arXiv:2305.02226v1 [cs.CC] 1 Apr 2023

$P \neq NP$相对于一个 P-完全预言机

Reiner Czerwinski 柏林工业大学（校友）
reiner.czerwinski@posteo.de

2023年5月4日

摘要

P 与 NP 问题仍未得到解决。然而，存在若干预言机，使得相对于这些预言机，P 不等于 NP。

这里我们将证明，相对于 P 完全预言机，P ≠NP。

在本文中，我们采用填充论证作为证明方法。填充论证不受任何可计算函数的限制。例如，我们可以利用可计算性理论中的方法来分离复杂性类。

1 引言

对于某些预言机，相对 P 与 NP 问题已经得到了解决。Baker、Gill 和 Solovay[1] 构造了一个预言机 A，使得$\mathbf{P}^A \neq \mathbf{NP}^A$，以及另一个预言机 B，使得$\mathbf{P}^B = \mathbf{NP}^B$。相对于随机预言机，$\mathbf{P}$ 不等于$\mathbf{NP}$[3]。在本文中，我们分析相对于 P 完全预言机的 P 与 NP 问题，即研究$\mathbf{P}^{\mathbf{P}} = \mathbf{NP}^{\mathbf{P}}$ 是否成立。

作为预言机，我们使用集合

$$U_{\mathbf{P}} = \{\langle M, x, 1^t\rangle \mid \text{ TM } M \text{ accepts } x \text{ within } t \text{ steps}\}$$

为了证明 $\mathrm{NP}^{U_{\mathrm{P}}} \neq \mathrm{P}^{U_{\mathrm{P}}}$，我们使用一个 NP 完全集

$$U_{\mathbf{NP}} = \{\langle M, 1^n, 1^t\rangle \mid \exists x \in \{0,1\}^n \text{其中，图灵机 } M \text{ 在 } t \text{ 步内接受 } x\}$$

在第2 节中，我们将分析没有时间限制的集合。在这种情况下，我们可以使用可计算性理论中的方法。

在第3 节中，我们将证明第2 节中的集合与集合 $U_{\mathbf{NP}}$ 和 $U_{\mathbf{P}}$之间的联系。因此，我们可以得出结论非确定性多项式时间$^{U_{\mathrm{P}}}$。

2 无时间限制的计算

为了分析 $U^{U_{\mathbf{P}}}$非确定性多项式时间是否能够被高效计算，我们定义两个与 $U_{\mathbf{NP}}$ 和 $U_{\mathbf{P}}$ 类似、但不受时间限制的集合。

$$D_{\mathbf{P}} = \{\langle M, x\rangle \mid \text{TM } M \text{ accepts } x\}$$
$$D_{\mathbf{NP}} = \{\{\langle M, 1^n\rangle \mid \exists x \in \{0,1\}^n \text{ where TM } M \text{ accepts } x\}$$

因此，$\langle M, x\rangle \in D_{\mathbf{P}}$，若 $x \in L(M)$；而 $\langle M, 1^n\rangle \in D_{\mathbf{NP}}$，若 $\exists x \in \{0,1\}^n$ with$x \in L(M)$。

显然，

- $\langle M, x\rangle \in D_{\text{确定性多项式时间}}$ 当且仅当 $\exists t$：$\langle M, x, 1^t\rangle \in U_{\text{确定性多项式时间}}$
- $\langle M,\ 1^n\rangle \in D_{\text{非确定性多项式时间}}$ 当且仅当 $\exists t$：$\langle M,\ 1^n,\ 1^t\rangle \in U_{\text{非确定性多项式时间}}$

引理 1. 若 $\langle M, \{0,1\}^n\rangle \in D_{\mathbf{NP}}$，则无法判定 $x \in \{0,1\}^n$ 是否属于 $L(M)$。

证明。 设 M 为任意一台图灵机。根据 Rice 定理，[4] 语言 $L(M)$ 的每个非平凡性质都是不可判定的。设 $x \in \{0,1\}^n$ 为任意但固定的值。判断 $x \in L(M)$ 是不可判定的。此外，如果 x 是 $(\{0,1\}^n \cap L(M))$中的唯一元素，那么判断这一点也是不可判定的，因为这是$L(M)$ 的一个非平凡性质。因此，判断长度为 n的哪个元素属于 $L(M)$ 是不可判定的。 □

