无需相对化的对角化 n

深入探讨贝克-吉尔-索洛维定理

Baruch Garcia*

2026年1月15日

arXiv:2601.09702v1 [cs.CC] 14 Jan 2026

摘要

我们已经知道，若干问题会相对化，例如 P类与 EXP 不等价，以及接受问题和停机问题的不可判定性。然而，相对化是一种有限的工具，无法分离其他复杂性类。尚未得到明确证明的是，接受问题的图灵可识别性是否会相对化。我们将考察一个使 R 类与递归可枚举等价的预言机； $R^A = RE^A$，其中 A 是复杂性类 ALL 中等价性问题的预言机，但不属于递归可枚举，也不属于 co-RE。随后，我们将区分相对化与我们所称的“半相对化”，即仅使用接受问题预言机来分离复杂性类。我们认为，R 类与递归可枚举的分离是只有“半相对化”才能证明的事实。接着，我们将 R 类和递归可枚举的多项式时间对应版本“缩小范围”，通过“半相对化”对角化避开贝克-吉尔-索洛维障碍，同时指出对角化与相对化之间这一微妙区别。随后，这个“多项式时间接受问题”可归约到电路可满足性问题和 3-CNF 可满足性问题，从而证明这些问题在多项式时间内不可判定，却能在多项式时间内验证。“半相对化”不使用算术化来避开相对化障碍，因此也能避开 Aaronson 和 Wigderson 提出的代数化障碍。最后，由于半相对化是一种非构造性技术，它避开了 Razborov 和 Rudich 提出的自然证明障碍。因此，R 类与递归可枚举的分离，以及 P类与 NP类的分离，都不相对化，却都能“半相对化”，从而避开全部三种障碍。

目录

1 序言 2 2 背景 3 3 回归基础：从复杂性到可计算性 4 4 相对化与“半相对化” 5 5 将问题“缩小”到多项式时间问题 7 6 讨论 9 7 致谢 10

*baruchgarcia@utexas.edu

1 序言

真理会使人消瘦，却不会使人折腰...[1]- 《堂吉诃德》，米格尔·德·塞万提斯

为了清楚地理解计算复杂性的基础，我们将考察 Stephen Cook 在 20 世纪 70 年代初讨论的可计算性基础[11]:

> 我读研究生时的导师、哈佛大学的王浩对逻辑和递归论很感兴趣，而促使我产生这个想法的，正是可计算函数理论。该理论涉及所谓的递归可枚举集，因此也存在同样的现象。递归可枚举完全集都等价于最难的递归可枚举集。当然，区别在于这些集合不可判定，根本不存在能够解决它们的算法，但这正是两者的类比所在。当然，NP 完全集有所不同。它们是可计算的，只是无法有效地计算[.....]解决这些问题大概需要指数级的时间，但这种类比仍然成立。这就是我产生这个想法的原因。

Wigderson[38] 进一步阐述了这种类比:

> 关于**P** 类与**NP** 类的问题，一个非常吸引人的特点是（这也是早期人们乐观地认为它可能很快得到解决的原因），它可以自然地看作可计算性理论中可判定性问题的一个有界类比[.....] 要理解这一点，可以将两个类中的多项式时间界都替换为有限界。对于**P**类，类比所得的就是所有具有有限算法的问题，也就是可判定问题，有时称为递归问题，记作**R** 类。对于**NP**类，类比所得的是这样一类性质：其成员资格可以通过有限算法和有限见证来验证。这个类称为递归可枚举类，或**RE**。

我们将讨论有限验证，或等价地说递归可枚举性、可计算可枚举性、半可判定性或图灵可识别性。以停机问题为例；尽管不存在针对停机问题的广义算法，但如果它确实停机，就可以在有限时间内得到验证 t。我们将把这一类称为:

$$\mathbf{RE}$$

其多项式时间对应版本总是被称为“非确定性多项式时间”，或:

$$\mathbf{NP}$$

我们还将使用有限余验证这一术语，等价地称为余递归可枚举性、余可计算可枚举性、余半可判定性或余图灵可识别性。以停机问题的补集为例；尽管不存在针对停机问题补集的广义算法（“图灵机永不停机吗？”），但其补集是可验证的，即如果它停机，就可以在有限时间内得到验证 t。我们将把这一类称为:

$$co-\mathbf{RE}$$

其补集的多项式时间对应版本是:

$$co-\mathbf{NP}$$

我们也会讨论递归，或者等价地，可判定性，或者等价地，可计算性 或算法的。我们将这个类称为:

$$\mathbf{R}$$

不属于此类的问题称为非递归或不可判定或不可计算[2]，也可以说不存在广义算法。其多项式时间对应版本称为“多项式时间”或

$$\mathbf{P}$$

[1]”真理或许会被拉得很薄，却不会断裂[...]” [2]”可判定”可能指二值判定，而”可计算”或”可解”可能指多值解，这种解可以由多个二元”判定”构成。

此类包含所有能够通过广义算法在可行（即多项式）时间内判定（或求解）的问题。本文将大量采用 Sipser 的《计算理论导论》（第 3 版）中的符号，但有两处显著不同：我们用**RE** 表示“图灵可识别性”，用**R** 表示“可判定性”。

