

关于相对化的计算复杂性类的研究 (摘要)

王 浩 侯广坤

(中山大学计算机科学系)

李 祥

(贵州大学数学系)

设 P^A 及 NP^A 分别表示被多项式时间有界的确定性与非确定性的带 oracle A 的图灵机所接受的语言类, E^A 及 NE^A 分别表示被指数时间有界的确定性与非确定性的带 oracle A 的图灵机所接受的语言类。不失一般性, 设图灵机的带上字母表为 $\{0,1\}$ 。本文所讨论的语言 (集合) 及字分别指 $\{0,1\}^*$ 的子集及元素。本文的证明使用了有穷损害优先方法。

§ 1. 定义

1. 任给 A, B , 若 $P^A \not\subseteq P^B$ (即 $A \not\leq_p B$), 则记为 $A \prec B$; 若 $A \prec B$ 或 $B \prec A$, 则称 A, B 可比较, 否则称为不可比较, 并记为 $A \parallel B$ 。
2. 称 A 为**密度可测**, 如果存在一个可计算函数 d , 使得 (1) 对任意多项式 p , 都可能找到无穷个 n 使 $p(n) < d(n)$; (2) $\forall n \in \omega$ ($\omega = \{0, 1, 2, \dots\}$): $d(n) \leq 2^n$; (3) $\forall n \in \omega: \|A \cap \{\alpha: \alpha \text{ 的长度为 } n\}\| = d(n)$ 。(这里 $\|\cdot\|$ 表示集合的基数)。
3. 称语言 A, B 具有**相同的构型**, 如果 $\forall n: \|A \cap \{\alpha: \alpha \text{ 的长为 } n\}\| = \|B \cap \{\alpha: \alpha \text{ 的长为 } n\}\|$, 记为 $A \simeq B$ 。
4. 一个 NP 集合称为**NP-低单纯的**, 如果它的补集包含无穷的 NP 集但不包含无穷的 P 集。

§ 2. 主要定理

1. 对任意 B 都有 A 使 $P^A = NP^B$ 当且仅当 NP^B 关于补运算封闭。

推论1 存在递归语言 A 使 $P^A = NP$ 当且仅当 $NP = co-NP$ 。

从而就把 $NP = ? co-NP$ 这个有名的尚未解决的问题与相对化联系起来。

2. ($\forall A \in NP$) [$NP^A = NP \iff NP = co-NP$].

下面的定理3、4、5、6、7是我们得到的关于多项式度的若干主要结果:

3. 对任意 A , 存在 B 使 $A \prec B$ 。若 A 递归, 则 B 亦递归。
4. 任给无穷语言 A , 可找到递归语言 B 使 $B \not\subseteq A$ 且 $P^B \not\subseteq P^A$ 。
5. 对任意 $A \neq \phi$, 都可找到 B, C 使 $C \in NP^A$, $C \neq \phi$, $C \not\subseteq B$ 且 $P^C \subseteq P^B$ 。若 A 是递归的, 则 B, C 亦递归。(ϕ 表示空集)。

本文1985年2月收到

6. 存在递归语言 A 及 B 使 $A \not\subseteq B$, 而 $A < B$.

7. 设语言 A 密度可测, 则 A 存在两个非空的不相交的子集 B 和 C 使 $B \perp C$ 且 $B \subseteq C$.

1983年, Homer 和 Maass 在 $P \neq NP$ 的假设下定义了 NP -单纯集, 讨论了 NP 集格的性质. 我们则定义了 NP -低单纯集 (定义 4).

8. 存在 oracle A 使 NP^A -低单纯集存在.

1982年, Book 等人证明存在 oracle A 使 $P^A \neq NP^A$ 但 $E^A = NE^A$, 从而 NE^A 关于补运算封闭. 我们则证明了

9. 存在 oracle B 使 NE^B 关于补运算不封闭.

10. 存在 A 使 $P^A \neq NP^A, E^A \neq NE^A$ 且 $(\forall k \in \omega) [NP^A \not\subseteq T^A(2^{n^k})]$. (有关 $T^A(\lambda n[f(n)])$ 的意义可见 [3]).

11. 对任意 B , 存在 A 使得有无穷语言 $C \in NP^A$ 满足 $(\forall C' \subseteq C) [C' \text{ 无穷} \Rightarrow C' \notin E^B]$.

12. 对任意 B , 存在 A 使得有无穷语言 $C \in NP^A$ 满足 $(\forall C' \subseteq C) [C' \text{ 无穷} \Rightarrow C' \notin NE^B]$.

注 1. 本文完成于 1984 年 6 月. 脱稿后曾得到国内外许多著名专家的注意.

2. 本文定理 1 及推论 1 的证明将在《科学通报》1985 年第 7 期发表.

主要参考文献

- [1] T. Baker, J. Gill, R. Solovay, *SIAM J. Comput.*, 4(1975) 431—442.
 [2] S. Homer, W. Maass, *Theoret. Comput. Sci.*, 3 (1983), 279—290
 [3] S. Moran, *SIAM J. Comput.*, 2 (1982), 344—349.
 [4] R. V. Book, C. B. Wilson, M. R. Xu, *SIAM J. Comput.*, 3 (1982), 511—581.

On Relativized Complexity Classes

Wang Jie Hou Guangkun Li Xiang

Abstract

We give a necessary and sufficient condition for an NP^B to be equal to a P^A . From this we show that there is an oracle A such that $P^A = NP^A$ if and only if $NP = co-NP$. We then define an order relation on 2^{ω} which describes the properly including relation among the relativized P classes, and we study the structure of the family of the relativized P classes under this order relation. For example, we show that there is a sequence of comparable recursive languages, and a density measurable set A has two disjoint nonempty subsets B and C such that B and C are incomparable and of the same form. Under the assumption $P \neq NP$, Homer and Maass⁽²⁾ defined an PN -simple set and proved that there is an oracle relative to which an NP -simple set exists. We then define an NP -lowersimple set and proved that there is an oracle relative to which an NP -lowersimple set exists. The construction of the oracle is finite injury priority arguments. By the construction of B in Theorem 4.1 in [2], we show that no NP^B -lowersimple sets exist. Finally, we discuss some properties between the relativized polynomial-time classes and the relativized exponential-time classes.