SPARSE相对化框架及其在最优证明系统中的应用

Fabian Egidy 德国维尔茨堡大学

摘要

我们研究由 Krajíček 和 Pudlák（《符号逻辑杂志》，1989年）、Sadowski（FCT 1997）、Köbler 和 Messner（CCC 1998）以及 Messner（博士论文，2000年）提出的以下长期悬而未决的开放问题。

> Q1：TAUT 是否存在（p-）最优证明系统？Q2：QBF 是否存在（p-）最优证明系统？Q3：是否存在具有（p-）最优证明系统的任意复杂度的集合？

最近，Egidy 和 Glaßer（STOC 2025）通过构造预言机，对这些问题作出了贡献：即使假设复杂性类分离方面公认的猜想，也不存在能够得出这些问题肯定回答的可相对化证明。我们沿着这一研究方向继续，通过构造一个预言机证明：即使假设复杂性类分离方面公认的猜想，也不存在能够得出这些问题否定回答的可相对化证明。为此，我们引入 SPARSE-相对化框架，它是 Hirahara、Lu 和 Ren（CCC 2023）提出的有界相对化概念的一种应用。该框架允许为某些命题构造稀疏预言机，同时满足其他有用性质（例如存在无限多项式时间层次）。

通过应用 SPARSE-相对化框架，我们证明 Egidy 和 Glaßer 的预言机构造还能给出以下新的预言机。

> O_1：PSPACE\非确定性多项式时间中没有集合拥有最优证明系统，非确定性多项式时间 $\subsetneq$ 多项式层级 $\subsetneq$ PSPACE，且多项式层级发生坍缩

Cook 和 Krajíček（J. Symb. L. 2007）以及 Beyersdorff、Köbler 和 Müller（Inf. Comp. 2011）构造了针对所有递归可枚举集的最优证明系统，前提是这些证明系统可以使用一比特的非一致建议。我们将他们的技术推广到预言机设定，并应用 SPARSE相对化框架，得到以下新的预言机。

> O_2：PSPACE 中的所有集合都有 p-最优证明系统，存在具有 p-最优证明系统的任意复杂度的集合，且多项式层级是无限的

结合先前的结果，我们的预言机表明，问题 Q1 和 Q2 独立于多项式时间层次是无限的还是发生坍缩。这为 Pudlák（Bull. Symb. Log. 2017）寻找可信猜想作出了贡献：这些猜想通过相对化蕴含 Q1 的否定答案。具体而言，预言机O_2 排除了将多项式时间层次无限作为此类猜想。

2012 年 ACM 学科分类 计算理论 → 预言机与决策树；计算理论 → 证明复杂性；计算理论 → 复杂性类

关键词与短语 相对化、预言机、证明复杂性、最优证明系统

资助 *Fabian Egidy*：获德国学术奖学金基金会资助。

致谢 我们感谢 Christian Glaßer 和 Katharina Pfab 提供的宝贵反馈和建议。

1 引言

我们研究集合存在（p-）最优证明系统与复杂性类分离之间的关系。Cook 和 Reckhow [CR79] 将集合 L 的证明系统定义为一个多项式时间可计算函数 f，其值域为 L。他们提出研究

证明系统，是因为证明系统与复杂性类分离有关：他们证明，NP = coNP 当且仅当存在针对命题重言式集合 TAUT、具有多项式规模证明的证明系统。因此，排除 TAUT 的所有证明系统都具有多项式规模证明这一可能性，就足以证明 NP ≠ coNP。这种解决 NP 与 coNP 问题的方法称为 Cook-Reckhow 计划 [Bus96]。

Krajíček 和 Pudlák [KP89] 为 Cook-Reckhow 计划提出了一个核心定义，刻画了最强证明系统的概念。对于集合 L，如果某个证明系统的证明长度至多比 L的任何其他证明系统中的证明长多项式倍，则该证明系统称为最优。如果集合 L 的证明系统 f 能够将 L 的任何其他证明系统中的证明在多项式时间内转换为 f中的证明，则称其为 p-最优。对于 Cook-Reckhow 计划而言，TAUT 存在最优证明系统 f 意味着，只需研究 f 的下界，而无需研究 TAUT 的所有证明系统。

Krajíček 和 Pudlák [KP89] 提出了一个问题：TAUT 是否存在（p-）最优证明系统。随后，Sadowski [Sad97] 针对真量化布尔公式集合 QBF 提出了同样的问题；Köbler 和 Messner [KM98] 以及 Messner [Mes00] 则分别明确提出了关于任何非确定性多项式时间之外的集合以及 P[1]的问题。本文关注以下由来已久的开放问题。

Q1：TAUT 是否存在（*p*-）最优证明系统?

Q2：QBF 是否存在（*p*-）最优证明系统?

Q3：是否存在具有（*p*-）最优证明系统的任意复杂度的集合?

最近，Egidy 和 Glaßer [EG25]研究了这些问题，并给出了预言机，证明即使假设一些广为接受的猜想成立，也不存在能对这些问题给出肯定答案的可相对化证明；这些猜想分别是 Q1 和 Q2 中的无穷多项式层次，以及 Q3 中的 NP ≠coNP。我们沿着这一研究方向继续推进，构造了一个预言机，证明即使假设无穷多项式层次成立，也不存在能对这些问题给出否定答案的可相对化证明。为此，我们引入了 SPARSE-相对化框架，这是 Hirahara、Lu 和 Ren[HLR23]提出的有界相对化概念的一种应用。在具体阐述我们的贡献之前，我们先概述复杂性理论中的（p-）最优证明系统。

1.1 关于（P-）最优证明系统的先前工作

复杂性类分离。Krajíček 和 Pudlák [KP89] 通过证明以下结论，将（p-）最优证明系统与复杂性类分离联系起来：如果 TAUT 不存在最优证明系统，那么 NE ≠coNE；如果 TAUT 不存在 p-最优证明系统，那么 E ≠NE。Köbler、Messner 和 Torán [KMT03] 将这两个结果分别改进为：对于 TAUT 的最优证明系统，NEE ≠ coNEE；对于 TAUT 的 p-最优证明系统，EE ≠ NEE。Chen、Flum 和 Müller [CFM14] 证明，在 NE\非确定性多项式时间中不存在最优证明系统，会导致测度假设 [Lut97] 不成立；也就是说，NP 在 E 中的测度为 0。

显然，NP（分别地，P）中的所有集合都有（p-）最优证明系统。我们不知道任何一个 NP（分别地，P）之外的集合拥有（p-）最优证明系统。然而，Messner [Mes99, Mes00] 证明，所有对 E 困难的集合都没有 p-最优证明系统，而所有对 coNE 困难的集合都没有最优证明系统。此外，Messner [Mes00]

[1] 显然，NP（分别为 P）中的所有非空集合都存在最优（分别为 p-最优）证明系统。

证明，NP = coNP（分别地，P = NP）意味着对于（p-）最优证明系统，Q3 的答案为肯定。

近似最优算法。 Krajíček 和 Pudlák [KP89] 证明，TAUT 存在 p-最优证明系统，当且仅当 TAUT 存在近似最优算法（即在正实例上最优的算法，也称为最优接受器）。Sadowski [Sad99]将这一结果推广到 SAT（可满足布尔公式集合），Messner [Mes99, Mes00] 则将二者推广到所有可填充集合。此外，Messner 证明，P = NP 蕴含一个集合存在最优接受器，当且仅当它存在 p-最优证明系统。

承诺类。 最优证明系统与承诺类密切相关。Razborov[Raz94] 证明，TAUT 存在最优证明系统，蕴含类 DisjNP（不相交 NP 对类）中存在完全集。类似地，Sadowski[Sad97] 证明，QBF 存在 p-最优证明系统，蕴含 NP ∩ coNP 存在完全集。Köbler、Messner 和 Torán [KMT03] 发现了证明系统与承诺类完全集之间的一般联系。他们改进并推广了以往的结果，证明多项式时间层次中若干集合存在最优和 p-最优证明系统，蕴含承诺类和概率类中存在完全集。例如，TAUT 存在 p-最优证明系统，蕴含 UP 和 NP ∩ SPARSE 存在完全集；多项式时间层次第二层的完全集存在 p-最优证明系统，蕴含 BPP、ZPP 和 RP [KMT03]存在完全集。Beyersdorff、Köbler 和 Messner [BKM09] 以及 Pudlák [Pud17] 建立了 p-最优证明系统与函数类之间的联系。他们共同证明，SAT 存在 p-最优证明系统，蕴含 TFNP 存在完全集。

Pudlák [Pud17] 启动了一项研究计划，旨在证明更多此类蕴含关系，或证明这些关系在某个预言机下不成立。与此同时，除了 Pudlák 正在考虑的一对猜想外，对于所有猜想对，我们要么已有蕴含关系的证明，要么已有在某个预言机下对该蕴含关系的反驳。因此，已有若干预言机（见 [DEG24, DG20, Dos20b, Dos20a, EEG22, GSSZ04, Kha22]）能够分离关于（p-）最优证明系统存在性的猜想与关于承诺类中完全集的其他猜想。

1.2 我们的贡献

1.2.1 SPARSE相对化框架

Egidy 和 Glaßer [EG25] 将一个稀疏预言机与一个使多项式时间层次无限的预言机相结合，使得相对于组合预言机，多项式时间层次仍然是无限的。下面的定理说明了这种方法奏效的主要原因。

▶**定理 1** ([BBS86, LS86])。 如果存在一个稀疏集合 S，使得相对于 S 的多项式时间层次坍缩，那么（未相对化的）多项式时间层次也会坍缩。

因此，当多项式时间层次是无限的时，它相对于所有稀疏预言机也都是无限的。我们引入稀疏预言机独立 命题这一概念，用来指那些成立当且仅当相对于任意稀疏预言机也成立的复杂性理论陈述。请注意，根据定理 1，多项式时间层次是无限的这一命题具有稀疏预言机独立性，而且还有更多此类命题（参见定理 9）。

我们推广了 Egidy 和 Glaßer 的方法，提出一个框架，用以将某个命题 S 的稀疏预言机转化为一个预言机，相对于该预言机，S 与一个稀疏预言机-

独立命题[2] 成立。这样，新框架便提供了更强的证明障碍。

该框架的主要优点在于简单易用且适用范围广。通常，将两个现有的预言机构造结合起来非常困难。然而，我们的框架使得在某些情况下，能够轻松地将两个独立的预言机构造结合起来。更确切地说，只要某个命题相对于稀疏预言机成立，我们的框架就很可能只需付出很小代价，便能为该稀疏预言机增添复杂的性质。第 3 节将深入阐释该框架。此外，我们还为两个新结果给出了简单的证明；若不应用该框架，这些结果将难以实现。

1.2.2 对 Q1、Q2 和 Q3 的贡献

我们应用 SPARSE-相对化框架，并证明 Egidy 和 Glaßer 的预言机构造 [EG25] 可以与 Ko 的一个预言机 [Ko89] 结合，从而得到以下预言机。

