arXiv:2304.00610v1 [cs.CC] 2 Apr 2023

排除不可证句子的短证明很难

Hunter Monroe

2023年4月4日

摘要

如果不存在最优命题证明系统，我们（以及独立地，Pudl´ak）证明，排除任意不可证句子的长度为 t 的证明是困难的。这种从不可证句子到难以证明的句子的映射，有力地将不可计算性的事实转化为复杂性理论中的结论。例如，由于证明字符串 x 是柯尔莫哥洛夫随机的（$x \in R$）通常是不可能的，因此证明"没有长度为 t 的证明能够证明 $x \in R$"通常也很困难，证明编码了这一点的重言式也同样困难。因此，一个拥有一族困难重言式的证明系统，其族的枚举中有稠密地分布着这类重言式。该假设还意味着，某种自然语言是 NP 中间的：重新定义皮亚诺算术，使其具有稀疏补集后，语言 $\{\langle x, 1^t \rangle |$ "不存在长度为 t 的证明来证明 $x \in R\}$"的补集也同样稀疏。

高效地排除长度为 t 的 $x \in R$ 证明，可能会违反这样的限制：不得利用 $x \in R$ 不可证这一事实。我们的猜想是：任何可用于如果—那么语句（或基于分类的证明）的、关于 R 的可计算谓词，其效果都不优于随机分支，因为任何有效检验都会显示 R 似乎是随机的。这一限制也可能妨碍非门和消去在电路及命题证明中的作用——它们是编码如果—那么语句所必需的。如果 R 能击败如果—那么逻辑，就必须进行穷举搜索。

1 引言

我们证明，在一个被广泛相信的猜想成立时，不可计算性与复杂性之间存在深刻联系——即不存在用于重言式的最优命题证明

系统。[1] 该猜想最初提出时，主张的是在施加资源界后，不可计算性结果仍然成立。哥德尔第二不完备性定理指出，任何足够强且一致的理论都无法证明自身的一致性。普德拉克与 Friedman 独立提出了可行一致性猜想：在某个理论中，难以排除任何长度的证明来证明该理论本身不一致。克拉伊切克与普德拉克证明，在较弱理论中，不存在高效证明来证明不一致性，这等价于不存在最优证明系统；后者仍是证明复杂性理论中的一个关键猜想。¨

我们证明：如果能够高效地排除某个不可证明句子 ϕ 存在长度为 t 的证明，那么也能够高效地排除一个稍短的一致性矛盾证明，而后者可用于通过反证法证明 ϕ 的长度为 t 的证明。这蕴含一个强有力的推广——如果难以排除长度为 t 的矛盾证明，那么也难以排除任意不可证明句子的长度为 t 的证明。这进而意味着，可以将关于不可证性和不可计算性的已知事实引入复杂性理论。这有广泛影响——各类不可证明句子都可转化为断言，表明复杂性理论中的开放问题有预期的答案。例如，形如 $x\in R$ 的不可证明句子是稠密的，因此，编码“没有长度为 t 的证明能证明 $x\in R$”的困难的重言式族也同样稠密。将 R 重新定义为具有稀疏补集——字符串属于 R，当且仅当它不是可指数压缩的——之后，该补集

[1]本文旨在向戴维森学院过去和现在的教职员工致敬，其中包括 Hansford Epes、L. Richardson King、Benjamin Klein 和 Clark Ross。感谢 Pavel Pudl´ak 和 Bill Gasarch 提出的意见。本文及其早期版本中的思想得益于与以下人士的讨论：Scott Aaronson、Eric Allender、Olaf Beyersdorff、Ilario Bonacina、Maria Luisa Bonet、Cristian Calude、Marco Carmosino、Yuval Filmus、Vijay Ganesh、Bill Gasarch、Valentina Harizonov、Pavel Hrubeˇs、Rahul Ilango、Russell Impagliazzo、Valentine Kabanets、Mehmet Kayaalp、Yanyi Liu、Ian Mertz、Daniel Monroe、Igor Oliveira、Toniann Pitassi、Hanlin Ren、Rahul Santhanam、Till Tantau、Neil Thapen、Luca Trevisan、Avi Wigderson、Ryan Williams、Marius Zimand，以及乔治·华盛顿大学和戴维森学院研讨会、西蒙斯研究所 2023 年元复杂性项目、2022 年计算复杂性会议、2022 年证明复杂性研讨会和 2022 年具有人文关怀的复杂性会议的其他参与者。其余错误均由我本人负责。[2]参见 Pudl´ak[21] 第 6.4 节及 [22]。Pudl´ak[19] 表明最初的猜想并不正确——某个理论 $\mathcal{T}$ 可以高效地证明 $\mathcal{T}$ 不存在一个长度为 t 的、关于“0=1”的证明。1989 年的重新表述指的是在一个较弱理论中缺乏高效证明。另见 Pudl´ak[21]的定理 59。[3]另见 Kraj´ıˇcek[11] 第 21.3 节。