2 背景

G¨odel 致冯·诺依曼的信[15][3] 提出了一个问题，后来人们将其称为“**P** 与 **NP**”问题。能够在多项式时间（即“可行”时间）内验证的问题，是否也能在多项式时间内求解（判定）？ Sipser[31], Cook[10] 和 Aaronson[3]的综述介绍了这一问题。Sipser[32],Wigderson[38], Arora 和 Barak[7],以及 Aaronson[2] 所著的教材也对这一问题有所阐述。

需要指出的是，如果 P $\neq$ NP，Ladner 定理[21] 告诉我们，一定会存在一个中间类，即 NP $-$ $intermediate$ 中必然存在这样的类。尽管像图同构、整数分解和离散对数这类自然问题可能会[4] 归入 P 类或 NP 类 $-$ $complete$，但 NP 类 $-$ $intermediate$ 将永远存在，就像递归可枚举类 RE $-$ $intermediate$ 一样；而 RE 类中并没有自然问题[27][20][13][23][2]。如果 P $\neq$ NP，那么那些始终无法在可行时间内判定的问题称为“NP $-$ $complete$”。 $3-CNF-SAT$——也简称为 $3SAT$或 SAT——是一个典型问题[5]，我们可从该问题出发进行多项式时间归约，以证明其他一些知名问题也属于 NP 类 $CLIQUE$和 $SUDOKU$。然而，如果 P 等于 NP，那么 P、NP$-intermediate$和 NP $-$ $complete$ 问题将合并为同一个类。P 与 NP 不等价这一点似乎有许多显而易见的理由。例如，NP $-$ $intermediate$ 问题数不胜数，但至今尚未发现任何一个问题具有多项式时间判定算法。第二个理由是，尽管某些 NP $-$ $intermediate$ 问题存在量子多项式时间（BQP）算法[4]，例如用于因数分解的 Shor 算法[30]，但 Bennett、Bernstein、Brassard 和 Vazirani[9] 曾著名地证明，我们无法对 NP $-$ $complete$ 问题实现指数级加速。在最理想的情况下，我们只能获得二次（多项式）加速，Grover[17]对此作出了著名展示。因此，我们不仅会预期在经典计算机上 P $\neq$ NP，在量子计算机上也是如此[1]。第三，假设所有可行验证的问题也都能在可行时间内求解，这有悖于“常识”——不管这个说法究竟有多少分量。讨论 P 与 NP 可能等价的唯一好处，似乎就是促使人们证明二者并不等价。

遗憾的是，出现了三大障碍，使得使用证明 **P** $\neq$ **EXP**、**IP** $=$ **PSPACE** 和 $PARITY \notin \mathbf{AC}^0$ 等其他结果时所采用的已知技术，难以处理区分 **P** 和 **NP** 这一问题。Baker、Gill 和 Solovay（BGS）[8]，提出了一种论证，说明某些结果成立，例如停机问题的不可判定性，或者重要结果[18]：无论选择哪一个预言机，**P** $\neq$ **EXP**。这些结果是“相对化的”。而另一些结果则不相对化。例如，可以选择两个预言机，使 **P** 和**NP** 之间的关系得到不同的结果。可以选择一个预言机 B，得到预期结果，即**P** 和**NP** 并不等价：

$$\mathbf{P}^B \neq \mathbf{NP}^B$$

然而，正如 BGS 所展示的，也可以选择一个预言机 A，它是一个**EXP** （或 **PSPACE**）预言机，在这种情况下，可以证明**P**和**NP**之间出人意料的等价性。

$$\mathbf{P}^A = \mathbf{NP}^A$$

任何使用“相对化”的技术都无法分离这些复杂性类。后来，人们证明某些有效结果并不能相对化。例如，Shamir[29] 研究交互式证明时，证明了 $IP = PSPACE$；这一结果通过一种称为“算术化”的过程绕过了相对化障碍。算术化是一种