O_1：PSPACE 中没有集合拥有最优证明系统，非确定性多项式时间 $\subsetneq$ 多项式层级 $\subsetneq$ PSPACE，且多项式层级坍缩

此外，我们构造了一个计数预言机，使得对 Q1 和 Q2 的回答均为肯定。由于该预言机是使用 SPARSE-相对化框架构造的，我们得到了一个预言机 O_2，相对于它，以下结论成立。

O_2：PSPACE 中的所有集合都有 p-最优证明系统，存在具有 p-最优证明系统的任意复杂度的集合，并且多项式层级是无限的

对 Q1 和 Q2 的贡献。Baker、Gill 和 Solovay 的预言机 [BGS75] 使得相对化后 P = PSPACE；Egidy 和 Glaßer 的预言机 [EG25], 则表明，以下蕴含不存在可相对化证明。

多项式层级坍缩 $\Longrightarrow$ 对 Q1 和 Q2 [BGS75] 的否定回答；
多项式层级无限 $\Longrightarrow$ 对 Q1 和 Q2 [EG25] 的肯定回答

我们的预言机表明，另外两个蕴含也不存在可相对化证明。

多项式层级坍缩 $\Longrightarrow$ 对 Q1 和 Q2 的肯定回答（根据定理 13 得出 O_1）；多项式层级无限 $\Longrightarrow$ 对 Q1 和 Q2 的否定回答（根据推论 38 得出 O_2）

注意到，鉴于人们相信多项式时间层次是无限的，且 Q1 和 Q2 的答案都是否定的 [Pud17], ，我们的两个结果都排除了通过可相对化证明从一个“很可能成立的前提”推出一个“很可能成立的结论”。总而言之，就可相对化证明技术而言，问题 Q1 和 Q2 与多项式时间层次是无限还是发生坍缩无关。此外，Pudlák [Pud17] 在寻找能够通过相对化方式推出 Q1 答案为否定的可信猜想。预言机 O_2 表明，无限多项式时间层次不能作为这样的猜想。

[2] 更准确地说，对于那些相对于至少一个预言机成立的稀疏预言机独立命题，这是可能的。

对 Q3 的贡献。Egidy 和 Glaßer [EG25] 构造了一个预言机，表明即使假设 NP $\neq$coNP，也不存在能证明 Q3 答案为肯定的可相对化证明。Messner[Mes99, Mes00] 表明，对 Q3 给出否定答案意味着 NP $\neq$coNP。预言机 O_2拓展了 Messner 的障碍，表明即使假设多项式时间层次是无限的，也不存在能证明 Q3 答案为否定的可相对化证明。这表明，否定地证明 Q3 本身存在一定难度，并非仅仅因为它与 NP 对 coNP 问题有关。

1.3 比较稀疏预言机与随机预言机

我们的 SPARSE-相对化框架与 Fortnow 的 [For99] "Book Trick"理念相似，因此我们在此作简要介绍。与我们一样，Fortnow 关注的是这样的相对化世界：其中某些命题成立，同时存在无限多项式时间层次。他还指出，"构造这样的世界仍然是一项艰巨的任务"，而手动运用 Yao [Yao85] 或 Håstad [Hås89] 的技术实现无限多项式时间层次，"充其量也相当复杂"。因此，他引入了 Book Trick，其依据是 Book [Boo94]的一项结果。

▶**推论 2** ([Boo94]). 对于任意预言机 A，如果相对于 A 的多项式时间层次是无限的，那么对于随机 R，相对于 $A \oplus R$ 的多项式时间层次也是无限的。

▶**引理 3** ([For99], Book Trick). 如果 P 是一个可相对化命题，且对于所有A和随机 R， $P^{A\oplus R}$ 都成立，那么存在一个预言机 B，使得 P^B成立，并且相对于 B的多项式时间层次是无限的。

利用 Book Trick，Fortnow [For99]构造出了几个预言机，使得相对于这些预言机，多项式时间层次是无限的，并且相对于随机预言机成立的命题也成立（类似于我们在定理 13 中使用 SPARSE-相对化框架的方式）。然而，Håstad、Rossman、Servedio 和 Tan[HRST17] 取得的突破性结果表明，多项式时间层次相对于随机预言机是无限的，这使 Book Trick 过时了。显然，任何一对分别相对于随机预言机成立的命题，也会共同相对于随机预言机成立。

总而言之，如果我们希望找到一个具有某种性质 P 且多项式时间层次无限的预言机，那么有两种同样简洁优雅的方法：要么证明 P相对于随机预言机成立，要么证明 P 相对于稀疏预言机成立[3]。请注意，随机预言机方法不适用于多项式时间层次塌缩的情况（这通常也是一种值得追求的性质），而我们的 SPARSE-相对化框架则适用（参见定理 6）。

1.4 O_2 的构造概述

主要难点在于构造一个稀疏预言机，使得相对于该预言机，(a) PSPACE 中的所有集合都有 p-最优证明系统；(b) 存在具有 p-最优证明系统的任意复杂度的集合。然后，SPARSE-相对化框架还会提供一个无限多项式时间层次。

对于 (a)：Cook 和 Krajíček [CK07] 展示了如何在获得一比特非一致建议的情况下，为 TAUT 构造最优证明系统。Beyersdorff、Köbler 和 Müller [BKM11]将这一结果推广到了所有递归可枚举集。对于一个集合 L，其工作方式如下：设 f 为

[3] 如第 3 节所述，与任意基础预言机合并。

任意一个多项式时间可计算函数，且 $n \in \mathbb{N}$。若对所有 $x \in \Sigma^n$，都有 $f(x) \in L$，则将长度为$\langle \mathsf{code}(f)\ n\rangle$的建议位设为 1；否则设为 0。p-最优证明系统可以利用这些建议位来判断自己能够模拟哪些计算，而不会输出 L之外的元素。我们将这一思路推广到预言机。需要注意的是，这种推广并不直接，因为建议设置是不对称的：证明系统可以访问一比特非一致建议，而被证明集合是由不带建议的图灵机识别的。相比之下，我们的预言机设定是对称的：证明系统和识别被证明集合的图灵机都可以访问同一个预言机。[4]由于 PSPACE机器和证明系统只能提出多项式有界的查询，我们可以通过多项式长度填充，将建议隐藏在预言机中，使其无法被编码该建议的计算获取。这样一来，p-最优证明系统仍可利用建议，而证明长度只会因此增加多项式长度。

对于 (b)：对每个时间可构造函数 t，我们定义一个集合 L_t，若某个长度为 $\approx t(n)$ 的码字位于预言机中，则该集合包含 0^n。我们对任何试图在不查询长度为 $\approx t(n)$ 的字的情况下判定 L_t 的图灵机进行对角化，即当且仅当这样的图灵机拒绝 0^n 时，才将长度为 $\approx t(n)$ 的码字加入预言机。由此，任何判定 L_t 的图灵机的运行时间必须至少为 t。由于运行时间 t 也足以判定 L_t，且 $x \in L_t$ 的证明是通用的（预言机中存在一个固定码字），因此可得 L_t 存在 p-最优证明系统。

2 预备知识

设 $\Sigma := \{0,1\}$ 为默认字母表，Σ^* 为 Σ 上的有限字集合。所有（正）自然数的集合记为 $\mathbb{N}$ ($\mathbb{N}^+$)。对于 a、$b \in \mathbb{N}$，我们定义 $a\mathbb{N}+b := \{a\cdot n+b \mid n \in \mathbb{N}\}$。我们将空集写作 $\emptyset$。集合 A 的基数记为 $\#A$。对于集合 $A \subseteq \Sigma^*$ 和数 $n \in \mathbb{N}$，我们定义 $A^{\leq n} := \{w \in A \mid |w| \leq n\}$，对 $=$ 亦类似。为使记号更清晰，我们用 $\Sigma^{\leq n}$ 表示 $\Sigma^{*\leq n}$，用 Σ^n 表示 $\Sigma^{*=n}$。运算符 $\cup$、$\cap$ 和 $\setminus$ 分别表示并集、交集和差集。我们将集合 A、B 的标记并记为 $A \oplus B := 2A \cup (2B+1)$。函数 f 的定义域和值域分别记为 $\mathsf{dom}(f)$ 和 $\mathsf{ran}(f)$。我们采用 [AB09] 中所述的时间可构造函数概念。我们使用图灵机的默认模型，包括确定性与非确定性两种变体。由图灵机 M 判定的语言记为 $L(M)$。我们使用图灵转导器来计算函数。对于图灵转导器 F，当输入 x 时该转导器输出 y，我们记作 $F(x) = y$。因此，图灵转导器 F 计算一个函数，我们可以用 F 本身来表示“由 F 计算的函数”。

复杂性类。 P、FP、非确定性多项式时间、coNP、Σ_k^p、Π_k^p、多项式层级、IP、PSPACE、E、DTIME 等基本复杂性类，以及完全集 TAUT 和 QBF 的定义可参见[AB09]。EXPH 类在 [HLR23] 中有严格定义。若存在一个多项式 p，使得对所有 $n \in \mathbb{N}$ 都有 $\#\, S^{\leq n} \leq p(n)$，则集合 $S \subseteq \Sigma^*$ 是稀疏的。集合 $T \subseteq 0^*$ 是 tally。我们将所有稀疏集合构成的类记为 SPARSE，将所有 tally 集合构成的类记为 TALLY。当我们使用表达“存在任意复杂度的集合，使得.....”时，指的是一个集合族 $\mathcal{C}$

[4] 考虑 coNE难集时，这一区别便显而易见：正如 Messner [Mes99]所证明的那样，这类集合没有最优证明系统。Messner 的结果具有相对化性质，即当 coNE机器和证明系统可以访问任意预言机时，该结论仍然成立。另一方面，根据 Beyersdorff、Köbler 和 Müller [BKM11], 的结果，对于任意 coNE难集，都存在一个带有 1 比特非一致建议的最优证明系统。

的集合，使得对于任意时间可构造函数 t，都存在某个可判定集合 $A \in \mathcal{C}$，满足$A \notin$ DTIME(t)。

证明系统。 我们采用 Cook 和 Reckhow [CR79] 对集合所定义的证明系统。他们将函数 $f \in$ FP 定义为 ran(f) 的一个证明系统。此外：

- 若存在一个全函数 π（分别地，$\pi \in$ FP）和一个多项式 p，使得对所有 $x \in \Sigma^*$ 均有 $|\pi(x)| \leq p(|x|)$ 且 $f(\pi(x)) = g(x)$，则称证明系统 g 可由证明系统 f（多项式时间）模拟，记作 $g \leq f$（分别地，$g \leq^{\mathrm{p}} f$）。在此语境下，函数 π 称为模拟函数。注意，$g \leq^{\mathrm{p}} f$ 蕴含 $g \leq f$。若对于所有满足 ran(g) $=$ ran(f) 的 $g \in$ FP，均有 $g \leq f$（分别地，$g \leq^{\mathrm{p}} f$），则称证明系统 f 是 ran(f) 的（多项式时间）最优证明系统。