语言 $\{\langle x, 1^t\rangle |$ 中不存在 $x \in R\}$ 的长度为 t 的证明；它既不属于 P，也不是 NP 完全的，而是 NP 中间。

排除任何不可证明句子的长度为 t 的证明的困难，揭示了不可计算性与复杂性之间的深层联系。我们证明，从不可证明句子到某个理论中难以证明的句子族的隐式映射是一个同构。这将是 ZFC 等理论此前未被注意到的一项重要结构特征。

要形式化“排除长度为 t 的证明很困难”这一直觉，就必须明确哪个理论缺乏长度为 t 的证明，以及哪个理论难以排除这些证明。这些理论必须不同，因为一个能够证明自己缺乏某个 ϕ 的短证明的理论，将证明自身的一致性。我们的主要结果是：

定理 1.1 以下各项等价：[4]

(i) 不存在最优命题证明系统。

(ii) 对于一致理论 $\mathcal{S}$，存在某个更强的理论 $\mathcal{T}$，使得 $\mathcal{S}$ 无法在 $\mathcal{T}$ 中高效地排除 $0{=}1$ 的长度为 t 的证明（即，$\mathcal{S} \nvdash_{t^{\mathcal{O}(1)}} \mathcal{T} \nvdash$“$0{=}1$”）。

（iii）对于（ii）中的 $\mathcal{S}$ 和 $\mathcal{T}$，以及在 $\mathcal{T}$ 中不可证明的任意 ϕ，$\mathcal{S}$ 都无法有效地排除在 $\mathcal{T}$ 中对 ϕ 的长度为 t 的证明（即，$\mathcal{T} \nvdash \phi$ 蕴含 $\mathcal{S} \nvdash_{t^{\mathcal{O}(1)}} \mathcal{T} \nvdash \phi$）。[5]

证明：根据 Kraj´ıˇcek 和 Pudl´ak[12] 的结果，（i）和（ii）等价。

（ii）$\to$（iii）假设（ii）成立。如果 $\mathcal{T}$ 没有长度为 t 的 ϕ 证明，那么就不可能存在比 t 略短的 $0{=}1$ 证明，因为那将产生一个长度为 t 的 ϕ 反证法证明。因此，如果 $\mathcal{S}$ 有效地证明了 $\mathcal{T}$ 没有长度为 t 的 ϕ 证明，这与（iii）相矛盾，那么它也能有效地证明不存在比 t 略短的 $0{=}1$ 证明。这与（ii）相矛盾。因此，（ii）蕴含（iii）。如果 ϕ 在 $\mathcal{T}$ 中是可证明的，那么它在某个长度 t 内可证明，因此（iii）不可能成立，因为 $\mathcal{S}$ 是一致的，无法证明 $\mathcal{T}$ 没有该长度的证明。

(iii)$\to$(i) Chen等人[4]。 ∎

[4]Monroe[17] 还给出了另一个等价条件：对于任意 M 接受型 coBHP $=\{\langle N, y, 1^t\rangle |$，不存在非确定性图灵机（NTM）$N$ 在输入 y 上经过 t 步或更少步骤的接受路径；存在某个 $\langle N'$、$y'\rangle$，使得 N' 在 y' 上不停机，并且 $\langle N'$、y'、$1^t\rangle$ 是一族困难输入。[5]这一猜想由作者提出，并由 Pudl´ak 在一般情形下独立证明；对于句子 $x \in R$，则由作者证明。

对于上文括号中的记号，如果 $\mathcal{T}$ 分别有或没有长度不限的 ϕ 证明，则分别写作 $\mathcal{T}\vdash\phi$ 或 $\mathcal{T}\nvdash\phi$ 。如果理论 $\mathcal{T}$有一个长度为 t （或更短）的句子 ϕ 证明，则写作$\mathcal{T}\vdash^{t}\phi$；否则写作 $\mathcal{T}\nvdash^{t}\phi$。其中，证明长度是表示该证明的二进制串中的符号数。[6] 同样， $\mathcal{T}\nvdash^{t^{\mathcal{O}(1)}}\phi$ 表示 $\mathcal{T}$ 没有关于 ϕ的高效（长度有多项式界的）证明。$\mathcal{T}\vdash\phi$ 与 $\mathcal{T}\vdash^{\mathcal{O}_{(1)}}\phi$ 等价；可证明的句子有有限证明，因此可在某个常数界内得到证明。