[3]John Nash 发现了一个关于**NP** $-$ $intermediate$ 类问题[3]不可行性的部分版本。[4].....随着 Agrawal、Kayal和Saxena算法的出现，素性问题从**NP** $-$ $intermediate$ 类问题转变为**P**类问题[6][5]一个**NP** $-$ $complete$ 类问题的例子是 $3-CNF-SAT$，它询问下面的陈述是否可满足：

$$(x_1 \vee \neg x_2 \vee x_3) \wedge (\neg x_1 \vee x_3 \vee \neg x_4) \wedge (x_2 \vee \neg x_3 \vee x_4)$$

将布尔函数转换为多项式[6] 并基于以下规则[7]的技术：

$$x \wedge y \equiv xy \qquad x \vee y \equiv x + y - xy \qquad \neg x \equiv 1 - x$$

Baker、Gill 和 Solovay 的较简单预言机无法捕捉这种代数结构。遗憾的是，Aaronson 和 Wigderson[5] 表明，使用算术化的这类技术无法分离**P** 和**NP**类，因为可以构造一个~“代数预言机” A，以捕捉更微妙的代数结构，并证明：

$$\mathbf{P}^{\widetilde{A}} = \mathbf{NP}^{\widetilde{A}}$$

最后，我们可以尝试放弃“全局”搜索，转而进行“局部”搜索，将论证限制在位级。更具体地说，我们可以放弃对角化论证等非构造性证明，转而采用依赖电路复杂性论证的构造性证明；这类论证已成功证明了诸如 $PARITY \notin \mathbf{AC}^0$[14] 这样的结果。然而，Razborov 和 Rudich 指出，沿着这条路走会遇到一道“自我挫败”的**第**三重障碍，称为“自然证明”障碍。Aaronson 解释道[3]:

> 正如 Razborov 和 Rudich 本人强调的那样，我们要汲取的教训并不是应该放弃证明**P** $\neq$ **NP**类。事实上，自复杂性理论诞生以来，我们至少有一种能够轻易避开自然证明障碍的技术：也就是对角化 [....] 当然，对角化也受到相对化障碍的限制 [....] 因此，如何同时避开相对化和自然证明障碍这一问题仍然悬而未决 [....]

我们需要的是一种能够避开全部三道障碍的证明，就像 Williams 的结果 NEXP $\not\subset$ ACC^0[39] 一样。“元复杂性”研究计划也旨在避开自然证明障碍[19]。

我们在 P类与 NP类问题，甚至它们所面临的障碍中，看到了共同的自指脉络，而 Ketan Mulmuley 的几何复杂性理论（GCT）研究计划[24] 一直试图打破这一脉络。不过，据说这项研究计划需要 100 年才能实现[12], ，所以我们不妨花些时间，深入回顾 Baker、Gill 和 Solovay 确立的最简单障碍——相对化[8]。

3 回归基础：从复杂性到可计算性

让我们来定义算法和图灵机。Wigderson[38]解释道：

> 图灵将算法（也称为判定过程）定义为一种图灵机（用现代术语来说，就是一个计算机程序），它会在有限时间内对每个输入停机。

图灵机在形式上定义为[32]一个七元组：

$$(Q, \Sigma, \Gamma, \delta, q_0, q_{acc}, q_{rej})$$

- Q 是状态集合。
- Σ 是输入字母表，不包含空白符号。 $\textvisiblespace$
- Γ 是纸带字母表，包含空白符号。 $\textvisiblespace$
- δ: $Q \times \Gamma \times \{L, R\}$ 是转移函数，用于将读写头向左 L 或向右 R移动。
- $q_0 \in Q$ 是初始状态。
- $q_{acc} \in Q$是图灵机**停机**并**接受**时的状态。
- $q_{rej} \in Q$ 是图灵机**停机**并**拒绝**时的状态。

[6]布尔语句算术化的一个示例如下

$$(x \wedge y)\neg x \implies xy - x^2y$$

[7].....正如人们在概率论中所遇到的那样。

从历史上看，图灵发现的停机问题的不可判定性[37]——继 G¨odel 证明皮亚诺算术中存在不可判定命题之后[16]——始终是可计算性理论的基石和黄金标准。然而，Sipser[32]正确地指出，接受问题（他将其记为 A_{TM} ）是更一般的情形，可以从中归约得到停机问题不可判定性的证明。接受问题定义如下：

$$A_{TM} = \{\langle M, w\rangle | \ M \text{ is a } TM \text{ and } M \text{ accepts } w\}.$$