相对化概念。 我们通过为图灵机和图灵转导器提供只写预言机带，使图灵机和图灵转导器的概念相对化。我们通过将复杂性类、证明系统、机器以及（多项式时间）模拟定义在可访问预言机的机器之上，使这些概念相对化；也就是说，每当定义中涉及图灵机或图灵转导器时，我们就将其替换为预言机图灵机或预言机图灵转导器。对于空间有界图灵机，我们采用 Simon [Sim77]，提出的模型，在该模型中，预言机带也受多项式空间界限制。我们在相关概念的上标中标明对某个预言机 O 的访问，例如，对于复杂性类 $\mathcal{C}^O$ 以及图灵机或图灵转导器 M，分别记作 $\mathcal{C}$ 和 M^O。有时，为了阐释直观思路，我们会省略上标中的预言机，例如在勾勒思路时；但在实际证明中绝不省略。我们也将所有记号推广到相应的预言机概念。

3 SPARSE相对化框架

有界相对化。 最近，Hirahara、Lu 和 Ren [HLR23]引入了有界相对化这一概念，为建立强于通常相对化的证明障碍提供了一个框架。

▶**定义 4**。 （有界相对化 *[HLR23]*）对于一个复杂性类 C，如果一个复杂性理论命题相对于每个 $O \in C$预言机都成立，则称该命题是 C-相对化的。

Hirahara、Lu 和 Ren 提出了这样一个假设：“当前证明技术”是 PSPACE相对化的，也就是说，“当前技术”能够证明的命题相对于所有$O \in$PSPACE预言机都成立。他们通过证明一些由算术化等非相对化技术证明的典型结果是 PSPACE相对化的，来支持这一假设，例如 IP $=$ PSPACE。此外，他们还解释了这一假设如何带来强有力的证明障碍：

- 如果某个命题 S 相对于一个 $O \in$PSPACE预言机不成立，那么就可以推出，“当前技术”（根据他们的假设，这些技术是 PSPACE相对化的）无法证明 S。此外，如果该命题 S 相对于一个 $O \in$EXPH预言机不成立，那么“当前技术”就无法证明 S，除非该证明蕴含 PSPACE $\neq$ EXPH；而这将是复杂性理论中的突破性结果。根据他们的假设，这一结论成立，因为基于“当前技术”的 S 证明对 PSPACE 中的所有预言机都成立，但并非对 EXPH 中的所有预言机都成立，从而将 PSPACE 与 EXPH 区分开来。

SPARSE-相对化框架。 我们通过提出稀疏预言机独立性的概念，继续推进这项研究，并由此获得比通常的相对化更强的证明障碍。

▶**定义 5。 </style}复杂性理论陈述 是稀疏预言机独立的，当且仅当 为真等价于相对于来自 SPARSE** 的每个预言机， S 为真。

直观地说，我们不知道稀疏预言机独立命题是否为真；但如果它为真，那么按照 [HLR23] 的意义，该命题就是SPARSE 相对化的。因此，只要该命题为真，其正确性就独立于它是否可以访问稀疏预言机。我们将先通过一个例子说明稀疏预言机独立命题的用途，然后再将其一般化。

Long 和 Selman [LS86] 以及 Balcázar、Book 和 Schöning [BBS86] 分别独立地证明了 Karp-Lipton 定理 [KL80]的如下推广。

▶ **定理 6** ([BBS86,LS86])。 **(i)** 如果存在一个稀疏集合 S 使得相对于 S 的多项式时间层次发生坍缩，那么（非相对化的）多项式时间层次也会发生坍缩。**(ii)** 如果存在一个稀疏集合 S 使得相对于 S 的多项式时间层次是无限的，那么（非相对化的）多项式时间层次也是无限的。

换句话说，我们不知道多项式时间层级是无限的还是会坍缩，但我们知道这两种情况都具有 SPARSE 相对化性质。因此，“多项式层级是无限的”和“多项式层级会坍缩”都是与稀疏预言机无关的命题。

正如 Bovet、Crescenzi 和 Silvestri [BCS95]所指出的，对相应证明的分析表明，定理 6 本身具有相对化性质，由此得到以下结果。

▶**定理 7**。设 $A \subseteq \Sigma^*$ 且 $B \in \mathrm{SPARSE}$。多项式层级^A 会坍缩，当且仅当多项式层级$^{A\oplus B}$会坍缩。

这表明，将任意预言机与稀疏预言机结合，不会改变相对于该任意预言机的多项式时间层级是否有限。根据 Yao[Yao85] 以及 Baker、Gill 和 Solovay [BGS75], , 存在一个预言机 A_{Yao} 使得相对于它，多项式时间层级是无限的；也存在一个预言机 A_{BGS} 使得相对于它，多项式时间层级会坍缩。

假设我们想要证明某个命题 S的困难性。针对 S 的传统预言机告诉我们

$$\text{“the statement } S \text{ is not relativizably provable”.}$$

然而，根据定理 7，仅仅解决任务

任务 constructSPARSE(命题 S，集合 A)：构造 $B \in \mathrm{SPARSE}$，使得 S 相对于 $A \oplus B$失败

对于 S 和 A_{Yao}，即可立即得到更强的证明障碍

“即使假设存在无穷多项式层次，命题 S 也不是相对化可证明的”。

由于无限多项式时间层次是结构复杂性理论中的标准假设，在该假设下排除 S 的可相对化证明，进一步说明了证明 S的困难性。

我们可以将这一方法推广到任意相对于所有预言机都具有稀疏预言机独立性的命题，也就是说，这些命题即使自身相对于某个预言机进行相对化，仍然具有稀疏预言机独立性[5]。

[5] 由于证明“某个命题是稀疏预言机独立”的证明通常本身也具有相对化性质，因此稀疏预言机独立的命题通常对所有预言机都成立。

►**定理 8**。 设 S_1 是一个相对于所有预言机都具有稀疏预言机独立性的命题， A 是一个预言机， S_1 相对于该预言机成立，并且对于某个命题 S_2， B 根据 constructSPARSE(S_2, A)构造而成。那么， S_1 成立，而 S_2 相对于 $A \oplus B$不成立。

证明。预言机 B 的构造满足 $B \in \mathrm{SPARSE}$ 和 S_2 相对于 $A \oplus B$失败。此外， S_1 相对于 A 成立，且相对于所有预言机均与稀疏预言机无关，因此 S_2 也相对于 $A \oplus B$成立。◄

constructSPARSE(S， A) 的要求是“S 相对于 $A \oplus B$ 失败”，而不是S 仅仅相对于 B 失败；这是定理 8 所必需的，否则我们会得到矛盾。多项式层级 $\mathrm{PH}^{\emptyset}$ 要么是无限的，要么会坍缩。于是定理 8 将推出，多项式层级 $\mathrm{PH}^{\emptyset \oplus A_{\mathrm{BGS}}}$ 或多项式层级 $\mathrm{PH}^{\emptyset \oplus A_{\mathrm{Yao}}}$ 既是无限的，又会坍缩。

然而，在许多情况下，实现“S 相对于$A \oplus B$失败”未必比实现“S 相对于 B 失败”更困难。至少对于这样一些预言机构造，这一结论成立：它们使用的对角化论证不取决于构造开始时是否已经存在某个基础预言机 A 。事实上，我们在第 4 节中的预言机构造就属于这种类型。这使我们能够描述一个适用于所有集合 $A \subseteq \Sigma^*$ 作为基础预言机的单一预言机构造。因此，在这些情况下，构造一个相对于它 S 失败的稀疏预言机，就能让我们将定理 8 应用于许多与稀疏预言机无关的命题。

除定理 6 外，还有其他与稀疏预言机无关的命题。下述定理列举了其中一些。

►**定理 9** （ [BBS86、LS86、KSTT92]提出的稀疏谕示无关陈述）。
1. 对所有 $S \in SPARSE$，$PH = PSPACE$ 当且仅当 $PH^S = PSPACE^S$ 。 *[LS86，BBS86，命题 3.13，定理 3.3]2.* 对所有 $S \in SPARSE$，$PH \neq PSPACE$ 当且仅当 $PH^S \neq PSPACE^S$ 。 *[BBS86，定理 4.8]3.* 对所有 $S \in SPARSE$，$PP \subseteq PH$ 当且仅当 $PP^S \subseteq PH^S$ 。 *[BBS86，定理 3.4]4.* 对所有 $S \in SPARSE$，$PP \not\subseteq PH$ 当且仅当 $PP^S \not\subseteq PH^S$ 。 *[BBS86，定理 4.6]5.* 对所有 $S \in SPARSE$，$NP \subseteq C{=}P$ 当且仅当 $NP^S \subseteq C{=}P^S$ 。 *[KSTT92，定理 6.3]6.* 对所有 $S \in SPARSE$，$NP \subseteq \oplus P$ 当且仅当 $NP^S \subseteq \oplus P^S$ 。 *[KSTT92，定理 6.3]7.* 对所有 $S \in SPARSE$， $\oplus P \subseteq PP$ 当且仅当 $\oplus P^S \subseteq PP^S$ 。 *[KSTT92，定理 6.3]*

Bovet、Cresczeni 和 Silvestri [BCS95，定理 4.3] 通过给出命题成为稀疏预言机独立命题的充分条件，推广了这类稀疏预言机独立命题。此外，定理 9 中命题 2 和 4 的性质相对于 A_{Yao}[6] 成立，而其余命题的性质相对于 A_{BGS}成立。

总之，根据定理 8，对于任意命题 S_2 以及定理 6 和 9 中的任意稀疏预言机独立命题S_1 ，通过按照 constructSPARSE(S_2， A) 构造预言机 B ，并令 $A \in \{A_{\mathrm{Yao}}, A_{\mathrm{BGS}}\}$，我们得到以下障碍

> “即使假设 S_1，命题 S_2 也不是相对化可证明的”。

在第 4 节中，我们将这一方法应用于如下命题：“PSPACE 中的所有集合都有 p-最优证明系统，并且存在具有 p-最优证明系统的复杂度任意高的集合”。

[6] 相对于该预言机，PSPACE 和概率多项式时间具有完全集，这与多项式层级的情况相反。

TALLY相对化框架。 通过使用复杂度类 TALLY 而非 SPARSE 来扩展定义 5，我们称复杂性理论陈述 S 是与计数预言机无关的陈述，如果 S 成立等价于对每个来自 TALLY 的预言机， S 相对该预言机成立。运用与 SPARSE相对化框架相同的推理，我们可以得出 constructSPARSE 的 TALLY 版本（称为 constructTALLY）以及定理 8 的 TALLY 版本。下面介绍文献中一些已知的与计数预言机无关的陈述。