下面，我们将通过识别某些不可证明的句子并援引定理 1.1(iii)，说明不存在最优证明系统会推出各种复杂性理论猜想。在许多情况下，我们选择声称字符串 x 是柯尔莫哥洛夫随机的不可证明句子（记作$x\in R$），也就是说， x 的不可压缩部分达到一半，并且不存在以能打印出 x 的程序形式给出的简短描述。[7] 柯尔莫哥洛夫不完备定理指出，在具有可计算枚举（c.e.）定理集合的理论中，证明 $x\in R$ 通常是不可能的。否则，“第一个长度为 n 且可证明没有简短描述的字符串”本身就会成为某个字符串的简短描述，从而导致矛盾。在这里， $x\in R$ 是一个算术语句，用于编码字符串 x （表示为二进制数）缺少简短描述这一事实。由于 R 稠密且不可计算， $x\in R$ 的集合提供了一个稠密的非构造性集合，其中包含大量不可证明的句子。[8]

更正式地，将柯尔莫哥洛夫随机字符串的集合定义为 $R=\{x|\forall p$：如果 $|p|\leq|x|/2$，那么 $p\nearrow$ 或 $p\downarrow$，其中 $U(p)\neq x\}$； U 是运行时间不受限制的确定性通用图灵机（不一定是前缀自由的）， x 和 p是二进制字符串， $|x|$ 表示 x 的长度， $p\downarrow$和 $p\nearrow$ 表示程序 p是否停机，而“$x\in R$”是编码了 $x\in R$的算术语句。单引号和双引号表示一个语句，即一串符号，用于编码一个数学陈述。

如果不存在最优证明系统，那么根据定理 1.1，将会产生重大影响：

- 以正密度排除长度为 t 的证明很难，因为不可证句子 $x\in R$ 具有正密度。等价地，证明

[6]关于证明长度的综述，请参见 Pudl´ak[20]。[7]以压缩一半来定义不可压缩性是任意的，定理 5.1 除外，因为它要求对数不可压缩性。[8]关于柯尔莫哥洛夫复杂度的概述，请参见 Li 和 Vitanyi[14]。近年来，关于元复杂性的文献迅速增长；请参见 Santhanam[25]。

编码“没有长度为 t 的 $x \in R$证明”的重言式很难达到正密度。重言式不存在最优证明系统；稠密的难解 P-一致族见证了其非最优性。

- 一种自然语言属于 NP 中间：该语言“$x \in R$ 缺少长度为 t 的证明”（其中，R 通过要求对数不可压缩性而重新定义为具有稀疏补集）的稀疏补集。该语言不属于 P，但具有 P/poly 电路。
- 从不可证明句子到难以证明的句子的隐式映射是一个同构。然而，它并不完备——例如，需要更强的猜想才能推出多项式层次（PH）不会坍缩；而要确定与其他开放复杂性问题相关的猜想及其对应的同构，可能还需要大量工作。

本文的组织如下。第 2 节介绍预备知识。第 3 节表明，不可证明句子“$x \in R$”在长度为 n的句子中是稠密的。第 4 节讨论其对重言式和证明系统的影响。第 5 节表明，一种自然语言属于 NP 中间。第 6 节表明，从不可证明句子到难以证明的句子的映射是一个同构，并讨论开放问题。第 7 节作结。

2 预备知识

字符串：设二进制字母表为 $\{0,1\}$，令 S^n 为长度为 n 的字符串集合，其中的元素是有序的 n 元组。令 $|x|$ 表示字符串的长度，令 $|S|$ 表示集合 S 的基数。语言 L 是 $\cup_{n \geq 0} S^n$ 的子集。

密度：如果存在 $c > 0$，使得对于充分大的 n，$|L \cap S^n|/n \geq c$，则称 L 中长度为 n 的字符串所占的比例有正的下界。这意味着较弱的条件：L 具有正上密度，即 lim sup $\frac{|L \cap \{1,2,\ldots,n\}|}{} > 0$。如果一个取决于 n 的事件以随着 n 趋于无穷而趋近于一的概率发生，例如 $x \in R$，其中 $|x|=n$，则称该事件以高概率（w.h.p.）发生。

理论：假设理论是皮亚诺算术（PA）或皮亚诺算术的扩展。[9] 为进行平均情况分析，标准定义

[9]该猜想也可以一致地指向一种较弱的理论，例如不含归纳法或无界量词的罗宾逊 Q；通过验证一次停机计算的执行记录，如果事实上 $p\downarrow$，该理论仍然可以证明“$p\downarrow$”。