推论 1。设 M 为任意一台图灵机，且 $n \in \mathbb{N}$。要测试$\langle M$是否成立，$1^n\rangle \in D_{\mathbf{NP}}$ 最坏情况下需要访问预言机 $D_{\mathbf{P}}$ $\theta(2^n)$ 次。

证明。 根据引理 1，对于任意一台图灵机 M，判断长度为 x 的输入 n 是否属于 $L(M)$ 是不可判定的。但 $L(M)$ 的特征函数为：

$$\chi_{L(M)}(x) = \begin{cases} 1 & x \in L(M) \\ 0 & \text{otherwise} \end{cases}$$

可将预言机 $D_{\mathbf{P}}$ 作为黑箱来计算。因此，黑箱复杂度是指数级的。

□

3 主要结果

在本节中，我们从带有预言机 $D_{\mathbf{P}}$ 的 $D_{\mathbf{NP}}$ 得出带有预言机$U_{\mathbf{P}}$的 $U_{\mathbf{NP}}$ 。

定理 1. 如果 M 是任意图灵机，那么在最坏情况下，需要访问预言机 $U_{\mathbf{P}}$ $\theta(2^n)$ 次，才能决定 $\langle M、\ 1^n、\ 1^t\rangle \in U_{\mathbf{NP}}$。

证明。令 M 为任意一台图灵机，且 $n \in \mathbb{N}$。集合 $\{0,1\}^n$ 是有限的。因此，存在一个 $T \in \mathbb{N}$，使得

$$\langle M, 1^n, 1^T\rangle \in U_{\mathbf{NP}} \iff \langle M, 1^n\rangle \in D_{\mathbf{NP}}$$

在这种情况下，我们知道，对于 $x \in \{0,1\}^n$: $\langle M,\ 1^n,\ 1^T\rangle \in U_{\mathbf{P}}$ 当且仅当 $\langle M,\ x\rangle \in D_{\mathbf{P}}$。因此，使用预言机 $U_{\mathbf{P}}$ 计算 UNP的时间复杂度，与使用预言机 $D_{\mathbf{P}}$计算 DNP 的时间复杂度相同。根据引理 1，这是 $\theta(2^n)$。

也许有人会认为，当时间限制较短时，存在比黑箱搜索更快的计算方法。假设对于 $\langle M、\ 1^n、\ 1^t\rangle \in^? U_{\mathbf{NP}}$，存在一种更快的计算方法，当

$$\exists x \in \{0,1\}^n \text{ with } \langle M, x, 1^t\rangle \in U_{\mathbf{P}} \text{ but } x \in L(M). \tag{1}$$

那么就可以判定 M 是否在超过 t 步内接受一个 x。但事实并非如此。 □

4 结论

也许 $\mathrm{P}^{\mathbf{P}} = \mathrm{P}$ 且 $\mathrm{NP}^{\mathbf{P}} = \mathrm{NP}$。在这种情况下，结果将解决 P 与 NP 问题。但正如 Oded Goldreich 在其网页[2]上所提到的，解决 P 与 NP 问题需要新的洞见。本文中是否有新的洞见？一位匿名人士告诉我：“专家们一致认为，不能用可计算性技巧解决 P 与 NP 这类问题。”因此，这是一个新颖的洞见。

参考文献

[1] Theodore Baker、John Gill 和 Robert Solovay。《相对化的确定性多项式时间=？非确定性多项式时间问题。《SIAM 计算杂志》，4(4):431–442，1975。[2]O. Goldreich。论确定性多项式时间与非确定性多项式时间问题的解决。https://www.wisdom.weizmann.ac.il/~oded/p-vs-np.html。访问日期：2023-02-09。[3] Johan H˚astad、Benjamin Rossman、Rocco A. Servedio 和 Li-Yang Tan。布尔电路的平均情形深度层级定理。《美国计算机协会会刊》（JACM），64:1–27，2017。

[4]H. G. Rice。递归可枚举集的类别及其判定问题。《美国数学会汇刊》，74(2):358–366，1953年。