▶**定理10** （ [LS86]提出的与计数预言机无关的陈述）。
1. P =非确定性多项式时间，当且仅当对所有 $T \in TALLY$，P^T = 非确定性多项式时间^T。 *[LS86，推论 3.5]2.* 非确定性多项式时间 =*coNP*，当且仅当对所有 $T \in TALLY$，非确定性多项式时间^T = *coNP*^{T}。 *[LS86，推论 3.3]3.* P =*PSPACE*，当且仅当对所有 $T \in TALLY$，$P^T = PSPACE^T$。 *[LS86，命题 3.11]4.* 非确定性多项式时间 = *PSPACE*，当且仅当对所有 $T \in TALLY$，非确定性多项式时间^T = *PSPACE*^{T}。 *[LS86，命题 3.12]5.* 非确定性多项式时间 ⊆*E*，当且仅当对所有 $T \in TALLY$，非确定性多项式时间$^T \subseteq E^T$。 *[LS86，命题 3.10]*

由于定理10的所有命题都相对于预言机 A_{BGS}成立，我们可以推导出上述与计数预言机无关的陈述的以下应用。对于任意命题 S_2以及定理10中的任意与计数预言机无关的陈述 S_1 ，通过根据 constructTALLY(S_2， A_{BGS}) 构造预言机 B，我们得到以下障碍

“即使假设 S_1，命题 S_2 也不是相对化可证明的”。

来自 SPARSE 的预言机∩EXPH。 众所周知，“可相对化证明技术”已经无法涵盖我们的“当前技术”。事实上，SPARSE相对化技术也无法涵盖算术化等“当前技术”。Shamir [和 Sha92] 证明了 IP = PSPACE，但 Fortnow 和 Sipser [FS88] 展示了一个稀疏预言机[7] A ，使得 IP^A ≠PSPACE^A。因此，将 Hirahara、Lu 和 Ren [HLR23] 的有界相对化方法与我们的方法结合起来，是很有意义的。

设 S_1 是一个稀疏谕示无关陈述，且它相对于某个 EXPH 可计算预言机 A 为真。对于命题 S_2，令 B 按照 constructSPARSE(S_2, A) 的 SPARSE ∩EXPH 版本来构造。如果“当前技术”是 PSPACE相对化的，且不能证明 PSPACE ≠EXPH，我们就得到如下证明障碍

“即使假设 S_1，‘当前技术’也不能证明命题 S_2”，

因为 $A \oplus B \in$ EXPH，从而 [HLR23] 适用，并且针对 S_1、 S_2、 A 与B 的定理 8 也适用。因此，这类预言机为命题提供了最强的证明障碍，由此引出以下两项任务。

1.证明存在EXPH可计算预言机，相对于这些预言机，稀疏谕示无关陈述为真。**2.** 按照一个SPARSE ∩EXPH 版本的 constructSPARSE 为命题构造预言机[8]。我们尤其关注以下问题。

开放问题：是否存在一种 EXPH可计算谕示，使得相对于它的多项式时间层次是无限的?

[7] Fortnow 与 Sipser 所构造的预言机并不稀疏，但很容易转化为稀疏预言机。[8] 如前所述，其难度可能仅相当于从 SPARSE ∩EXPH 构造针对命题的预言机。

据我们所知，目前只知道相对于 Håstad、Rossman、Servedio 和 Tan [HRST17] 构造的随机预言机，以及相对于 Hitchcock、Sekoni 和 Shafei [HSS21, Thm. 4.4] 构造的某种空间随机预言机，多项式时间层次是无限的。

SPARSE-相对化框架的应用。Egidy 和 Glaßer [EG25] 证明了以下定理。

▶ **定理 11** ([EG25])。 任取 $A \subseteq 2\mathbb{N}$。存在一个稀疏预言机 $B \subseteq 2\mathbb{N}+1$，使得所有 $L \in \mathrm{PSPACE}^{B\cup A}$ |非确定性多项式时间$^{B\cup A}$ 相对于 $B \cup A$都没有最优证明系统。

此外，分析 Balcázar、Book 和 Schöning 的定理 4.5 的证明 [BBS86]，可得以下结果，该结果对所有预言机也成立。

▶ **推论 12** ([BBS86], 定理 4.5 的推论)。 对于所有 $k \geq 3$，都有

$$\Sigma_k^p \neq \Pi_k^p \implies \Sigma_{k-2}^{p,S} \neq \Pi_{k-2}^{p,S} \text{ for all } S \in \mathrm{SPARSE}.$$

请注意，上述推论不同于定理 6 和定理 9。命题 $\Sigma_k^p \neq \Pi_k^p$ 可能不是稀疏预言机独立的，但它几乎是，因为稀疏预言机至少能将多项式时间层次第 k 层的分离保持到第 $k-2$层。

使用我们的 SPARSE-相对化框架，可以得到以下定理。

▶**定理 13.** 存在一个预言机 O_1，使得 非确定性多项式时间^{O_1} $\subsetneq$ 多项式层级^{O_1} $\subsetneq$ PSPACE^{O_1}，多项式层级^{O_1}塌缩，并且所有 $L \in \mathrm{PSPACE}^{O_1}$ |非确定性多项式时间^{O_1} 都没有相对于 O_1 的最优证明系统。

证明。 令 S 为命题“所有 $L \in$ PSPACE \非确定性多项式时间都没有最优证明系统”。根据定理 7 和定理 9，命题“多项式层级塌缩”和“PSPACE $\neq$多项式层级”相对于所有预言机都是稀疏预言机无关的。根据 Ko [Ko89，定理 4.4], ，存在一个预言机 A_{Ko}，相对于它，PSPACE$^{A_{\mathrm{Ko}}} \neq \Sigma^{p,}_{4}{}^{A_{\mathrm{Ko}}} = \Pi^{p,}_{4}{}^{A_{\mathrm{Ko}}} \neq \Sigma^{p,}_{3}{}^{A_{\mathrm{Ko}}}$。根据定理 11，存在一个按照 constructSPARSE($\neg S$, A_{Ko}) 构造的预言机 B。于是定理 8 给出，存在一个预言机 $O_1 := A_{\mathrm{Ko}} \oplus B$，使得 PSPACE^{O_1} $\neq$ 多项式层级^{O_1}，多项式层级^{O_1} 塌缩，并且所有$L \in$ PSPACE^{O_1} \非确定性多项式时间^{O_1} 都没有相对于 O_1 的最优证明系统。

剩下要证明的是 NP^{O_1} $\neq$ PH^{O_1}。由推论 12 以及 $\Sigma^{p,}_{3}{}^{A_{\mathrm{Ko}}} \neq \Pi^{p,}_{3}{}^{A_{\mathrm{Ko}}}$和$B \in$ SPARSE，可得 NP$^{O_1} = \Sigma^{p,}_{1}{}^{O_1} \neq \Pi^{p,}_{1}{}^{O_1}$ =coNP^{O_1}。因此，NP^{O_1} $\neq$PH^{O_1}。◀

我们想指出，与简单应用 SPARSE-相对化框架相比，手动构造这样一个预言机尤其困难。定理 13 揭示了关于 Q1 和 Q2 的以下结论，因为 TAUT^{O_1}，QBF^{O_1} $\in$ PSPACE^{O_1} \ NP^{O_1}。

▶**推论 14**。 对Q1 和Q2 的否定回答，并不能通过相对化推出多项式层级 是无限的。

4 P-最优证明系统与 TALLY 预言机

在本节中，我们构造一个计数预言机，相对于该预言机，PSPACE 中的所有集合都具有 p-最优证明系统，并且存在具有 p-最优证明系统的任意复杂度的集合。通过在构造开始时使用任意预言机 $A \subseteq \Sigma^*$ 作为基础预言机，我们可以应用定理 8，从而得到一些预言机，相对于这些预言机，定理 6、9、10 中 tally谕示无关的以及与稀疏预言机无关的陈述也成立。

4.1 谕示构造的记号

字与集合。我们用 $|w|$ 表示字 $w \in \Sigma^*$ 的长度。空字的长度为 0，记为 ε。对于 $0 \le i < |w|$，字 w 的第 $(i+1)$ 个字母记为$w(i)$，即 $w = w(0)w(1)\cdots w(|w|-1)$。若 v 是 w 的（严格）前缀，则记为 $v \sqsubseteq w$ ($v \sqsubseteq w$) 或 $w \sqsupseteq v$ ($w \sqsupseteq v$)。

我们通过一个多项式时间可计算且多项式时间可逆的双射 enc: $\Sigma^* \to \mathbb{N}$，将 Σ^* 与 $\mathbb{N}$ 对应起来，该双射定义为 $\mathrm{enc}(w) = \sum_{i<|w|}(1+w(i))2^{|w|-1-i}$。因此，我们可以将来自 Σ^* 的字视为来自 $\mathbb{N}$ 的数，反之亦然；这使我们能够将字的记号、关系和运算用于数，反之亦然（例如，我们可以据此定义数的长度）。诸如 0^i 和 1^i 这样的表达式含义模糊，因为它们既可以解释为来自 Σ^* 的字，也可以解释为数。我们根据上下文消除这种歧义，或明确指出采用哪种解释。因此，一个字 $w \in \Sigma^*$ 可以解释为集合 $\{i \in \mathbb{N} \mid w(i) = 1\}$，进而解释为一个部分预言机；该预言机对长度不超过 $|w|-1$的所有字都有定义。因此，$|w|$是 w 尚未定义的第一个字，即 $|w| \in w1$ 和 $|w| \notin w0$。在谕示构造过程中，我们经常用来自 Σ^* 的字表示部分定义的预言机。特别地，对于部分预言机中未定义的字，谕示查询均得到否定回答。

函数。函数 f' 是函数 f 的扩展，记作 $f \sqsubseteq f'$ 或 $f' \sqsupseteq f$，如果 $\mathrm{dom}(f) \subseteq \mathrm{dom}(f')$，且对所有 $x \in \mathrm{dom}(f)$，$f(x) = f'(x)$。如果 $x \notin \mathrm{dom}(f)$，则 $f \cup \{x \mapsto y\}$ 表示 f' 对 f 的扩展，使得 $f'(z) = f(z)$ 对 $z \neq x$ 成立，且 $f'(x) = y$。如果对于某个证明系统 f，$y \in \mathrm{ran}(f)$，则我们将 y 的最短 f-证明记作 y_f，即 $f(y_f) = y$，并且对所有 $x < y_f$，$f(x) \neq y$。如果 $y \notin \mathrm{ran}(f)$，则 y_f 未定义。

