相对化 One-Way 函数的存在性 *

曹子宁[1], 吕义忠[2], 石纯一[1]

[1](清华大学 计算机科学与技术系,北京 100084);

[2](南京航空航天大学 计算机科学与工程系,江苏 南京 210016)

E-mail: caozn@263.net

摘要: One-Way 函数在计算复杂性和密码技术中均有重要的应用. 将 Grollmann 和 Selman 的结果推广到相对化和非一致复杂类的情形,证明了复杂类 UP/poly, UP, P/poly 等之间的包含关系与强相对化 one-way 函数、弱相对化 one-way 函数存在问题的等价性.

关键词: 计算复杂性;one-way 函数;相对化;非一致复杂类

中图法分类号: TP301 **文献标识码**: A

One-Way 函数在计算复杂性和密码技术中均有重要的应用. 粗略地讲,one-way 函数是多项式时间可计算函数,但其逆函数却不是多项式时间可计算的.

Grollmann 和 Selman 在文献[1]中证明了 one-way 函数存在$\Leftrightarrow P\neq UP$,其中 P 为确定图灵机在多项式时间内所接受的语言类,UP 为至多只有一条接受路径的不确定图灵机在多项式时间内所接受的语言类.

对于给定的字符集 Σ,Γ,函数 $f:\Sigma^*\to\Gamma^*$ 为 one-way 函数当且仅当

(1) f 为多项式时间可计算函数;

(2) f 为单射函数;

(3) f 为 honest 的,即存在多项式 $p(n)$,使得对任何 x, $|x|\leqslant p(|f(x)|)$. 这里,$|s|$ 为字符串 s 的长度;

(4) f^{-1}不是多项式时间可计算的.

如此严格定义的 one-way 函数,迄今还未找到一个. 但是,根据密码技术,人们相信 one-way 函数是存在的. 当然,由于 $P\subseteq UP\subseteq NP$,因此由 one-way 函数存在便可推出 $P\neq NP$. 所以,证明其存在性是非常困难的.

Grollmann 和 Selman 的结果是在图灵模型下证明的. 文献[2]在布尔线路模型中证明了相应的结果. 文献[3]提出了分层 one-way 函数的概念,用逆函数不能在 k 次多项式时间内计算代替原定义中逆函数不能在多项式时间内计算的要求,证明了其存在性等许多性质. 文献[4]将分层的概念推广到布尔线路中,证明了布尔线路分层 one-way 函数的相应性质. 在计算复杂性理论中,另一个重要的开问题是:NP-P/poly$\neq\varnothing$? 易见,若结论成立,则 $P\neq NP$. 文献[5]证明了若 $NP\subseteq P$/poly,则 $PH\subseteq\sum_2^p$. 文献[6]改进了这一结果,证明了若 $NP\subseteq P$/poly,则 $PH\subseteq ZPP$(从而 $PH\subseteq\sum_1^p$). 近年来的研究表明,计算复杂性中的有关问题很可能在非一致复杂类方面获得突破,问题

* **收稿日期**: 1999-10-13; **修改日期**: 2000-03-23

基金项目: 国家自然科学基金资助项目(69875007);江苏省自然科学基金资助项目(BK99119)

作者简介: 曹子宁(1972-),男,浙江人,博士生,主要研究领域为多 Agent 系统;吕义忠(1937-),男,江苏人,教授,主要研究领域为数理逻辑,理论计算机科学;石纯一(1935-),男,河北人,教授,博士生导师,主要研究领域为人工智能基础.

NP-P/poly$\neq\varnothing$?将 NP 类与非一致复杂性类 P/poly 联系起来,因此对该问题的研究可为解决 P-NP 问题提供一条途径.在这方面更强的一个开问题是UP-P/poly$\neq\varnothing$?易知,若UP-P/poly$\neq\varnothing$,则有 NP-P/poly$\neq\varnothing$.

本文将问题 UP-P/poly$\neq\varnothing$? 与相对化 one-way 函数的存在性联系起来,证明了这两类问题的等价性.由于计算复杂性中的许多开问题的相对化情形已得到解决,因此本文的结果将为解决 UP-P/poly$\neq\varnothing$? 及有关的一系列问题提供一条途径.