你看，停机问题预设图灵机甚至有永不停止的选项，这与其停止的设计相矛盾。图灵从G¨odel在1931年的发现中得知，并非所有图灵机都会停止。不过，与其从G¨odel的发现出发，不如从接受问题不可判定性的证明入手，Sipser便是这样做的。

	$\ulcorner M_1 \urcorner$	$\ulcorner M_2 \urcorner$	$\ulcorner M_3 \urcorner$	$\ldots$	$\ulcorner D \urcorner$
M_1	接受	接受	拒绝	$\cdots$	拒绝
M_2	拒绝	拒绝	接受	$\cdots$	接受
M_3	接受	拒绝	拒绝	...	拒绝
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\ldots$
D	拒绝	接受	接受	$\cdots$	?

图1：接受问题的对角化。既然我们从右下角的单元格得知，并非所有图灵机都会停机，那么我们就可以提出图灵的问题：是否存在一种广义算法，能够判定一台图灵机是否停机或永不停机。正如图灵所证明的那样，这样的算法并不存在。

那么，接受问题告诉我们什么关于**R** 类和**RE**类的分离呢？它告诉我们，存在一个不可判定的问题，因此它不属于**R**类，但这个问题可以在有限时间内得到验证，因此属于**RE**类。在有限时间内验证是什么意思？这意味着，尽管不存在解决接受问题的广义算法，但如果声称某台图灵机接受了输入，那么根据定义，它必定会在有限时间内停机，因此可以验证[8]。

根据接受问题的不可判定性，我们可以确立复杂性类**RE**。我们还可以考虑**预言机**图灵机。例如，一个用于接受问题的预言机图灵机（Sipser 将其记作 $T^{A_{TM}}$ ）可以从“外部”为接受问题提供一种广义算法，从而避开自指，只需为图1中的右下角单元格选择“接受”或“拒绝”。然而，将预言机应用于其自身时，仍会遇到原始接受问题同样的不可判定性。这样一来，无论选择哪种预言机，接受问题始终都在**R**类之外——我们称接受问题的不可判定性相对化[9]。

4 相对化与“半相对化”

我们从 Baker、Gill 和 Solovay[8][22]得知，我们可以构造一个**EXP** （指数时间[10]）预言机 A ，使得：

$$\mathbf{P}^A = \mathbf{NP}^A$$

所以我们知道，任何关于**P** $\neq$ **NP** 的证明都无法相对化。现在我们来看看**R** 和**RE**的预言机 A 类比。首先，我们来证明**R** 和**RE** 确实彼此不同。我们从接受问题和停机问题的不可判定性得知，存在一个属于**RE**但不属于**R**的问题，从而将这两个类区分开来。接受问题的补集（Sipser 称之为 A_{TM}）属于**RE**的补集，即“$co-$**RE**”。现在有一个严格包含上述语言、实际上包含所有语言的类，称为

[8]请注意，接受问题的补集 A_{TM} 与递归可枚举的拒绝问题 $REJECT_{TM}$并不相同，因为接受问题的补集表示拒绝或永不停止（无限循环）。[9].....停机问题的不可判定性也同样如此，论证方法相同。[10]请注意，正如**R** $\neq$ **ALL** 相对化一样，**P** $\neq$ **EXP** 也会相对化。

“ALL”，也称为**“LANG”**。**ALL** 包含“等价性问题”，Sipser[32] 将其称为 EQ_{TM}，并将其归入这个拥有不可数无限多个语言的类。等价性问题 EQ_{TM} 定义如下：

$$EQ_{TM} = \{\langle M_1, M_2\rangle |\ M_1 \text{ and } M_2 \text{ are TMs and } L(M_1) = L(M_2)\}.$$

Sipser[32] 在推论 5.29中指出，只要证明接受问题可归约到问题 B的补集，就能证明 B 不是图灵可识别的（或称“递归可枚举”**RE**）：

$$A_{TM} \leq \overline{B}$$

接着，Sipser用一个简单的策略说明，$E\overline{Q_{TM}}$ 和 EQ_{TM} 都可以从接受问题 A_{TM} 归约而来，从而证明 EQ_{TM} 既不是图灵可识别的，也不是余图灵可识别的；也就是说，EQ_{TM} 既不属于**RE**，也不属于 $co-$ **RE**。为了证明 $EQ_{TM} \notin$ **RE**，Sipser通过以下论证说明 $A_{TM} \leq EQ_{TM}$：