将皮亚诺算术中的二进制字符串编码为算术句子中的自然数时，采用二进制而非一进制，并在前面加上一个“1”，以避免丢失前导零。

证明系统：命题证明系统是一个多项式时间函数 $h \in \mathrm{FP}$，其值域为 TAUT (Cook 和 Reckhow[6])。对于重言式 τ，任何满足 $h(w) = \tau$ 的字符串 w 都是 τ的证明。若存在 $c \geq 1$，使得 x 的最短 f 证明的长度关于 $|x|$ 以指数 c 多项式有界，且界定于最短 h 证明，则证明系统 h 是最优的（Kraj´ıˇcek 和 Pudl´ak[12]）。当且仅当存在一个 P-一致的重言式族，使得该证明系统所需的证明长度超多项式增长时，证明系统才不是最优的。

3 不可证明句子的密度

Calude 和 J¨urgensen[3] 证明，长度为 n 的算术句子中，真实且不可证明的句子所占比例有一个严格为正的上界。该结果依赖于两个事实：“$x \in R$”通常是不可证明的，并且长度为 n 的字符串以 R的概率为 [10]。在此背景下，定理 1.1 意味着类似的结果也适用于 $\mathtt{coTHEOREMS}_{\leq t} = \{\langle \phi, 1^t \rangle | \mathcal{T} \nvdash_t \phi\}$。

Chaitin 不完备定理指出：

定理 3.1 对于每个一致且算术健全的理论 $\mathcal{T}$，其定理集合可计算枚举，$\exists k \forall x$: $|x|>k$, $\mathcal{T} \not\vdash$‘$x \in R$’。

证明：否则，字符串 x 就可以被简洁地描述为“长度为 n 且满足以下条件的第一个字符串：x $\mathcal{T}$ 证明‘$x \in R$’”，这与 R 的定义相矛盾。一个输入为二进制数 n （长度为 $\log n$）的图灵机可以枚举 $\mathcal{T}$ 的定理，并打印满足以下条件的第一个字符串 x： $\mathcal{T}$证明‘$x \in R$’。于是，k由这台图灵机描述的长度决定，而由于 R 由无法压缩一半的字符串构成，这个长度需要加倍。形式化论述见 Li 和 Vitanyi 的[14] 推论 2.7.2。

引理 3.2 $x \in R$以高概率成立。

证明：根据计数论证，可能的短描述数量很少。长度为 n 的字符串共有 2^n 个。满足 $|p| \leq n/2$ 的程序 p 有 $2^{n/2+1}-1$ 个，这给出了长度为 n 的字符串数量的上界

[10]参见 [3] 中定理 5.2 的证明。

不属于 R 的字符串。因此， R 在长度为 n 的字符串中所占的比例至少为 $1-2^{-n/2}$，所以 $\blacksquare \in R$ 以高概率成立。

Calude 和 J¨urgensen 的结果表明：

定理 3.3 对于每个理论 $\mathcal{T}$，长度为 n 的算术句子中，形如 $\{\text{`}x \in R\text{'} \mid x \in R$ 和 $\mathcal{T} \nvdash x \in R\text{'}\}$ 的句子所占比例有一个大于零的下界，只要 n 足够大。在句子的某种枚举中（例如按字典序排列），不可证明句子具有正上密度。

证明：根据定理 3.1，理论 $\mathcal{T}$ 通常无法证明满足 $x \in R$ 的句子‘$x \in R$’。句子‘$x \in R$’满足 $|\text{`}x \in R\text{'}| = |x| + c$，其中 c 是一个不依赖于 $|x|$ 的常数，这给出了对‘$x \in R$’进行编码的开销，扣除 $|x|$ 后亦然。长度为 n 、形式为‘$x \in R$’的句子所占比例恰为 2^{-c} ，并且这些句子以高概率满足 $x \in R$ 。因此，对于 $\epsilon > 0$，只要 n 足够大，该比例就有下界 $2^{-c} - \epsilon$ 。因此，在句子的某种枚举中，不可证明句子具有正上密度。 $\blacksquare$

下一节需要用到这样一个事实：句子“$x \in R$”在扣除 $|x|$ 后，只需额外增加常数 c 位来编码 $x \in R$ 。

4 重言式与证明系统

重言式可以如下编码句子 $\mathcal{T} \nvdash$“$x \in R$”。对于给定的 x，$\mathcal{T} \nvdash$“$x \in R$”等价于 $\langle$“$x \in R$” $1^t\rangle \in \mathtt{coTHEOREMS}_{\leq t}$。$\mathtt{coTHEOREMS}_{\leq t}$ 和 TAUT 都是 coNP 完全语言，因此存在从 $\mathtt{coTHEOREMS}_{\leq t}$ 到 TAUT 的某个多项式时间归约 r，将 $\langle \phi, 1^t \rangle$ 映射到重言式 $r(\langle \phi, 1^t \rangle)$。

