2)$,如上所提的GNI问题,

证明者 P 知道这2个无向图是不同构的,P 向验证者 V 证明这一点.

一般认为它不属于 NPC,只是属于 $Co\text{-}NP$. 证明步骤为:

(1) V 为验者,V 从它自己的随机带上读取 n 比特随机数 $b_1,b_2,...,b_n$ 和 n 个随机置换 $\pi_1,\pi_2,...,\pi_n$,根据 π_i 和 b_i 计算新的同构图 H_i,

$$H_i=\begin{cases}\pi_i(G_1), & \text{若 } b_i=0,\quad i=1,2,...,n\\ \pi_i(G_2), & \text{若 } b_i=1,\end{cases}$$

V 发送 $H_1,H_2,...,H_n$ 给 P.

(2) 因为 P 有无限的计算能力,P 计算二进制序列 $c_1,c_2,...,c_n$,

$$c_i=\begin{cases}0 & \text{若 } H_i\cong G_1,\quad i=1,2,...,n\\ 1 & \text{若 } H_i\cong G_2,\end{cases}$$

P 发送 $c_1,c_2,...,c_n$ 给 V.

(3) V 检查 c_i 是否等于 b_i,对 $i=1,2,...,n$,若有一个不等,则拒绝接受 G_1 不同构于 G_2 的结论;否则可接受此结论.

此协议满足:

1. 若 (P,V) 的输入为 x:G_1 不同构于 G_2,P,V 都遵守协议的话,V 一定会接受此结论;
2. 若 (P,V) 的输入为 x:G_1 同构于 G_2,则对任意与 V 交互的 P',它都不能由 H_i 正确预测 b_i,因为 $H_i\cong G_1$,$H_i\cong G_2$ 同时成立,P' 只能瞎猜 c_i,但是 $c_i=b_i$ 的概率为 1/2,所以对所有的 i,$c_i=b_i$ 都成立的概率为 $1/2^n$,当 $n\to\infty$ 时,此概率趋向于 0;
3. V 的计算能力为多项式阶的.

在以上的图的非同构证明协议可能不是零知识的,因为验证者可能通过此协议来测试另外一个图 H_i,同 G_1 或 G_2 中的哪一个图是同构的. 所以,在交互式证明系统中,怎样来判断它是零知识的是比较困难的事情,这就给论证协议的安全性提出了新的课题,现在有许多协议初看起来是安全的,是零知识的,但是仔细考察起来却不是. 当前对许多零知识方面的定理证明也仅限于一种说明性质的论证,缺乏严格的数学证明,需要进一步的严格论证.

所以,关于图的非同构问题的零知识证明协议[2],应修改为如下形式:

前提:P 向 V 证明他知道 2 个图 G_1 和 G_2 不是同构的,P 有无限的计算能力.

协议 1.3

(1) V 随机选择 $b\in\{0,1\}$,随机选择置换 π,做图 G_{b+1} 的随机拷贝 $H=\pi(G_1)$,V 将 H 发给 P.

(2) V 向 P 零知识的证明他的确知道 H 是和图 G_1,G_2 中的之一是同构的;

(3) P 判断,如果 H 和 G_1 同构,记 $c=0$,如果 H 和 G_2 同构,记 $c=1$,否则拒绝,P 将 c 发给 V.

(4) V 判断 c 是否和 b 相等,若相等,则接受,否则拒绝.

此协议需执行 n 圈. 这个协议初步看来是零知识的,它的零知识性依赖于关键的第 2 步,虽然文献[1]的作者说明了以下定理:

定理 1.1. GNI 问题是属于 ZIP 问题类的.

但是,由于文献[1]中以及后来的所有文献都没有对以上协议的第 2 步提出严格的正式的零知识协议,所以我们认为有必要对以上定理进行严格论证.

下面我们给出一个针对协议 1.3 的第 2 步的零知识证明协议.

2　新问题的零知识证明协议

我们可以明显地看出，零知识的证明图 H 和 2 个图 G_1 及 G_2 中的之一是同构的，决不同于 2 个图 G_1 和 G_2 是同构的 GI 问题的零知识证明，所以协议 1.1 是不能直接用于协议 1.3 的，所以我们需要对新的问题进行零知识证明协议的设计.

前提：P,V 均是多项式时间的概率图灵机，P 知道图 H 同 2 个图 G_1 和 G_2 之一是同构的，并且知道同构置换是 β，$H=\beta G_1$ 或 $H=\beta G_2$，P 向 V 零知识的证明这一点，协议如下.

协议 2.1

(1) P 随机选择比特串 $B=b_1b_2...b_n$，$b_i=0$ 或 1，和随机置换对 (α_1,π_1)，(α_2,π_2)，...，(α_n,π_n)，

对 $i=1,2,...,n$ 计算：

若 $b_i=0$，$C_i=(\alpha_iG_1,\pi_iG_2)$

若 $b_i=1$，$C_i=(\alpha_iG_2,\pi_iG_1)$

发送 $C_1,C_2,...,C_n$ 给 V；

(2) V 随机选择比特串 $D=d_1d_2...d_n$，$d_i=0$ 或 1，并发送给 P；

(3) P 对 $i=1,2,...,n$，计算：

若 $d_i=0$，$E_i=(\alpha_i,\pi_i)$；

若 $d_i=1$，$E_i=(\beta\alpha_i^{-1},\beta\pi_i^{-1})$；

发送 $E_1,E_2,...,E_n$ 给 V；

(4) V 进行验证：对 $i=1,2,...,n$.

若 $d_i=0$，则 $C_i=(\alpha_iG_1,\pi_iG_2)$；

若 $d_i=1$，则 H 应和 $(\beta G_2,\beta G_1)$ 或 $(\beta G_1,\beta G_2)$ 2 个分量中的之一相等；

当这 2 点有一点不满足时，V 拒绝承认 P 的结论，都满足时就接受 P 的结论.

完备性：如果 P,V 双方都遵守协议，则 V 一定会接受 P 的结论；

有效性：如果 P 的 H 不是 G_1 或 G_2 的一个拷贝，则 P 欺骗成功的概率为 $1/2^n$；

零知识性：如果在图的同构问题是困难的假设前提下，由于 P,V 都是多项式时间的，所以在 V 不知道随机序列 B 的条件下，V 是无法知道 H 到底和 G_1,G_2 中的哪一个是同构的，所以是零知识的.

通过将协议 2.1 嵌入协议 1.3 中，我们可得到一个完整的图的非同构问题的交互式零知识协议，只是交互圈数增加到了 6 圈，如何设计出低于 6 圈的协议是一个新的技术问题.

对于我们所设计的 GNI 问题的协议的安全性，请大家进行分析和攻击.

参考文献

1　Goldreich O, Micali S, Wigderson A. Proofs that yield nothing but their validity and a methodology of cryptographic protocol design. FOCS, 1986. 174～187.

2　朱洪，吴京. 零知识证明浅介. 密码与信息，1992，(4)：1～38.

THE ZERO-KNOWLEDGE PROOF PROTOCOL OF THE NONISOMORPHISM OF GRAPHS

GUO Bao'an　LU Kaicheng

(*Department of Computer Science　Tsinghua University　Beijing*　100084)

Abstract　The discussion of the zero-knowledge proof protocol of the nonisomorphism of graphs (GNI) has appeared in many papers, but they are not complete zero-knowledge proof protocols at all. This paper proposed a complete zero-knowledge proof protocol on the problem.

Key words　Cryptograph, complexity, zero-knowledge proof, nonisomorphism of graphs.

Class number　TP301