- 选择 M_1，使其对任何输入都拒绝。
- 选择 M_2，使其对任意给定的输入都在 w上运行 M。如果它接受，$accept$。

如果 M 拒绝 w，那么它总是拒绝，并且 M_1 与 M_2 相等。如果 M 接受 w，那么它总是接受，并且 M_1与 M_2 不相等。接下来，只需通过以下论证证明 $EQ_{TM} \notin co-RE$：

- 选择 M_1，使其在任何输入上都接受。
- 选择 M_2，让它在任意给定输入上对 w 运行 M。如果它接受，$accept$。

我们可以从等价性问题出发，以类似于构造接受问题预言机或停机问题预言机的方式，构造一个**等价性问题预言机**。虽然等价性问题预言机能告诉我们等价性问题的答案，但不存在能回答“某个与自身等价的预言机图灵机的等价性问题”的广义算法。现在我们有了一个能解决接受问题的预言机，但它既不是图灵可识别的，也不是图灵余可识别的：

$$T^{EQ_{TM}} \notin \textbf{RE} \quad \text{and} \quad T^{EQ_{TM}} \notin co-\textbf{RE}$$

总结如下问题和预言机：

- **接受问题 (A_{TM})** 是**递归可枚举** $-complete$：对图灵机而言不可判定，但如果图灵机确实接受，则可在有限时间内验证。
- **接受预言机 ($T^{A_{TM}}$)** 是**递归可枚举** $-complete$：对等价的预言机图灵机而言不可判定，但如果预言机确实接受，则可在有限时间内验证。
- **等价性问题 (EQ_{TM})**属于**ALL**：不可判定；既不可验证，也不可共同验证。
- **等价预言机 ($T^{EQ_{TM}}$)**属于**ALL**：可以判定接受问题，但任何等价预言机都是不可判定的；在有限时间内既不可验证，也不可共同验证。

我们可以展示预期结果：

$$\mathbf{R}^B \neq \mathbf{RE}^B$$

其中 B 是**RE**中的一个预言机，例如接受预言机，因此：

$$\mathbf{R}^{A_{TM}} \neq \mathbf{RE}^{A_{TM}}$$

这并不令人意外，也在预料之中。但接下来，我们可以得到本文重点介绍的一个更令人惊讶的结果：

$$\mathbf{R}^A = \mathbf{RE}^A = co - \mathbf{RE}^A$$

其中 A 是一个属于 **ALL** 的预言机，而且我们可以具体使用等价预言机，因此：

$$\mathbf{R}^{EQ_{TM}} = \mathbf{RE}^{EQ_{TM}} = co - \mathbf{RE}^{EQ_{TM}}$$

因为现在接受问题是可判定的，但等价预言机本身是不可判定的，不过在**ALL**中如此。如果等价预言机判定了接受问题或其补集，就无法验证，也无法共同验证预言机本身的状态。因此我们得到：所以，普遍接受的[11] 陈述是：

$$\mathbf{R} \subsetneq \mathbf{RE}$$

只能通过接受预言机来证明，而不能通过一般的相对化来证明，因为后者涵盖所有预言机，包括像等价预言机这样的**ALL** 预言机。仅凭接受问题进行分离，我们称之为“半相对化”。因此， $R \subsetneq RE$ 不具有相对化性质，却具有半相对化性质，这证明了半相对化技术的有效性，也就是说，仅使用接受预言机进行对角化。

5 将问题“缩小”到多项式时间问题

现在我们将定义一个称为“多项式时间接受问题”的问题，它询问一台图灵机（TM）是否在多项式时间内接受，其形式化定义如下：

$$A_{TM-PTIME} = \{\langle M, w\rangle | \ M \text{ is a } TM \text{ and } M \text{ accepts } w \text{ in } \mathcal{O}(n^k) \text{ time}\}.$$

我们可以像图1那样构造一个对角化证明，但这里的选择是：在多项式时间内接受，或在多项式时间内拒绝。图1中的每个 "$ACCEPT$" 单元格都会替换为 "$ACCEPT\ in\ \mathcal{O}(n^k)\ time.$"，而每个 "$REJECT$" 单元格都会替换为 "$REJECT\ in\ \mathcal{O}(n^k)\ time.$"。对角化论证右下角的单元格指示图灵机：当且仅当它在多项式时间内拒绝时，才在多项式时间内接受。虽然不存在能在多项式时间内停机并接受的广义算法，但图灵机可以在**EXP**内停机、接受或拒绝，即 2^{n^k} 时间[12], , 这与穷举搜索相同。不过，一旦图灵机到达 $ACCEPT$ 状态，即 q_{acc}，就可以在多项式时间内验证，因此该问题不属于**P类**，但属于**NP类**。我们还可以定义一个预言机：

$$T^{A_{TM-PTIME}}$$

请注意，尽管这一结果半相对化，以“多项式时间接受预言机” $T^{A_{TM-PTIME}}$为典型例子，但它并不相对化。

半相对化无需借助算术化方法来避开相对化障碍。由于半相对化无需算术化技术就能避开相对化障碍，因此它不会像其他证明中的技术（例如，**IP类** $=$ **PSPACE类**）那样遭遇代数化障碍[13]。所有相对化也