1 相对化 one-way 函数的存在性

本文将讨论复杂类 UP/poly,UP 等与 P/poly 之间的包含关系及其与强相对化 one-way 函数、弱相对化 one-way 函数存在性的联系.不失一般性,假设图灵机的输入字符集为{0,1}.本文中所指的函数包括偏函数和全函数.下面首先给出几个类的定义:

定义 1. $UPSV=\{f\mid f$ 为具有惟一一条计算路径的不确定图灵机在多项式时间内可计算的函数$\}$.

定义 2. $PF=\{f\mid f$ 为确定图灵机在多项式时间内所计算的函数$\}$.

定义 3. 设 C 是一个集合类,F 是一个函数集,则 $C/F=\{B\mid\exists\ A\in C\exists\ f\in F(B=\{x\mid\langle x,f(|x|)\rangle\in A\})\}$.

定义 4. UP/poly$=\{B\mid\exists\ A\in UP\exists\ f\in$poly$(B=\{x\mid\langle x,f(|x|)\rangle\in A\})\}$.

定义 5. $UPSV$/poly$=\{f\ f$ 为函数且$\exists\ g\in UPSV\exists\ h\in$poly$\forall\ x(f(x)=y\Leftrightarrow g(x,h(|x|))=y)\}$.

定义 6. P/poly$=\{B\mid\exists\ A\in P\exists\ f\in$poly$(B=\{x\mid\langle x,f(|x|)\rangle\in A\})\}$.

定义 7. PF/poly$=\{f\mid f$ 为函数且$\exists\ g\in PF\exists\ h\in$poly$\forall\ x(f(x)=y\Leftrightarrow g(x,h(|x|))=y)\}$.

其中 poly 是函数类,函数 $f\in$poly 当且仅当:$\exists$ 多项式 $p\forall\ x(|f(x)|\leqslant p(|x|))$.其他有关概念见文献[7,8].

定义 8. 对于给定的字符集 $\sum$,$\sum^*$ 的子集 S 为稀疏集是指存在一个多项式 p,使 $|S^{\leqslant n}|\leqslant p(n)$,其中 n 为自然数,$|S^{\leqslant n}|$ 为 S 中长度不超过 n 的字符串的个数.

定义 9. 强相对化 one-way 函数是满足下列条件的函数 f

① f 是多项式时间可计算的;

② f 是单射;

③ f 是 honest 的;

④ 不存在稀疏集 S,使 f^{-1}借助于 S 相对多项式时间可计算.

定义 10. 弱相对化 one-way 函数是满足下列条件的函数 f

① 存在稀疏集 S,使 f 借助于 S 相对多项式时间可计算;

② f 是单射;

③ f 是 honest 的;

④ 不存在稀疏集 S,使 f^{-1}借助于 S 相对多项式时间可计算.

引理 1. 函数 $f\in PF$/poly$\Leftrightarrow$存在稀疏集 S,使借助于 S,f 相对多项式时间可计算.

本引理及证明类似于文献[8]中的定理 3.1.

定理 1. 以下命题等价

(1) UP-P/poly$\neq\varnothing$;

(2) 存在强相对化 one-way 函数;

(3) $UPSV\text{-}PF/\text{poly}\neq\varnothing$.

证明:(1)⇒(2)

设 $A\in UP\text{-}P/\text{poly}$,$M$ 为在多项式时间内接受 A 的有至多一条接受路径的不确定图灵机.

令 $f(x)=\begin{cases}y & \text{如果 } x=(y,\text{comp}(y)),\\ x & \text{否则.}\end{cases}$

其中 comp(y)表示 M 在 y 上的惟一接受路径的编码.

易见,f 满足强相对化 one-way 函数定义中的①~③,下面证明不存在稀疏集 S,使 f^{-1} 借助于 S 相对多项式时间可计算.反设,有稀疏集 S,使 f^{-1} 借助于 S 相对多项式时间可计算.