归约 r 产生的重言式证实，$\mathcal{T} \nvdash$“$x \in R$”的每一个可能证明都不是有效证明。归约 r 将一组陈述“不存在长度为 t 的证明”翻译为一组重言式。不要将其与命题翻译混淆，后者将带有单个有界全称量词、且易于在算术的弱片段中证明的句子翻译为易于证明的重言式。[11]

采用这种编码，可以立即得出两个结论：难以证明的重言式族在族的枚举中具有正上密度；并且存在稠密的见证，表明证明系统并非最优。

[11]参见 Kraj ı˘cek[11] 、Cook 和 Nguyen[5]。

4.1 以正密度证明重言式是困难的

R的密度立即意味着，难以证明的重言式族在此类族的枚举中具有正上密度。考虑这样一种族的枚举：其中的布尔公式编码“ ϕ不存在长度为 t的证明”，每个族由 t为 ϕ 编索引，并按 ϕ的字典序枚举这些族。当 ϕ 可在长度 t内证明时，有些公式就不是重言式。在此枚举中， ϕ 形如“$x\in R$”且满足 $x\in R$ 的那些族具有正上密度，而这些族通常是难以证明的重言式。

这个定义并不一定意味着长度为 n 的 TAUT 元素在接受方面是平均情形困难的。例如，允许以小概率出错的算法可以接受任何形如‘$x\in R$’的 ϕ ，并且以高概率正确。无错误的概率多项式时间算法则必然会以非零概率失败。

4.2 非最优性的稠密见证

如果不存在最优证明系统，那么对于任意证明系统 P，都存在一个稠密的困难重言式族集合 $r(\langle$‘$x\in R$’ $1^t\rangle)$，其中 x 遍历所有 $x\in R$。一种以高概率生成此类族的概率多项式时间可计算过程是选择一个足够长的随机字符串 x。然后，根据引理 3.2，$x\in R$ 以高概率成立，因此重言式 $r(\langle$‘$x\in R$’ $1^t\rangle)$ 以高概率对 P 是困难的。对 ZFC 而言难以证明的重言式，对任何其他已知证明系统而言也同样难以证明，因为其可靠性由 ZFC 证明。“足够长”与柴廷定理中的 k 相同，取决于枚举某个理论的定理的图灵机的描述长度。

5 从图灵中间问题到 NP 中间问题

R 是图灵中间集——它不可计算，且其补集是可计算可枚举的，但在多对一可计算归约下并非完备（Rogers[10]定理 8.I(a) 和 (c)）。这引出了一个问题：定理 1.1 是否意味着存在某种相关语言属于 NP 中间类——也就是说，属于 NP、不属于 P，且在多项式时间多对一归约下不是 NP 完全。最后一段将介绍 NP 中间语言的背景。

我们证明，判定语言“在长度t范围内不存在‘$x\in R$’的证明”属于 NP 中间类；为此，我们放宽 R 的定义，使其补集变得稀疏。按这一放宽后的定义，除非字符串能够被压缩超过指数级，而不仅仅是压缩一半，否则就将其视为随机。这使可能的短描述集合变得稀疏，其规模随 $|x|$多项式增长，因此非随机字符串集合也同样稀疏。将这一稀疏版本的 R 定义为 $R^{sp}=\{x|\forall p$: 若 $|p|\leq \log\ |x|$，则 $p\nearrow$或 $p\downarrow$，其中 $U(p)\neq x\}$。与 R一样， R^{sp}不可计算。柴廷定理仍然成立，但参数 k 大了指数级。根据定理 1.1，固定 $\mathcal{S}$和 $\mathcal{T}$。按定义，$\mathcal{T}\not\vdash^{t}$‘$x\in R^{sp}$’当且仅当 $\langle$‘$x\in R^{sp}$’ $1^t\rangle\in$coTHEOREMS$_{\leq t}$。令$R_t^{sp}=\{\langle$‘$x\in R^{sp}$’ $1^t\rangle|\mathcal{T}\not\vdash^{t}$‘$x\in R^{sp}$’$\}$，于是$R_t^{sp}\in$coTHEOREMS$_{\leq t}$。定义$\overline{R_t^{sp}}=\{\langle$‘$x\in R^{sp}$’$1^t\rangle|\neg\mathcal{T}\not\vdash^{t}$‘$x\in R^{sp}$’$\}$。根据 x， $\overline{R_t^{sp}}$可分为$x\notin R^{sp}$，其中对所有 t都有 $\langle$‘$x\in R^{sp}$’ $1^t\rangle\in\overline{R_t^{sp}}$；以及 $x\in R^{sp}$，其中对充分大的 t有 $\langle$‘$x\in R^{sp}$’ $1^t\rangle\in\overline{R_t^{sp}}$。接下来：