[11]Sipser 在《*Introduction...*》定理 4.11 的配套文字中，用通俗语言指出**R 类** $\subsetneq$ **递归可枚举**：[32],"[.....]识别器比判定器更强。" 原文使用斜体。[12].....或更长。[13]考虑一种熟悉的交互式证明的推广版本，其中有一个强大却不诚实的证明者 $\tilde{P}$和一个有限但持怀疑态度的验证者 V，这以著名的图非同构验证协议[32]为例。将其推广到有限可验证问题，或许能进一步揭示交互式证明的局限性。Boone、Novikov 和 Britton[28][36] 证明了以下结论：

"存在一个有限表示群 B，其字问题不可解（不可判定）。"

我们将研究群的非 -同构问题，即有限表示群的 . 关于这一问题的阐述，参见 Rotman[28] .

我们使用称为 Thue 系统[33]（或局部规范 Post 系统[26]）的规则。确实存在某些初始列表的特定选取，使得不存在用于判定的算法。Tseitin[34][25] 给出的一个具体列表如下：

(1) AC=CA (2) AD=DA (3) BC=CB (4) BD=DB (5) ECA=CE (6) EDB=DE (7) CCA=CCAE

一些关系，例如：

ACCA=ACAC

代数化。所有相对化也都是半相对化。关键的是，存在一些半相对化实例，既不是相对化，也不是代数化。

我们如何将 $A_{TM-PTIME}$与规范的**NP** $-$ $complete$问题联系起来？来看下面的“Cook-Levin计算表”：它将 $A_{TM-PTIME}$归约为一个 $CIRCUIT-SAT$问题，而该问题属于**NP** $-$ $complete$，本身还可归约为 $3-CNF-SAT$[14]

$$A_{TM-PTIME} \leq CIRCUIT-SAT \leq 3-CNF-SAT$$

因此 $A_{TM-PTIME}$，也就是说，判断图灵机 M是否在多项式时间内接受某个输入 w的问题，不可在多项式时间内判定，但可以在多项式时间内验证，因为任何多项式时间验证都可以用 Cook-Levin计算表中的一个实例表示，并以 q_{acc} 结束。

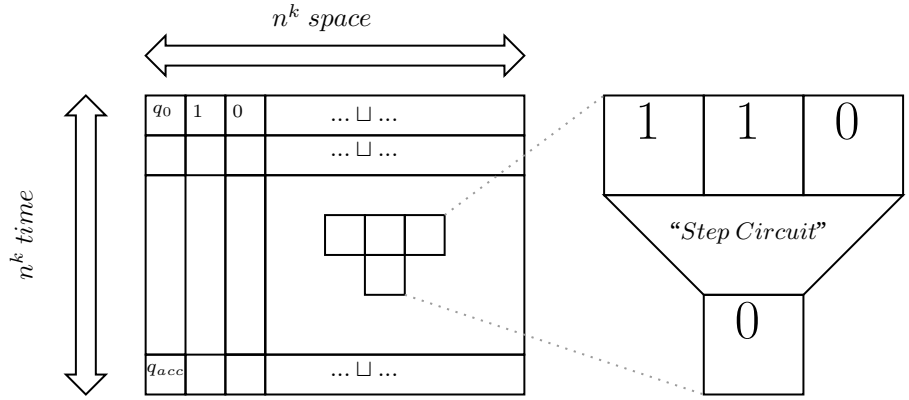


图 2：一个*Cook-Levin*计算表 展示了多项式时间运行的图灵机的内部结构，并表示了其七元组。“步进电路”包含常数个逻辑门——AND、 OR、 NOT——我们用它将图灵机的转移函数 δ： $Q \times \Gamma \times \{L, R\}$ 描述为一个电路，使纸带向左 L或向右 R 移动，也可以保持不动。请注意，步进电路顶部的条目可以包含空白符，而不只是 0 和 1，因此纸带可以向右移出后再向左移回。多项式时间、多项式空间以及规模为常数的步进电路共同保证了逻辑门的数量为多项式级。 $CIRCUIT-SAT$不要与 $CIRCUIT-VALUE$ 问题混淆：该问题读取输入，并在多项式时间内接受 或拒绝，从而将 $CIRCUIT-VALUE$置于**P**中；P类是**R**的多项式时间对应版本。 $A_{TM-PTIME}$可通过 Cook-Levin计算表归约为 $CIRCUIT-SAT$，而 Cook-Levin计算表本身又可通过 Tseitin变换归约为 $3-CNF-SAT$。