我们定义多项式函数 p_k: $\mathbb{N} \to \mathbb{N}$，对 $k \in \mathbb{N}^+$ 定义为 $p_k(n) := n^k + k$。此外，令$\langle\cdot\rangle$: $\bigcup_{i\ge 0}\mathbb{N}^i \to \mathbb{N}$ 为一个单射的、多项式时间可计算且多项式时间可逆的序列编码函数，使得 $|\langle u_1, \ldots, u_n\rangle| = 2(|u_1| + \cdots + |u_n| + n)$。

确定性计算 如果计算 $F^w(x)$ 对所有长度小于或等于 $F^w(x)$ 运行时间上界的字都已定义，则称其为确定的。此外，若空间受限计算 $M^w(x)$ 的空间上界为 $p(|x|)$，且对所有长度小于或等于 $p(|x|)$ 的字，w 都已定义，则称其为确定的。若计算是确定的并且接受（分别为拒绝），则称其确定地接受（分别为确定地拒绝）。我们可以将计算组合成更复杂的表达式，并在其中每个单独的计算都是确定的时称这些表达式为确定的。例如，“$F^w(x) \in L(M^w)$ 是确定的”表示 $F^w(x)$ 输出某个 y且是确定的，并且 $M^w(y)$ 是确定的。

枚举。对于任意预言机 O，令$\{F_k^O\}_{k\in\mathbb{N}^+}$ 为多项式时间预言机图灵转导器的一个标准枚举，其中 F_k^O的运行时间恰为 p_k。对于任意预言机 O，令$\{S_k^O\}_{k\in\mathbb{N}^+}$ 表示多项式空间预言机图灵机的一个标准枚举，其中S_k^O的空间上界恰为 p_k。令 t_1，t_2，.....为所有时间可构造函数的一个不一定可计算的枚举。

4.2 谕示构造

对于第 4.2 节，令 $A \subseteq 2\mathbb{N}$ 为任意值。注意，根据 enc 的定义，有 $A \cap 0^* = \emptyset$。

相对化的 PSPACE 完全集。

▶ **定义 15** (PSPACE^O 完全集)。 对于所有预言机 O，定义

$$K^O := \{\langle 0^i, 0^t, x\rangle \mid i,t \in \mathbb{N}^+, x \in \Sigma^* \text{ and } S_i^O(x) \text{ accepts using space} \leq t\}.$$

此外，固定 κ 为满足 $L(S_\kappa^O) = K^O$的第一个图灵机 S_κ 的编号。

▶**观察 16**。 对于所有预言机 O， K^O 都是 PSPACE^O-完全的。

注意，任何计算 $S_\kappa^O(\langle 0^i, 0^t, x\rangle)$只依赖长度至多为 t的预言机字。

PSPACE 完全集的码字。 对于图灵机 F_k 和 $n \in \mathbb{N}$，我们希望对如下事实进行编码：“F_k^O是一个可靠证明系统，可用于处理长度为 n的输入上的 K^O ”。我们对这些编码进行填充，使得某些计算无法查询到它们。

▶**定义 17** （ K^O的码字）。 定义

$$c_K \colon \mathbb{N}^+ \times \mathbb{N} \to \Sigma^*, \quad c_K(k,n) := 0^w \text{ where } w = \langle 0, k, n, p_k(n)\rangle.$$

▶ **观察 18**。 对于固定的 k，函数 $n \mapsto c_K(k,n)$ 关于 n 是多项式时间可计算的。

▶ **观察 19**。 对于 $k \in \mathbb{N}^+$ 和 $O \subseteq \Sigma^*$， $S_\kappa^O(F_k^O(x))$ 不依赖于长度为 $\geq |c_K(k,|x|)|$ 的字。

任意复杂集合的码字。 相对于我们的预言机，我们希望任意复杂集合都存在 p-最优证明系统。我们使用第二种类型的码字来定义这些集合。

▶**定义 20** (任意复杂集合的码字)。 定义

$$c_L \colon \mathbb{N}^+ \times \mathbb{N} \to \Sigma^*, \quad c_L(i,n) := 0^w \text{ where } w = \langle 1, i, n, t_i(n)\rangle.$$

▶ **定义 21** (任意复杂集合)。 设 $i \in \mathbb{N}^+$ 和 O 为任意预言机。我们定义

$$L_i^O := \{0^n \mid c_L(i,n) \in O\}.$$

对于部分预言机 w，如果 w 对所有长度为 $\leq |c_L(i,|x|)|$ 的字都有定义，则称 $x \in L_i^{w \cup A}$ 或 $x \notin L_i^{w \cup A}$ 是确定的。

直观而言， L_i^O的复杂度取决于 t_i。我们构造预言机，使这一点成立。

▶ **观察 22.** 对于固定的 i，函数 $n \mapsto c_L(i,n)$ 关于 $|c_L(i,n)|$ 是多项式时间可计算的，因为 t_i 是时间可构造的。

▶**观察 23.** c_K 和 c_L 均为全函数、单射且多项式时间可逆，$\mathrm{ran}(c_K) \cap \mathrm{ran}(c_L) = \emptyset$，$\mathrm{ran}(c_K) \cup \mathrm{ran}(c_L) \subseteq 0^*$，并且 $\mathrm{ran}(c_K) \in \mathrm{P}$。

有效预言机。 在构造预言机的过程中，我们依次添加并维护各项要求。这些要求由一个部分函数 $r\colon \mathbb{N}^+ \times \mathbb{N}^+ \mapsto \mathbb{N}$ 指定，称为需求函数。如果预言机 w 满足以下要求，则称其对于需求函数 r 是 r-有效的。

V1 $w \subseteq \mathrm{ran}(c_K) \cup \mathrm{ran}(c_L)$。

（含义：预言机是 TALLY，且只包含码字。）

V2 若 $c_K(k,n) < |w|$，那么 $c_K(k,n) \in w$ 当且仅当对所有 $x \in \Sigma^n$, $F_k^{w\cup A}(x) \in K^{w\cup A}$.
（含义：预言机表示可靠性 o f proof 系统 f或 $K^{w\cup A}$.）

V3 如果 $r(k,\ i) = 0$，那么存在某个 x 使得 $F_k^{w\cup A}(x) \notin L_i^{w\cup A}$是确定的。
（含义：如果 $r(k,\ i) = 0$，那么 F_k 不是相对于 $w \cup A$ 及其所有扩展的 L_i 的证明系统。）

V4 如果 $r(k,\ i) = m > 0$，那么对于所有满足 $x \in L_i^{w\cup A}$的 $|x| > m$，都有 $x_{F_k^{w\cup A}}$未定义或 $p_k(|x_{F_k^{w\cup A}}|) \geq |c_L(i,\ |x|)|$。
（含义：如果 $r(k,\ i) > 0$，那么 F_k 对于来自 L_i 的元素没有短证明。）

V5 对于所有 $i \in \mathbb{N}^+$，都有 $\#L_i^{w\cup A} \geq \#\{k \in \mathbb{N}^+ \mid (k,\ i) \in \mathrm{dom}(r)\}$。
（含义：集合 L_i 所含元素数量达到最小值。）

我们将证明，对于各种预言机和需求函数，V1 到 V5 均成立。为了避免混淆，我们使用记号 V1(w)、V2(w)、V3($w,\ r$)、V4($w,\ r$) 和 V5($w,\ r$) 来明确指出所指的预言机 w 和需求函数 r。

关于 r-有效预言机 以下引理说明了如何扩展 r-有效预言机，使其仍然保持 r-有效。

▶ **引理 24**。如果 w 是一个 r-有效预言机，那么存在 $b \in \{0,1\}$，使得 wb 是 r-有效 d.

证明。令 w 为任意一个 r-有效预言机，并令 $z := |w|$ 为下一个要判定其是否属于该集合的字符串。我们按照以下过程选择 b：

(i) 如果 $z = c_K(k,n)$ 对于某个 $k \in \mathbb{N}^+$ 和 $n \in \mathbb{N}$，且对于所有 $x \in \Sigma^n$ 均有 $F_k^{w\cup A}(x) \in K^{w\cup A}$成立，那么 $b := 1$。**(ii)** 否则，$b := 0$。我们证明 wb 是 r-有效的。

对于 *V1(wb)*：由于 V1(w) 得到满足，因此有 $w \subseteq \mathrm{ran}(c_K) \cup \mathrm{ran}(c_L)$。此外，只有当对某些 k 和 n有 $z = c_K(k,n)$ 时，b 才会被选为 1。因此，$wb \subseteq \mathrm{ran}(c_K) \cup \mathrm{ran}(c_L)$。

对于 *V2(wb)*：V2(w) 成立。根据观察 19，对于任意 $c_K(k,n) < |w|$，它满足：对于所有 $x \in \Sigma^n$, $S_\kappa^{w\cup A}$, $F_k^{w\cup A}(x)$ 仅取决于长度为 $< |c_K(k,n)|$的字。因此，对于此类编码字 $c_K(k,n)$，V2(wb) 仍然成立。

若对于某些 k 和 n，$z = c_K(k,n)$ 成立，那么根据 c_K 的单射性（观察 23），k 和 n 是唯一的。此外，同样根据观察 19，对于所有 $x \in \Sigma^n$ 以及任意 $c \in \{0,1\}$，有

$$S_\kappa^{w\cup A}(F_k^{w\cup A}(x)) = S_\kappa^{wc\cup A}(F_k^{wc\cup A}(x)).$$

Th^us, 情况 (i) 扩展 ds w by adding $c_K(k\ n)$ 精确 ly if and only if 这是必要的 f或 V2 (wb) 。对于 *V3(wb, r)*：由于 V3(w, r) 成立，且相应的计算均有定义，因此对于任意选择的 b, V3(wb, r) 均成立。

对于 V4(wb, r)：设 $r(k,i) = m > 0$，并任取满足 $|x| > m$ 的 $x \in L_i^{w\cup A}$。根据 L_i 的定义，如果 $x \in L_i^{w\cup A}$，那么 $c_L(i,|x|) \in w$。因此，对于所有满足 $p_k(|y|) < |c_L(i,|x|)|$的 y，$||w|| \geq |c_L(i,|x|)|$，且 $F_k^{w\cup A}(y)$ 有定义。根据 V4(w, r)，$x_{F_k^{w\cup A}}$ 无定义，或者 $p_k(|x_{F_k^{w\cup A}}|) \geq |c_L(i,|x|)|$。因此，对于所有满足 $p_k(|y|) < |c_L(i,|x|)|$的 y，$F_k^{wb\cup A}(y) = F_k^{w\cup A}(y) \neq x$。最后，$x_{F_k^{wb\cup A}}$ 无定义，或者 $p_k(|x_{F_k^{wb\cup A}}|) \geq |c_L(i,|x|)|$。这表明，对于所有字 $x \in L_i^{w\cup A}$，V4(wb, r) 均成立。由于 $\mathrm{ran}(c_K)$ 与 $\mathrm{ran}(c_L)$ 不相交（观察 23），若对于某些 i 和 n，$z = c_L(i,n)$，则情形 (ii) 将 w 扩展为 $w0$。因此，$L_i^{wb\cup A} = L_i^{w\cup A}$，且对于 $x \in L_i^{wb\cup A}$ 中的所有字，V4(wb, r) 也成立。