定理 5.1 如果不存在最优证明系统，那么：(i) $\overline{R_t^{sp}}$ 是 NP 中间；(ii) $\overline{R_t^{sp}}$ 因此 R_t^{sp} 在 P/poly 中具有最小电路，但这些电路不是 P-一致的。

证明：(i) 根据假设和定理 1.1， $R^{sp}\notin$属于 P。$\overline{R_t^{sp}}$ 是稀疏语言，因为R^{sp}的定义正是为了确保这一点。除非 P=NP，否则稀疏语言在多对一归约下不是 NP 完全；而假设排除了这种情况（Mahaney[16]）。

(ii) $\overline{R_t^{sp}}$ 是稀疏语言，因此它在 P/poly 中有最小电路。这些电路不是 P-一致的，因为那将意味着 $R^{sp}\in$属于 P，而这与假设不符。
∎

Ladner[13] 在假设 P$\neq$NP 的条件下构造了人为的 NP 中间语言。Mahaney 证明，除非 P=NP，否则稀疏语言在多对一归约下不是 NP 完全；而在图灵归约下，除非多项式层次在第二层坍塌，否则也不是 NP 完全。Ogiwara 和 Watanabe[18] 给出了一项采用有界真值表归约的结果。Homer 和 Longpr´e[9]还给出了其他结果和替代性证明。

Allender 和 Hirahara[1] 还给出了自然语言的例子，这些语言在条件成立时属于 NP 中间类。他们证明，如果单向函数存在，那么近似最小电路规模和时间有界柯尔莫哥洛夫复杂度的问题属于 NP 中间类。对于不进行近似时这些问题是否为 NP-困难，目前仍是活跃的研究领域；例如参见 Hirahara[8]。

如果不存在最优证明系统，那么非确定性指数时间$\neq\neq$coNEXP（Krajıˇcek 和 Pudl´ak[12]），因此 NP 中存在不属于 P 的稀疏语言（Hartmanis 等人[7]）。我们的例子不同之处在于，它给出了一个明确的自然语言。

6 同构与开放问题

如果不存在最优证明系统，那么就存在一种隐式映射，将不可证明句子 ϕ 映射到困难的句子族："不存在长度为 t 的 ϕ证明"。这一映射可以扩展为将可证明句子映射到存在长度为 t 的证明的句子族。如果这一映射是满射，它就构成一种同构。这是一幅优雅的图景——数学中一种未被察觉的对称性。然而，还有几个问题尚待解决。

首先，在所有困难句子族的集合中，这一映射并非满射。假设理论 $\mathcal{S}$ 无法有效证明某个并非"在 $\mathcal{T}$ 中不存在长度为 t 的 ϕ 证明"这种形式的句子族，并且该句子族是 P-一致的。我们可以按如下方式使这一映射成为满射。对于每个不在映射值域内、对 $\mathcal{S}$ 而言困难的此类句子族，都存在一个在 $\mathcal{S}$ 中不可证明的句子，它断言"$\mathcal{S}$ 无法有效证明该句子族"。由于根据假设 $\mathcal{S}$ 是一致的，这个句子不可证明；而 $\mathcal{S}$ 也无法证明自己存在一个困难句子族，因为那样就等于证明自身的一致性。因此，将这个不可证明句子映射到该困难句子族。扩展后的映射就是满射。类似的方法也可以解决另一个问题：从不可证明句子到编码"t 不存在长度为 ϕ 的证明"的重言式族的映射并非满射。[12] 一种耐人寻味的理解是，在证明复杂性中，若将 ZFC 这类强大理论视为证明系统，那么困难的重言式族所扮演的角色，可以通过单独考察不可证明句子在 ZFC 中的作用来充分理解。因此，无须借助重言式也能理解证明复杂性。

其次，要将这个问题推广到其他开放问题，还需要额外的猜想。例如，猜想"TAUT不存在最优证明系统"，而某个语言是 Π_1^p -完备的，这还不足以推出 PH 不会坍缩。更强的猜想"对于Π_2^p -完备语言，不存在最优证明系统，即使该证明系统拥有针对 TAUT的预言机"