由引理 1 知,$f^{-1}\in PF/\text{poly}$,即$\exists\, g\in PF\ \exists\, h\in\text{poly}$ 使得 $g(y,h(|y|))=f^{-1}(y)$.构造一个确定图灵机 M' 如下:当输入 y 后,借助于 $h(|y|)$,模仿计算 g 的确定图灵机,若计算出$\langle y,z\rangle$,则在 M' 上对输入 y 模仿 z 编码的动作;若最后到达接受状态,则 M' 接受.否则,不接受.由 f 和 M' 的构造可知,$x\in A\leftrightarrow x$ 被 M' 借助于函数 h 所接受.又由于计算 g 的图灵机是多项式时间的,且由于 z 是 M 对输入 y 的计算路径的编码,而 M 可在多项式时间内接受 A,故在 M' 上对输入 y 模仿 z 编码的动作,也只需多项式时间,因此,A 可被 M' 借助于函数 h 在多项式时间内所接受,故 $A\in P/\text{poly}$,与前提矛盾.因此(1)→(2)成立.

(2)⇒(3)

设 f 满足强相对化 one-way 函数定义中的①~④,则 $f^{-1}\in UPSV\text{-}PF/\text{poly}$,证明如下:

先证 $f^{-1}\in UPSV$,因为当输入 x 后,可惟一地猜测 y,模仿计算 f 的图灵机对 y 进行计算,若 $f(y)=x$,则输出 y,否则,不输出.由于 f 是单射,故若 $f(y)=x$,则 $y=f^{-1}(x)$.又由于 f 是单射,故对每个 x,只有惟一的 y 使得 $f(y)=x$,故 f^{-1} 可被上述具有惟一计算路径的不确定图灵机在多项式时间内计算,故 $f^{-1}\in UPSV$.再证 $f^{-1}\notin PF/\text{poly}$,反设 $f^{-1}\in PF/\text{poly}$,由引理 1 知,存在稀疏集 S,使 f^{-1} 借助于 S 相对多项式时间可计算,与前提矛盾,故 $f^{-1}\notin PF/\text{poly}$,故(2)⇒(3)成立.

(3)⇒(1)

设 $f\in UPSV\text{-}PF/\text{poly}$.反设 $UP\text{-}P/\text{poly}=\varnothing$,则可以证明 $f\in PF/\text{poly}$,这与前提矛盾.

证明如下:

令 $S=\{\langle x,y\rangle\mid y$ 为 $f(x)$的前段$\}$,这里假设一个字符串本身也是该字符串的前段.

下面证 $S\in UP$,因为 $f\in UPSV$,故可模仿计算 f 的具有惟一计算路径的多项式时间不确定图灵机计算 x,然后比较,若 y 是 $f(x)$的前段,则接受$\langle x,y\rangle$.不难看出,可构造确定图灵机在多项式时间内比较 y 是否 $f(x)$的前段,故 $S\in UP$.由假设 $UP\text{-}P/\text{poly}=\varnothing$可知,$S\in P/\text{poly}$.从而存在 $h\in\text{poly}$,使$\langle x,y\rangle\in S\leftrightarrow\langle\langle x,y\rangle,h(|\langle x,y\rangle|)\rangle\in A$,$A\in P$.

下面证明 $f\in PF/\text{poly}$.

构造算法如下:

输入 x;

$z:=\lambda$;(λ 是空字符串)

循环:若$\langle\langle x,z0\rangle,h(|\langle x,z0\rangle|)\rangle\in A$,则 $z:=z0$(注:这里 $z0$ 表示字 z 与字 0 的连接);

否则,若$\langle\langle x,z1\rangle,h(|\langle x,z1\rangle|)\rangle\in A$,则 $z:=z1$;

否则,跳出循环;

若 $z\neq\lambda$,输出 z.