对于 *V5($wb,\ r$)*：由于 V5($w,\ r$) 成立且 $wb \sqsupset w$，V5($wb,\ r$) 也成立。 ◀

以下引理表明，如果我们能够构造一个 r-有效预言机 O，使得 $\mathrm{dom}(r) = \mathbb{N}^+ \times \mathbb{N}^+$，那么 O 就具有所需的性质。

▶ **引理 25.** 设 r 是一个需求函数，满足 $\mathrm{dom}(r) = \mathbb{N}^+ \times \mathbb{N}^+$，并设 O 是一个r-有效预言机。则下列结论成立：

(i) $O \in \mathrm{TALLY}$。**(ii)** $K^{O\oplus A}$ 具有 p-最优证明系统。**(iii)** 对所有 $i \in \mathbb{N}^+$，$L_i^{O\oplus A}$具有 p-最优证明系统。**(iv)** 对任意时间可构造函数 t，存在某个 $L_i^{O\oplus A} \notin \mathrm{DTIME}^{O\oplus A}(t)$。

证明。 对 *(i)*：由 V1(O) 与观察 23 可得。

To (ii):

设 f 是 $K^{O\oplus A}$ 的任意证明系统。定义

$$h(x) := \begin{cases} F_k^{O\oplus A}(x') & \text{if } x = \langle x', c_K(k, |x'|)\rangle \text{ and } c_K(k,|x'|) \in O \\ f(x') & \text{if } x = \langle x', 1\rangle \\ f(0) & \text{otherwise} \end{cases}$$

▷ 断言 26. $h \in \mathrm{FP}^{O\oplus A}$.

证明。 编码 $\langle\rangle$ 是多项式时间可逆的，$\mathrm{ran}(c_K) \in \mathrm{P}$ 且 c_K 是多项式时间可逆的（观察 23）。如果输入的第二部分是一个码字，我们可以在线性时间内查询预言机，并在多项式时间内计算输出，因为在这种情况下，输入长度至少为 $p_k(|x'|)$。◁

▷ 断言 27。$\mathrm{ran}(h) = K^{O\oplus A}$。

证明。 由于定义的第二行 h 保证$\mathrm{ran}(h) \supseteq \mathrm{ran}(f)$ 且 f 是 $K^{O\oplus A}$的证明系统，$\mathrm{ran}(h) \supseteq K^{O\oplus A}$。

如果输入 x 不符合定义第一行的要求 h，那么 h 的输出是 $K^{O\oplus A}$中的一个元素。否则，$x = \langle x', c_K(k, |x'|)\rangle$ 且 $c_K(k, |x'|) \in O$。由 V2(O) 可知，对于所有 $z \in \Sigma^{|x'|}$, $F_k^{O\oplus A}(z) \in K^{O\oplus A}$。因此，$F_k^{O\oplus A}(x') \in K^{O\oplus A}$。这说明 $\mathrm{ran}(h) \subseteq K^{O\oplus A}$。◁

▷ 断言 28。$K^{O\oplus A}$ 的所有证明系统均可被 h多项式模拟。

证明。 设 g 为针对 $K^{O\oplus A}$的任意证明系统。设 $F_k^{O\oplus A}$为计算g的图灵机。考虑如下模拟函数 π：

$$\pi(x) := \langle x, c_K(k, |x|)\rangle$$

根据观察 18，对于固定的 k，我们可以在关于 $|x|$ 的多项式时间内计算 $c_K(k, |x|)$，因此$\pi \in \mathrm{FP}$。此外，成立

$$h(\pi(x)) = h(\langle x, c_K(k, |x|)\rangle) = F_k^{O\oplus A}(x) = g(x).$$

我们必须证明第二个等式成立。根据 $\mathrm{ran}(g) = K^{O\oplus A}$，对于所有 $x \in \Sigma^*$,$F_k^{O\oplus A}(x) \in K^{O\oplus A}$。结合 V2($O$)，这意味着 $c_K(k, n) \in O$ 对于所有 $n \in \mathbb{N}$。因此，$c_K(k, |x|) \in O$，第二个等式成立。◁

命题 26、27 和 28 表明， h 是 $K^{O\cup A}$的 p-最优证明系统。

To (iii):

令 $i \in \mathbb{N}^+$ 为任意对象，并令 a 为 $L_i^{O\cup A}$ 中的任意元素（由 V5(O, r) 且 r 是全函数可知，该元素存在）。定义

$$h(x) := \begin{cases} 0^n & \text{if } x = c_L(i,n) \in O \\ a & \text{otherwise} \end{cases}$$

由于根据 V1(O)， $O \subseteq \mathrm{ran}(c_K) \cup \mathrm{ran}(c_L)$ 且 $\mathrm{ran}(c_K) \in \mathrm{P}$（观察 23），我们可以在多项式时间内检查第 1 行。由于我们可以从 $c_L(i, n)$ 计算出 0^n，因此得到 $h \in \mathrm{FP}^{O\cup A}$。此外，$\mathrm{ran}(h) = L_i^{O\cup A}$，因为 $a \in L_i^{O\cup A}$，并且第一行符合 $L_i^{O\cup A}$的定义。因此， h是 $L_i^{O\cup A}$的证明系统。

剩下要证明的是 h 是 p-最优的。令 g 为 $L_i^{O\cup A}$的任意证明系统。令 $F_k^{O\cup A}$ 为计算 g 的图灵机。考虑以下模拟函数 π:

$$\pi(x) := c_L(i, |F_k^{O\cup A}(x)|)$$

由于 $L_i^{O\cup A} \in \mathrm{TALLY}$ 且 $F_k^{O\cup A}$是 $L_i^{O\cup A}$的证明系统，因此对所有 x均成立

$$F_k^{O\cup A}(x) = 0^{|F_k^{O\cup A}(x)|} \in L_i^{O\cup A} \quad \text{and} \quad c_L(i, |F_k^{O\cup A}(x)|) \in O.$$

利用这一点，我们得到对所有 x均成立

$$h(\pi(x)) = h(c_L(i, |F_k^{O\cup A}(x)|)) = 0^{|F_k^{O\cup A}(x)|} = F_k^{O\cup A}(x) = g(x).$$

剩下需要证明 $\pi \in \mathrm{FP}^{O\cup A}$。根据 $\mathrm{dom}(r) = \mathbb{N}^+ \times \mathbb{N}^+$这一前提条件，可知 $(k, i) \in \mathrm{dom}(r)$。此外， $r(k, i) = m > 0$，因为否则根据 V3(O, r)，存在某个 x 使得 $F_k^{O\cup A}(x) \notin L_i^{O\cup A}$，这与 $F_k^{O\cup A}$是 $L_i^{O\cup A}$的证明系统相矛盾。根据 V4(O, r)，对于满足 $|y| > m$ 的 $y \in L_i^{O\cup A}$，有 $p_k(|y_{F_k^{O\cup A}}|) \geq |c_L(i, |y|)|$。我们利用这一点来界定 π的复杂度。

令 x为任意对象。若 $|F_k^{O\cup A}(x)| \leq m$，则 $c_L(i, |F_k^{O\cup A}(x)|)$ 由某个常数界定，因为这样的编码字只有有限多个。否则，令 $y := F_k^{O\cup A}(x)$，且$|y| > m$。于是有

$$p_k(|x|) \geq p_k(|y_{F_k^{O\cup A}}|) \geq |c_L(i, |y|)|.$$

因此， $c_L(i, |F_k^{O\cup A}(x)|)$至多比 $|x|$长一个多项式因子。由于 $x \mapsto |F_k^{O\cup A}(x)|$ 可以在 $|x|$ 的多项式时间内计算，且 $|F_k^{O\cup A}(x)| \mapsto c_L(i, |F_k^{O\cup A}(x)|)$可以在 $|c_L(i, |F_k^{O\cup A}(x)|)|$ 的多项式时间内计算（观察 22），因此我们可以在 $|x|$的多项式时间内计算 $x \mapsto c_L(i, |F_k^{O\cup A}(x)|)$。于是， $\pi \in \mathrm{FP}^{O\cup A}$ 和 h 是 p-最优的。

To (iv):

首先，我们必须证明，对于所有 $i \in \mathbb{N}^+$， $L_i^{O\cup A}$都不是有限的。

▷ 断言 29。对于所有 $i \in \mathbb{N}^+$，都有 $\#L_i^{O\cup A} = \infty$。

证明。 由 V5(O, r) 和 $\mathrm{dom}(r) = \mathbb{N}^+ \times \mathbb{N}^+$。 ◁

令 t 为任意时间可构造函数，并令 $t' := 2^t$。那么 t' 也是时间可构造的，因此存在某个 i，使得 $t' = t_i$。

假设 $L_i^{O\cup A} \in \mathrm{DTIME}^{O\cup A}(t)$，且由图灵机 $M^{O\cup A}$ 实现。令 a 为 $L_i^{O\cup A}$ 中的任意一个元素（根据断言 29，这样的元素存在）。考虑以下证明系统 g:

$$g(x) := \begin{cases} y & \text{if } x \text{ is an accepting computation path of } M^{O\cup A}(y) \\ a & \text{otherwise} \end{cases}$$

由于根据假设，$M^{O\cup A}$ 在时间 $O(t)$ 内判定 $L_i^{O\cup A}$，因此 g 拥有长度为 $\leq c \cdot t$ 的$L_i^{O\cup A}$中各元素的证明，其中 c为某个常数。根据 (iii)，$L_i^{O\cup A}$拥有一个 p-最优证明系统 h，对于几乎所有 $x \in L_i^{O\cup A}$，该系统都有长度为 $|c_L(i,|x|)| \geq t_i(|x|)$ 的证明。由于 h 是一个 p-最优证明系统，h 通过某个 $\pi \in \mathrm{FP}^{O\cup A}$ p-模拟 g。令 p 表示 π的运行时间多项式。于是，π 至多将证明长度增加 p。这与 h的 p-最优性矛盾，因为 $\#L_i^{O\cup A} = \infty$ （断言 29），因此 h 无穷多次拥有长度为 $\geq t_i$的证明。由于存在某个 m，使得对于所有 $n \geq m$ 都有

$$p(c \cdot t(n)) < 2^{t(n)} = t_i(n),$$

π 无法将所有 g-证明转换为 h-证明。因此，$L_i^{O\cup A} \notin \mathrm{DTIME}^{O\cup A}(t)$。 ◀

本节的剩余部分讨论一个全函数需求函数r 以及一个 r-有效预言机的构造。

谕示构造。该谕示构造将处理以下任务集合$\{\tau_{k,i} \mid k,i \in \mathbb{N}^+\}$。设 T 为这些任务的一个枚举。在每一步中，我们按 T指定的顺序处理最小的任务，并在处理完一个任务后将其从 T中移除。