[12]假设重言式的 P-一致族 τ_n 对于证明系统 P 而言是困难的，并且该证明系统已由理论 $\mathcal{S}$ 证明其可靠性，且该族 τ_n 对于 $\mathcal{S}$而言也同样困难。那么，在 $\mathcal{S}$ 中存在不可证明句子："$\mathcal{S}$ 无法高效地证明 τ_n"以及"P 无法高效地证明 τ_n"。

意味着 $\Pi_2^p \neq \Pi_1^p$。[13] 定理 1.1(iii) 的一个版本将适用于 $\mathcal{S}$，其中包含一个用于判定 Π_1 成员资格的谓词，该集合属于算术层次（AH），从而为具有更高不可解度的句子建立同构。[14] 对于 PH 的每一层，这类猜想都断言：由于 AH 的每一层都存在不可证句子，PH 不会坍缩。简洁地说，这些猜想断言，PH 不会坍缩，是因为 AH 不会坍缩。

这表明，一项研究计划可以为复杂性理论中的每个开放问题确定一个与之相关的猜想及其所蕴含的同构，或者确定这样做所面临的障碍。例如，Liu和Pass[15]等人近期一系列成果表明，断言证明"$\mathcal{T} \nvdash x \in R^t$"的困难性（其中，$R^t$ 是相对于时间有界柯尔莫哥洛夫复杂度定义的）将通过断言时间有界柯尔莫哥洛夫复杂度具有平均情形困难性，进而蕴含单向函数的存在。

如果这些猜想都具有相同的结构，那么可以将它们归纳为一个统一的总猜想，从而有可能为多个开放问题提供洞见。一个非常强的猜想是，定理 1.1(iii)中形式为某种条件的断言，能够解决复杂性理论中的大多数开放问题。

7 结论

定理 1.1 中的条件对复杂性理论具有如此重大的影响，以至于确定它们是否为真、甚至是否可证，都是值得的。一个非正式的论证是：排除长度为 t 的证明来证明一个不可证句子 ϕ 很困难，因为关键事实——不存在任何长度的证明——是无法获取的。对于句子 $x \in R$，这个非正式论证似乎最有力；这类句子是稠密的、非构造性的，通常也不可能被证明。为了以最极端的形式表述这一点，假设关于 $x \in R$ 的任何其他可有效计算的事实，在排除长度为 t 的证明时都可能毫无用处。在任何排除 $x \in R$ 的长度为 t 的证明的程序中，如果—那么语句都需要计算 R 上的一个谓词，以确定应采取哪个分支。同样，在任何执行相同任务的证明中，任何基于分类的推理都需要计算 R 上的一个谓词。然而，R 上的谓词受到这样一个事实的约束

[13] Chen等人[4] 证明，一个 Π_2^p-完全语言没有最优证明系统，当且仅当TAUT没有最优证明系统，因此需要提及预言机，才能区分 Π_2^p 和 Π_1^p。[14] 关于TAUT的构造，参见 Pudl´ak[21] 第569页。

即 R 通过了所有已知的以及可以设想的随机性的有效检验（Li 和 Vitanyi [14] 第 2.4 节）。如果在排除 $x \in R$ 的长度为 t 的证明时，如果—那么语句和基于分类的证明表现得完全随机，那么这种情况是可能的。若果真如此，程序或证明所能做到的不会比逐一穷举检查所有情形的循环更好。

这一约束也可能以非一致的方式发挥作用。布尔电路和命题证明需要非门和消去来实现条件逻辑，例如编码如果—那么语句和基于分类的推理。因此，根据一个由来已久的猜想，这类电路和证明可能会从使用非门和消去中获得有限的益处。已知对于某些单调布尔函数，其非单调电路复杂性与单调电路复杂性之间的差距（分别是带有和不带有非门的最小电路中的门数）是指数级的（Razborov[23],Tardos[27]）；人们希望，对于其他一些单调布尔函数（例如 CLIQUE（Razborov[24],Alon 和 Boppana[2]）），这一差距较小。将这一猜想推广到非单调布尔函数后，结论是：对于某些函数，其可消去电路复杂性与不可消去电路复杂性之间的差距较小；其中，不可消去电路的形式多项式中没有任何单项式同时包含某个文字及其否定（Sengupta 和 Venkateswaran[26]）。[15] 这一论证或许支持这样一种观点：解密短消息等计算任务在实践中很困难，而不仅仅是在渐近意义下困难。