该程序对任何输入都会终止,因为若程序对某输入 x 不终止,则必定是程序中循环不结束,而

这意味着对于输入 x 的函数值 $f(x)$ 有任意长的前串,但任一字符串长度有限,故这是不可能的,因此该程序对任何输入都会终止.当程序结束时,若输出 z,必有 $f(x)=z$;否则,$f(x)$ 无定义.因为若输出 z,由上述算法可知,对任一字符串 y,y 是 $f(x)$ 的前段当且仅当 y 是 z 的前段,故 $f(x)=z$.反之,若 $f(x)$ 有定义,由 S 的构造可知,对任意 $n\leqslant|f(x)|$,必有长度为 n 的 $f(x)$ 的前段 y,使 $\langle x,y\rangle\in S$,而 $|f(x)|>0$,由上述算法可知,程序终止时,$z\neq\lambda$,从而 z 为输出.

显然,借助于 h,上述算法为确定多项式时间可计算的,故 $f\in PF/\text{poly}$.与前提矛盾,故 $UP-P/\text{poly}\neq\varnothing$,(3)⇒(1)成立.

综上可知,3 个命题等价.

定理 2. 以下命题等价:

(1) $UP/\text{poly}-P/\text{poly}\neq\varnothing$;

(2) 存在弱相对化 one-way 函数;

(3) $UPSV/\text{poly}-PF/\text{poly}\neq\varnothing$.

证明:类似定理 1,证明细节略.

引理 2. $(P/\text{poly})/\text{poly}=P/\text{poly}$.

证明:构造 F,使得对任意 n,$F(0^n)=0$(这里,0^n 是指由 n 个 0 组成的字符串).显然,$F\in\text{poly}$,故 $(P/\text{poly})/\{F\}\subseteq(P/\text{poly})/\text{poly}$.设 $A\in P/\text{poly}$,则存在 $f\in\text{poly}$,$B\in P$,使 $A=\{x|\langle x,f(|x|)\rangle\in B\}$.又显然可构造 $C\in P$,使 $A=\{x|\langle\langle x,f(|x|)\rangle,0\rangle\in C\}$,故 $A\in(P/\text{poly})/\{F\}$,故 $P/\text{poly}\subseteq(P/\text{poly})/\{F\}$,即 $P/\text{poly}\subseteq(P/\text{poly})/\text{poly}$.又设 $A\in(P/\text{poly})/\text{poly}$,则∃ $f,g\in\text{poly}$,∃ $B\in P$,使 $A=\{x\ \langle\langle x,f(|x|)\rangle,g(|x|)\rangle\in B\}$,令 $h(|x|)=\langle f(|x|),g(|x|)\rangle$,显然,$h\in\text{poly}$,且存在 $D\in P$,使 $A=\{x|\langle x,h(|x|)\rangle\in D\}$,故 $A\in P/\text{poly}$,故 $(P/\text{poly})/\text{poly}\subseteq P/\text{poly}$.综上所述,$(P/\text{poly})/\text{poly}=P/\text{poly}$.

定理 3. $UP/\text{poly}-P/\text{poly}\neq\varnothing\Leftrightarrow UP-P/\text{poly}\neq\varnothing$.

证明:⇒:反设 $UP-P/\text{poly}=\varnothing$.任取 $A\in UP/\text{poly}$,则有 $f\in\text{poly}$ 及 $B\in UP$,使得 $x\in A\Leftrightarrow\langle x,f(|x|)\rangle\in B$,因为 $UP-P/\text{poly}=\varnothing$,故 $B\in P/\text{poly}$,从而 $A\in(P/\text{poly})/\text{poly}$.据引理 2 得,$A\in P/\text{poly}$,从而 $UP/\text{poly}-P/\text{poly}=\varnothing$,矛盾,故假设不成立.