在第 $s = 0$ 步，我们将 $w_0 := \varepsilon$ 和 r_0 定义为处处无定义的需求函数。在第 $s > 0$ 步，我们通过处理 T 中最早的任务并将其从 T中移除来定义 $w_s \sqsupseteq w_{s-1}$ 和 $r_s \sqsupseteq r_{s-1}$，使得 w_s 是 r_s-有效的。我们按照以下过程进行:

任务$\tau_{k,i}$: 设 $r^0 := r_{s-1} \cup \{(k,i) \mapsto 0\}$。若存在一个 r^0-有效的部分预言机 $v \sqsupseteq w_{s-1}$，则令 $r_s := r^0$ 且 $w_s := v$。
否则，$n \in \mathbb{N}$ 使得 $c_L(i,n)$是w_{s-1} 尚未定义的字典序最小码字。通过引理 24将 w_{s-1} 扩展至 v，使得 $|v| = c_L(i,n)$。令$w_s := v1$ 且 $r_s := r_{s-1} \cup \{(k,i) \mapsto ||w_s|| + 1\}$。

（含义：尝试扩展预言机，使得 F_k 不是 L_i的证明系统。若无法做到，则强制 F_k 对来自 L_i的元素不具有短证明。无论哪种情况，L_i 都会获得一个额外元素。）

该过程产生两个序列 $w_0, w_1, \ldots$ 和 $r_0, r_1, \ldots$，由此我们定义期望谕示及其关联的需求函数。

▶ **定义30**（期望谕示）。定义 $O := \bigcup_{s\in\mathbb{N}} w_s$ 和 $r := \bigcup_{s\in\mathbb{N}} r_s$。

以下断言表明 O 和 r 是良定义的，且 O 是 r-有效的。

▷ 断言31。O 和 r 是良定义的，O 对来自 Σ^* 且属于 $\mathrm{dom}(r) = \mathbb{N}^+ \times \mathbb{N}^+$的所有字都有定义。

证明。对于所有 $s \in \mathbb{N}$，我们证明 $w_{s+1} \sqsupseteq w_s$、$r_{s+1} \sqsupseteq r_s$以及 $\mathrm{dom}(r) = \mathbb{N}^+ \times \mathbb{N}^+$，由此可得该断言。

令 $s \in \mathbb{N}$ 为任意对象，$\tau_{k,\,i}$ 为在步骤 $s+1$ 中处理的任务。在步骤 $s+1$ 处理任意任务时，w_s 至少扩展一个比特，并且会为（k，i）定义 r_s。枚举 T 不包含重复任务；当某个任务被处理时，它会在同一步骤中从 T 中移除。因此，r_s 不可能已经为（k，i）定义。此外，T 中的每个任务都会被处理一次，因此 $\mathrm{dom}(r) = \mathbb{N}^+ \times \mathbb{N}^+$。◁

▷ 断言32。对于每个 $s \in \mathbb{N}$，都有 w_s 是 r_s-有效的。

证明。 注意到 V1(w_0) 和 V2(w_0) 均得到满足，而 V3(w_0, r_0)、V4(w_0, r_0) 和 V5(w_0, r_0) 不需要任何条件。

令 $s \in \mathbb{N}^+$ 为任意对象。根据归纳假设，w_{s-1} 是 r_{s-1}-有效的。令 $\tau_{k,i}$ 为在第 s 步处理的任务。

或者，w_s 被选为 r_s-有效。否则，通过引理 24，w_{s-1} 被扩展为 v，从而 v 变为 r_{s-1}-有效。

▷ 断言 33。 w_s 是 r_{s-1}-有效的。

证明。 由于 $|v| \in \mathrm{ran}(c_L)$，V1($w_s$) 得到满足。使用与引理 24 中相同的论证，并且 $\mathrm{ran}(c_L)$ 与 $\mathrm{ran}(c_K)$不相交，V2(w_s) 也得到满足。正如引理 24 中所论证的，V3(w_s, r_{s-1}) 和 V5(w_s, r_{s-1}) 仍然得到满足，因为预言机只是在扩展。

对于 V4(w_s, r_{s-1})，我们使用反证法。假设 V4(w_s, r_{s-1}) 被违反。由于 V4(v, r_{s-1}) 未被违反，不存在 $x \in L_j^{w_s \cup A}$（满足 $c_L(j, |x|) < |v|$）是该违反的见证，否则针对 x 的相应最短证明将足够长，以至于依赖于长度为 $||v|| \geq |c_L(j, |x|)|$ 的字。这与该证明不能依赖于$c_L(j, |x|)$（在违反 V4(w_s, r_{s-1}) 时）相矛盾。

因此，只有 0^n（满足 $c_L(i, n) := |v|$）才能成为这样的见证。更精确地说，存在某个 ℓ，使得 $r_{s-1}(\ell, i) = m > 0$、$n > m$，并且 $p_\ell(|0^n_{F_\ell^{w_s \cup A}}|) < |c_L(i, n)|$。我们证明，在步骤$s' < s$ 的谕示构造中，当处理任务 $\tau_{\ell,i}$ 时，该构造本会将 $w_{s'-1}$ 扩展至 $v0$，并将 $r_{s'-1}$ 扩展至 $r^0 = r_{s'-1} \cup \{(\ell, i) \mapsto 0\}$，从而与 $r_{s-1}(\ell, i) > 0$ 相矛盾。

根据引理 24，$v0$ 是 r_{s-1}-有效的，因此也是 $r_{s'-1}$-有效的。此外，$c_L(i, n) \notin v0$，所以 $0^n \notin L_i^{v0 \cup A}$。由

$$p_\ell(|0^n_{F_\ell^{w_s \cup A}}|) < |c_L(i, n)| = ||v|| \leq ||v0|| = ||w_s||,$$

此可知

$$0^n_{F_\ell^{w_s \cup A}} = 0^n_{F_\ell^{v0 \cup A}}.$$

因此，存在某个 x（即 $0^n_{F_\ell^{v0 \cup A}}$），使得 $F_\ell^{v0 \cup A}(x) = 0^n \notin L_i^{v0 \cup A}$，而这是确定的。consequently，V3($v0, r^0$) 对于（$\ell, i$）成立。因此，$v0$ 是 r^0-有效的。在步骤 s'中，谕示构造本应选择 $v0 \sqsupseteq w_{s'-1}$ 和 $r^0 = r_{s'-1} \cup \{(\ell, i) \mapsto 0\}$，而不是 $w_{s'}$ 和$r_{s'}$，其中 $r_{s'}(\ell, i) > 0$，这与 $r_{s-1} \sqsupseteq r_{s'}$矛盾。这表明V4($w_s, r_{s-1}$)也成立。◁

还需证明 w_s 甚至是 r_s-有效的。由于 $r_s(k, i) > ||w_s||$，我们只需论证 V4(w_s, r_s) 和 V5(w_s, r_s)。由于 $L_i^{w_s \cup A}$ 不包含长度为 $> ||w_s||$的词，从 V4(w_s, r_{s-1}) 转到 V4(w_s, r_s) 不会造成任何区别。由于 w_s 被选为满足 $c_L(i, n) = |v|$的 $v1$，因此

$$\begin{aligned} \#L_i^{w_s \cup A} &\geq \#L_i^{w_{s-1} \cup A} + 1 \geq \#\{k \in \mathbb{N}^+ \mid (k, i) \in \mathrm{dom}(r_{s-1})\} + 1 \\ &= \#\{k \in \mathbb{N}^+ \mid (k, i) \in \mathrm{dom}(r_s)\}. \end{aligned}$$

因此，V5(w_s, r_s) 成立，故 w_s 是 r_s-有效的。 ◁

▷断言 34。 O 是 r-有效的。

证明。 直观地说， O 和 r 若违反 V1 至 V5 中的任一条件，就会与断言32矛盾，也就是说， w_s 对所有 r_s都是 $s \in \mathbb{N}$-有效的。

对于 *V1(O)*：假设存在某个 $a \notin \text{ran}(c_K) \cup \text{ran}(c_L)$，使得 $a \in O$，那么对于某个 $s \in \mathbb{N}$， $a \in w_s$。因此，V1(w_s) 不会成立，这与断言32矛盾。

对于 *V2(O)*：假设存在 k 和 n，使得 $c_K(k, n) \notin O$ 当且仅当对于所有$x \in \Sigma^n$， $F_k^{O \cup A}(x) \in K^{O \cup A}$，那么考虑某个预言机 w_s，使得 $||w_s|| > |c_K(k, n)|$。根据观察 19， $S_\kappa^{O \cup A}(F_k^{O \cup A}(x))$ 只查询长度为 $< |c_K(k, n)|$ 的字。因此， $c_K(k, n) \notin w_s$ 当且仅当对于所有 $x \in \Sigma^n$， $F_k^{w_s \cup A}(x) \in K^{w_s \cup A}$，这与 w_s 是 r_s-有效的说法矛盾。

对于 *V3(O, r)*：如果 $r(k, i) = 0$，令 s 为处理任务 $\tau_{k,i}$ 的谕示构造步骤。由于 w_s 是 r_s-有效的，存在某个 x，使得 $F_k^{w_s \cup A}(x) \notin L_i^{w_s \cup A}$ 是确定的。因此， $F_k^{O \cup A}(x) \notin L_i^{O \cup A}$，这表明 V3($O, r$) 得到满足。

对于 *V4(O, r)*：假设 $r(k, i) = m > 0$，且存在某个 $x \in L_i^{O \cup A}$，满足$|x| > m$，使得 $p_k(|x_{F_k^{O \cup A}}|) < |c_L(i, |x|)|$。考虑第一个满足以下条件的步骤 s： $r_s(k, i) = m$，且$||w_s|| > |c_L(i, |x|)|$。此时 $x \in L_i^{w_s \cup A}$ 是确定的。此外， $x_{F_k^{O \cup A}} = x_{F_k^{w_s \cup A}}$，因为对于长度为 $\leq p_k(|x_{F_k^{O \cup A}}|)$ 的字， O 和 w_s 的行为相同。因此，V4(w_s, r_s) 未得到满足，这与断言 32 矛盾。

对 *V5(O, r)*：假设存在一个 i，使得 $\#L_i^{O \cup A} < \#\{k \in \mathbb{N}^+ \mid (k, i) \in \text{dom}(r)\}$。根据断言31，$\text{dom}(r) = \mathbb{N}^+ \times \mathbb{N}^+$，因此对于某个 $c \in \mathbb{N}$，有 $\#L_i^{O \cup A} = c$。令 s 为所有任务 $\tau_{1,i}, \tau_{2,i}, \ldots, \tau_{c+1,i}$ 均已处理之后的步骤。根据 V5(w_s, r_s)，有

$$\#L_i^{w_s \cup A} \geq \#\{k \in \mathbb{N}^+ \mid (k, i) \in \text{dom}(r_s)\} \geq c + 1.$$