有些结论只需使用一次 (1) 就能轻松证明，但另一些则没那么明显。如果 $\widetilde{P}$声称两个单词同构，那么很容易在有限步内向 V展示验证过程以及所用的规则。然而，如果 $\widetilde{P}$声称这两个单词同构，却无法在有限步内向 V展示验证过程，那么 V就不会信服。或者，如果 $\widetilde{P}$声称这两个单词不同构，乍看之下， V似乎不可能在有限时间内验证这一说法, 因为该问题可从 $HALT_{TM}$ 和 A_{TM} 归约而来。因此， V可以选择进行交互式证明： V可以掷硬币，秘密地选择其中一个单词，然后按照给定规则对其进行变换。接着， V询问 $\widetilde{P}$最初选择的是哪个单词。如果这两个单词同构，那么 $\widetilde{P}$每次都猜对的概率极小——为 $Prob = 2^{-N}$，其中 N是掷硬币的次数。如果 $\widetilde{P}$每次都回答正确，那么 V就能以渐近趋近于 1 的概率验证这两个单词不同构：

$$Prob = 1 - (\frac{1}{2})^N$$

[14]Tseiti n[35] 变换是一种从 $CIRCUIT-SAT$到 $3-CNF-SAT$的简单归约。只需用 NAN构建电路 D 门，其中 v_1 并将 v_2 作为输入、将 v_3 作为输出。这样就对应于 CNF子句 $(v_1 \vee v_3) \wedge (v_2 \vee v_3) \wedge (\neg v_1 \vee \neg v_2 \vee \neg v_3$).

6 讨论

我们运用“半相对化”对角化的方法——可以想象到的最简单的对角化形式——证明了**P** $\subsetneq$ **NP**，尽管这种分离并不具有相对化性质；虽然所有相对化都是半相对化，但并非所有半相对化都是相对化。相对化障碍就此绕过。此外，我们还看到，尽管算术化有助于其他证明，但这里并未用到它，因此也绕过了代数化障碍。而且，由于该证明以对角化为基础，它也绕过了自然证明障碍。

7 致谢

作者感谢 Scott Aaronson 强调数学严谨性的重要性，感谢 Michael Sipser 帮助厘清早期的概念难点，也感谢 Noson Yanofsky 鼓励作者探究基础性问题。我感谢亚利桑那州立大学 BEYOND Center 及其主任 Paul C.W. Davies 邀请我前往访问并作研讨会报告。访问期间令人振奋的环境和跨学科交流，启发了本文中相关技术的发展。本研究未获得外部资助。