⇐:设 $A\in UP-P/\text{poly}$,构造 F,使得对任意 n,$F(0^n)=0$.显然,$F\in\text{poly}$.又如下可证 $B=\{\langle x,0\rangle|x\in A\}$ 属于 UP:因为当输入 w 后可先检查 w 的表示 $\langle x,0\rangle$,并分离出 x,然后,以 x 为输入模仿接受 A 的具有至多一条接受路径的不确定图灵机 M 进行计算,若 M 接受,则接受.显然,该图灵机有至多一条接受路径,故 $B\in UP$.又由 B 的构造可知,$x\in A\Leftrightarrow\langle x,F(|x|)\rangle\in B$.由于 $B\in UP$,所以 $A\in UP/\text{poly}$,而由假设:$A\in UP-P/\text{poly}$ 知,$A\notin P/\text{poly}$,故 $A\in UP/\text{poly}-P/\text{poly}$,即 $UP/\text{poly}-P/\text{poly}\neq\varnothing$.

由定理 1~3 可知:

定理 4. 以下命题等价:

(1) $UP-P/\text{poly}\neq\varnothing$;

(2) 存在强相对化 one-way 函数;

(3) $UPSV-PF/\text{poly}\neq\varnothing$;

(4) $UP/\text{poly}-P/\text{poly}\neq\varnothing$;

(5) 存在弱相对化 one-way 函数;

(6) $UPSV/\text{poly}-PF/\text{poly}\neq\varnothing$.

2 结束语

本文定义了强相对化 one-way 函数、弱相对化 one-way 函数,并证明了其存在性与 UP-P/Poly$\neq\varnothing$? 以及 UP/poly-P/poly$\neq\varnothing$? 等一系列开问题的等价性,将 Grollmann 和 Selman 的结果推广到相对化和非一致复杂类的情形.

References:

[1] Grollmann, J., Selman, A. L. Complexity measures for public-key cryptosystems. SIAM Journal on Computing, 1988,17(2):309~335.

[2] Boppana, R. B., Lagarias, J. C. One-Way functions and circuit complexity. In: Selman, A. L., ed. Lecture Notes in Computer Science 223. Berlin: Springer-Verlag, 1986. 51~65.

[3] Homer, S., Wang, J. Absolute results concerning one way functions and their applications. Mathematical Systems Theory, 1989,22(1):21~35.

[4] Lü, Yi-zhong, Gu, Lei. Existence of one-way function in boolean circuit. Computer Research and Development, 1992,29(7):1~5 (in Chinese).

[5] Karp, R. M., Lipton, R. J. Some connections between nonuniform and uniform complexity classes. In: Proceedings of the 12th ACM Symposium on Theory of Computing. New York: ACM Press, 1980. 302~309.

[6] Köbler, J, Watanabe, O. New collapse consequences of NP having small circuits. In: Fülep, Zoltán, eds. Lecture Notes in Computer Science 944. Berlin: Springer-Verlag, 1995. 196~208.

[7] Balcazar, J. L., Diaz, J., Gabarro, J. Structural Complexity I. Berlin: Springer-Verlag, 1988.

[8] Watanabe, O. On one-way functions. In: Du, D., Hu, G., eds. Combinatorics, Computing and Complexity. Boston: Kluwer Academic Publishers and Science Press, 1989. 98~131.

附中文参考文献:

[4] 吕义忠,顾蕾.右尔分层 one-way 函数的存在性.计算机研究与发展,1992,29(7):1~5.

The Existence of Relativization One-Way Functions *

CAO Zi-ning[1], LÜ Yi-zhong[2], SHI Chun-yi[1]

[1](*Department of Computer Science and Technology, Tsinghua University, Beijing* 100084, *China*);

[2](*Department of Computer Science and Engineering, Nanjing Aeronautics & Astronautics University, Nanjing* 210016, *China*)

E-mail: caozn@263.net

Abstract: One-Way functions play an important role in complexity theory of computation and public-key cryptography. Inspired by the work of Grollmann and Selman, the work of Grollmann and Selman to the result of relativization and nonuniform complexity classes are generalized in this paper, the equivalence of the include relation of complexity class UP/poly, UP, P/poly and the existence of strongly relativization one-way function, weakly relativization one-way function are proved.

Key words: computational complexity; one-way function; relativization; nonuniform complexity class

* Received October 13, 1999; accepted March 23, 2000

Supported by the National Natural Science Foundation of China under Grant No. 69875007; the Natural Science Foundation of Jiangsu Province of China under Grant No. BK99119