参考文献

[1] Eric Allender 和 Shuichi Hirahara，《电路最小化及相关问题的（非）困难性新见解》，ACMTrans. Comput. The- ory 11（2019），第4期，27:1–27:27。[2]Noga Alon 和 Ravi Boppana，《布尔函数的单调电路复杂度》，Combinatorica 7（1987），1–22。[3] Cristian S. Calude 和 Helmut J¨urgensen，《复杂性是不完备性的来源吗？》，《应用数学进展》35（2005），第1期，1–15。

[15]香农计数论证表明，大多数布尔函数需要 $2^n/n$ 个门。对于随机布尔函数，可消去电路与不可消去电路之间的差距不可能大到足以将电路规模缩减至多项式级别，正如 Tardos 的例子所示。

[4]Yijia Chen、J¨org Flum 和 Moritz M¨uller，《算法与证明系统的困难实例》，《计算世界的方式》（柏林、海德¨堡）（S. Barry Cooper、Anuj Dawar 和 Benedikt L¨owe 编），Springer Berlin Heidelberg，2012，第118–128页。[5] Stephen Cook 和 Phuong Nguyen，《证明复杂性基础：有界算术与命题翻译》，剑桥大学出版社，2014。[6] Stephen Cook 和 Robert Reckhow，《命题证明系统的相对效率》，J. Symb. Log. 44（1979），36–50。[7] Juris Hartmanis、Neil Immerman 和 Vivian Sewelson，《NP-P中的稀疏集合：指数时间与非确定性指数时间》，Inf. Control. 65（1985），第2/3期，158–181。[8] Shuichi Hirahara，《程序学习与部分最小电路规模问题的NP困难性》，Electron. Colloquium Comput. Complex. TR22-119（2022）。[9] Steven Homer 和 Luc Longpr´e，《NP集合到稀疏集合的归约》，计算机与系统科学杂志48（1994），第2期，324–336。[10] Hartley Rogers Jr.，《递归函数与有效可计算性理论》，麻省理工学院出版社，马萨诸塞州剑桥，1987。[11] Jan Kraj´ıˇcek，《证明复杂性》，剑桥大学出版社，纽约州纽约市，2019。[12] Jan Kraj´ıˇcek 和 Pavel Pudl´ak，《命题证明系统、一阶理论的一致性与计算复杂性》，J. Symb. Log. 54（1989），1063–79。[13] Richard E. Ladner，《多项式时间可归约性的结构》，J. ACM 22（1975），第1期，155–171。[14] Ming Li 和 Paul M. B. Vit´anyi，《Kolmogorov复杂性及其应用导论》，计算机科学丛书，施普林格，2008。[15] Yanyi Liu 和 Rafael Pass，《单向函数与Kolmogorov复杂性》，2020 IEEE第61届计算机科学基础年会（FOCS），2020，第1243–1254页。

[16] Stephen R. Mahaney，《NP的稀疏完全集：Berman 和 Hartmanis 猜想的解答》，计算机与系统科学杂志 25 (1982)，第 2 期，130–143 页。[17]Hunter Monroe，《自然问题的加速与不可计算性》，理论计算机科学 412 (2011)，第 4–5 期，478–481 页。[18] Mitsunori Ogiwara 和 Osamu Watanabe，《关于 NP 集合到稀疏集合的多项式时间有界真值表可约性》，SIAM计算杂志 20 (1991)，第 3 期，471–483 页。[19] Pavel Pudl´ak，《一阶理论中有限主义一致性陈述的证明长度》，《逻辑与数学基础研究》，第 120 卷，爱思唯尔，1986 年，第 165–196 页。[20] ———，《证明的长度》，《证明论手册》（Samuel R. Buss 编），爱思唯尔，1998 年。[21] ———，《数学逻辑基础与计算复杂性：通俗入门》，施普林格，2013 年。[22] ———，《有限域中的不完备性》，符号逻辑通报 23 (2017)，第 4 期，405–441 页。[23] Alexander A. Razborov，《逻辑永久式单调网络复杂性的一个下界》，苏联科学院数学札记 37 (1985)，485–493 页。[24] ———，《一些布尔函数单调复杂度的下界》，苏联科学院学报 281 (1985)，798–801 页，俄文。英文译文见《苏联数学学报》31：354–57，1985 年。[25] Rahul Santhanam，《元复杂性导论》，元复杂性训练营，西蒙斯计算理论研究所，2023 年 1 月。[26] Rimli Sengupta 和 H. Venkateswaran，《非消去布尔电路：单调布尔电路的推广》，理论计算机科学 237 (2000)，197–212 页。

[27] ´Eva Tardos，单调与非单调电路复杂度之间的差距是指数级的，Combinatorica 8 (1988)，141–42。