参考文献

[1] Scott Aaronson. NP完全问题与物理现实。ACM SIGACT News，36(1):30–52，2005年。[2] Scott Aaronson。《自德谟克利特以来的量子计算》。剑桥大学出版社，2013年。[3] Scott Aaronson。P=?NP。《数学中的开放问题》，第1–122页，2016年。[4] Scott Aaronson。要实现巨大的量子加速，需要多少结构？arXiv 预印本 arXiv:2209.06930，2022年。[5] Scott Aaronson 和 Avi Wigderson。代数化：复杂性理论中的一道新屏障。ACM计算理论汇刊（TOCT），1(1):2:1–2:54，2009年。[6] Manindra Agrawal、Neeraj Kayal 和 Nitin Saxena。素数属于 P。《数学年刊》，第781–793页，2004年。[7] Sanjeev Arora 和 Boaz Barak。《计算复杂性：现代方法》。剑桥大学出版社，2009年。[8] Theodore Baker、John Gill 和 Robert Solovay。P=?NP 问题的相对化。《SIAM计算杂志》，4(4):431–442，1975年。[9] Charles H Bennett、Ethan Bernstein、Gilles Brassard 和 Umesh Vazirani。量子计算的优势与弱点。《SIAM计算杂志》，26(5):1510–1523，1997年。[10] Stephen Cook。P 与 NP 问题。克雷数学研究所，2(6):3，2000年。[11] Stephen Cook。访谈。海德堡桂冠论坛 https://youtu.be/q0uAoOccBiw?si=bkkN6i8BnHle9lG7，2018年。访问日期：2026年1月15日。[12] Lance Fortnow。P 与 NP 问题的现状。《美国计算机协会通讯》，52(9):78–86，2009年。[13] Richard M. Friedberg。两个递归可枚举集具有不可比较的不可解度（波斯特问题的解答，1944年）。《美国国家科学院院刊》，43(2):236–238，1957年。[14] Merrick Furst、James B Saxe 和 Michael Sipser。奇偶性问题、电路与多项式时间层级。《数学系统理论》，17(1):13–27，1984年。[15] K. G¨odel。致 John von Neumann 的信，1956年3月20日。载于 Solomon Feferman、Jr. J ohn W. Dawson、Warren Goldfarb、Charles Parsons 和 Wilfried Sieg 编，《Kurt G¨odel：文集，第五卷：通信 H–Z》，第372–377页。牛津大学出版社，英国牛津，2003年。.[16] Kurt G¨odel。关于《数学原理》及相关系统中形式上不可判定的命题 I。《数学与物理月刊》，38(1):173–198，1931年。[17] Lov K Grover。量子力学有助于在大海捞针中寻针。《物理评论快报》，79(2):325，1997年。[18] Juris Hartmanis 和 Richard E Stearns。论算法的计算复杂性。《美国数学会汇刊》，117:285–306，1965年。[19] Rahul Ilango、Hanlin Ren 和 Rahul Santhanam。通过伪随机性实现平均情形元复杂性的稳健性。载于第54届 ACM SIGACT计算理论年会论文集，第1575–1583页，2022年。[20] Stephen C. Kleene 和 Emil L. Post。递归不可解度的上半格。《数学年刊》，59(3):379–407，1954年。[21] Richard E. Ladner。论多项式时间可约性的结构。《美国计算机协会学报》，22(1):155–171，1975年。

[22] Dana Moshkovitz。《第2讲：相对化》，2012年。[23] Albert A. Muchnik。《算法理论中可约性问题的不可解性》。苏联科学院学报，108：194–197，1956年。俄文。[24] Ketan D Mulmuley 和 Milind Sohoni。《几何复杂性理论 I：一种研究 P与NP问题及相关问题的方法》。《SIAM计算杂志》，31(2)：496–526，2001年。[25] Carl-Fredrik Nyberg-Brodda。《G. S. Tseytin 的七关系半群与不可判定的字问题》。arXiv 预印本 arXiv:2401.11757，2024年。包含对 Tseytin 和 Scott 于 1956 年所作贡献的历史概述，以及现代英文译本。[26] Emil L Post。《一般组合判定问题的形式化归约》。《美国数学杂志》，65(2)：197–215，1943年。[27] Emil L. Post。《正整数的递归可枚举集及其判定问题》。《美国数学学会通报》，50(5)：284–316，1944年。[28] Joseph J Rotman。《群论导论》，第148卷。Springer Science & Business Media，2012年。[29] Adi Shamir。《IP = PSPACE》。《美国计算机协会学报》（JACM），39(4)：869–877，1992年。[30] Peter W Shor。《量子计算机上用于素因数分解和离散对数的多项式时间算法》。《SIAM评论》，41(2)：303–332，1999年。[31] Michael Sipser。《P 与 NP 问题的历史与现状》。载于第二十四届 ACM计算理论研讨会论文集，第603–618页，1992年。[32] Michael Sipser。《计算理论导论》。《ACM SIGACT News》，27(1)：27–29，1996年。[33] Axel Thue。《根据给定规则改变符号串的问题》，Axel Thue 著……J. Dybwad，1914年。[34] G. S. Tseitin。《带有不可解等价问题的结合演算》。斯捷克洛夫数学研究所学报，52：172–189，1958年。俄文。英文译本载于《美国数学学会译丛》第二辑第94卷，1970年。[35] Grigori S Tseitin。《命题演算中推导的复杂性》。载于《推理自动化：第2卷：1967—1970年计算逻辑经典论文》，第466–483页。Springer，1983年。[36] Alan M Turing。《带消去律的半群中的字问题》。《数学年刊》，52(2)：491–505，1950年。[37] Alan Mathison Turing。《论可计算数及其在判定问题中的应用》。《伦敦数学学会会刊》，2(42)：230–265，1936年。[38] Avi Wigderson。《数学与计算：一场革新技术与科学的理论革命》。普林斯顿大学出版社，2019年。[39] Ryan Williams。《非一致ACC电路下界》。《美国计算机协会学报》（JACM），61(1)：1–15，2014年。