由于 $O \sqsupseteq w_s$， $\#L_i^{O \cup A} \geq \#L_i^{w_s \cup A} \geq c + 1$，矛盾。 ◁

4.3 谕示构造的结果

本节令 S 为以下命题:

S :=“PSPACE 中的所有集合都有 p-最优证明系统，并且存在具有 p-最优证明系统的任意复杂度的集合。”

▶ **定理35**。 令 $A \subseteq 2\mathbb{N}$ 任意。存在一个预言机 O，它按照$\text{construct}_{\text{TALLY}}(\neg S, A)$构造。

证明。 考虑定义30中的预言机 O。根据断言31和34以及引理 25，$O \in \text{TALLY}$ 和命题 S 相对于 $O \cup A$成立，即 $\neg S$ 相对于 $O \cup A$不成立。注意， $A \subseteq 2\mathbb{N}$ 且 $O \subseteq 2\mathbb{N} + 1$，因此在这种情况下， $\cup$ 可用作标记并 $\oplus$。 ◀

▶ **推论36**。 存在一个预言机 $O \in$，相对于该预言机，*TALLY* PSPACE^O 中的所有集合都有 *p*-最优证明系统，并且存在具有 *p*-最优证明系统的任意复杂度的集合。

证明。 由定理35可得 $A = \emptyset$。 ◀

▶**推论37**。 设 S' 为定理*6*、*9*和*10*中的任意一个命题。那么，存在一个预言机，使得命题 S 和 S' 同时成立。

证明。 定理6、9和10的所有命题，要么相对于 A_{Yao} 多项式时间层级是无限的预言机成立，要么相对于 A_{BGS} 满足 $\text{P} = \text{PSPACE}$的预言机成立。不失一般性，A_{Yao}， $A_{\text{BGS}} \subseteq 2\mathbb{N}$。于是，根据定理 8、定理 8 的 TALLY版本以及定理35，存在一个预言机，相对于它 S' 和 S 成立。 ◀

▶**推论 38**。 存在一个预言机 O_2 ，相对于它，多项式层级^{O_2} 是无限的，PSPACE^{O_2} 中的所有集合都有 p-最优证明系统，并且存在任意复杂度的集合拥有 p-最优证明系统。

▶**推论 39.** 一个无限的多项式层级 并不能通过相对化同时推出 *Q1*、*Q2* 和 *Q3* 的否定答案。

5 结论和开放问题

SPARSE-相对化框架是一种简单而实用的工具，可借助稀疏预言机获得更强的证明障碍。利用这一框架，我们能够构造预言机，将关于复杂性类的猜想与关于最优证明系统及 p-最优证明系统存在性的猜想区分开来。

SPARSE-相对化框架的一个关键组成部分是稀疏预言机独立命题，因为构造合适的稀疏预言机时，这些命题是我们可以“免费”得到的。因此，我们关注对以下任务的贡献。

T1：寻找更多对 tally 预言机和稀疏预言机独立的命题

如第 3 节所述，将 SPARSE 相对化框架限制为 SPARSE ∩ EXPH 后，我们可以得到更强的证明障碍。因此，我们也鼓励大家探究以下任务。

T2：构造 EXPH 可计算的预言机，使得相对于这些预言机，稀疏预言机独立和 tally 谕示无关的命题成立

特别值得关注的是，构造一个 EXPH 可计算的预言机，使得相对于该预言机，多项式时间层次是无限的。

参考文献

AB09 Sanjeev Arora 和 Boaz Barak。《计算复杂性：一种现代方法》。美国剑桥大学出版社，第1版，2009年。BBS86 Jose L. Balcázar、Ronald V. Book 和 Uwe Schöning。多项式时间层次与稀疏预言机。《ACM 杂志》，33(3):603–617，1986年5月。BCS95 Daniel P. Bovet、Pierluigi Crescenzi 和 Riccardo Silvestri。复杂性类与稀疏预言机。《计算机与系统科学杂志》，50(3):382–390，1995年。BGS75 Theodore P. 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。BKM09 Olaf Beyersdorff、Johannes Köbler 和 Jochen Messner。非确定性函数与最优证明系统的存在性。《理论计算机科学》，410(38):3839–3855，2009年。BKM11 Olaf Beyersdorff、Johannes Köbler 和 Sebastian Müller。接受建议的证明系统。《信息与计算》，209(3):320–332，2011年。Boo94 Ronald V. Book。关于多项式时间层次的坍缩。《信息处理快报》，52(5):235–237，1994年。Bus96 Sam R. Buss。证明论讲义。技术报告 SOCS 96.1，麦吉尔大学，1996年。CFM14 Yijia Chen、Jörg Flum 和 Moritz Müller。算法与证明系统的困难实例。《ACM 计算理论汇刊》，6(2)，2014年5月。CK07 Stephen A. Cook 和 Jan Krajíček。NP ⊆ P/poly 可证性的推论。《符号逻辑杂志》，72(4):1353–1371，2007年。

CR79 Stephen A. Cook 和 Robert A. Reckhow。命题证明系统的相对效率。《符号逻辑杂志》，44:36–50，1979年。DEG24 David Dingel、Fabian Egidy 和 Christian Glaßer。一个没有 UP 完全集的预言机，但 NP = PSPACE。在第49届计算机科学数学基础国际研讨会（MFCS 2024）上，卷306，页50:1–50:17，德国达格斯图尔，2024年。Schloss Dagstuhl – Leibniz-Zentrum für Informatik。DG20 Titus Dose 和 Christian Glaßer。NP 完全性、证明系统与不相交 NP 对。载于 C. Paul 和 M. Bläser 编，第37届计算机科学理论方面国际研讨会（STACS 2020），2020年3月10–13日，法国蒙彼利埃，LIPIcs 第154卷，页9:1–9:18。Schloss Dagstuhl – Leibniz-Zentrum für Informatik，2020年。Dos20a Titus Dose。有限域中不完备性猜想的更多分离预言机。《理论计算机科学》，847:76–94，2020年。Dos20b Titus Dose。一个分离有限域中不完备性猜想的预言机。《理论计算机科学》，809:466–481，2020年。EEG22 Anton Ehrmanntraut、Fabian Egidy 和 Christian Glaßer。一个满足 P =NP ∩ coNP、但在 UP、DisjNP 和 DisjCoNP 中不存在多对一完全性的预言机。载于 S. Szeider、R. Ganian 和 A. Silva 编，第47届计算机科学数学基础国际研讨会（MFCS 2022），莱布尼茨信息学国际会议论文集（LIPIcs）第241卷，页45:1–45:15，德国达格斯图尔，2022年。Schloss Dagstuhl – Leibniz-Zentrum für Informatik。EG25 Fabian Egidy 和 Christian Glaßer。复杂集合的最优证明系统难以找到。载于第57届 ACM 计算理论年度研讨会论文集，STOC ’25，页1329–1340，美国纽约州纽约市，2025年。计算机协会。For99 Lance Fortnow。具有无限层级的相对化世界。《信息处理快报》，69(4):309–313，1999年。FS88 Lance Fortnow 和 Michael Sipser。是否存在针对 co-NP 语言的交互式协议？《信息处理快报》，28(5):249–251，1988年。GSSZ04 Christian Glaßer、Alan L. Selman、Samik Sengupta 和 Liyu Zhang。不相交 NP 对。SIAM 计算杂志，33(6):1369–1416，2004年。Hås89 Johan Håstad。小深度电路的近乎最优下界。载于 S. Micali 编，《随机性与计算》，计算研究进展第5卷，页143–170。JAI Press，格林尼治，1989年。HLR23 Shuichi Hirahara、Zhenjian Lu 和 Hanlin Ren。有界相对化。载于 Amnon Ta-Shma 编，第38届计算复杂性会议（CCC 2023），莱布尼茨信息学国际会议论文集（LIPIcs）第264卷，页6:1–6:45，德国达格斯图尔，2023年。Schloss Dagstuhl – Leibniz-Zentrum für Informatik。HRST17 Johan Håstad、Benjamin Rossman、Rocco A. Servedio 和 Li-Yang Tan。布尔电路的平均情形深度层级定理。《ACM期刊》，64(5)，2017年8月。HSS21 John M. Hitchcock、Adewale Sekoni 和 Hadi Shafei。多项式时间随机预言机与复杂性类的分离。《ACM 计算理论汇刊》，13(1)，2021年1月。Kha22 Erfan Khaniki。有限域中不完备性猜想的新关系与分离。《符号逻辑杂志》，87(3):912–937，2022年。KL80 Richard M. Karp 和 Richard J. Lipton。非一致复杂性类与一致复杂性类之间的一些联系。载于计算理论研讨会，STOC ’80，页302–309，美国纽约州纽约市，1980年。ACM。KM98 Johannes Köbler 和 Jochen Messner。通过测试集的最优证明系统为承诺类提供完备问题。载于第13届 IEEE 计算复杂性年度会议论文集，页132–140，1998年。KMT03 Johannes Köbler、Jochen Messner 和 Jacobo Torán。最优证明系统蕴含承诺类的完全集。《信息与计算》，184(1):71–92，2003年。Ko89 Ker-I Ko。恰有 k 层的相对化多项式时间层次。SIAM 计算杂志，18(2):392–408，1989年。

22 SPARSE相对化框架与最优证明系统

KP89 Jan Krajíček 和 Pavel Pudlák。命题证明系统、一阶理论的一致性与计算复杂性。符号逻辑杂志，54：1063–1079，1989年。KSTT92 Johannes Köbler、Uwe Schöning、户田诚之助和 Jacobo Torán。具有少量接受计算的图灵机与 PP 的低集合。《计算机与系统科学杂志》，44(2)：272–286，1992年。LS86 Timothy J. Long 和 Alan L. Selman。利用稀疏预言机对复杂性类进行相对化。ACM期刊，33(3)：618–627，1986年。Lut97 Jack H. Lutz。指数时间的定量结构，第225–260页。Springer-Verlag，柏林，海德堡，1997年。Mes99 Jochen Messner。关于最优算法和最优证明系统。载于《计算机科学理论专题研讨会》，第541–550页，柏林，海德堡，1999年。Springer-Verlag。Mes00 Jochen Messner。关于证明系统的模拟序。博士论文，乌尔姆大学，2000年。Pud17 Pavel Pudlák。有限域中的不完备性。《符号逻辑通报》，23(4)：405–441，2017年。Raz94 Alexander Razborov。关于可证明不相交的 NP 对。技术报告 TR94-006，《计算复杂性电子讨论会》，1994年。Sad97 Zenon Sadowski。关于一个最优量化命题证明系统及一个 NP ∩ coNP 的完全语言。载于《计算理论基础》，第1279卷，第423–428页。Springer，1997年。Sad99 Zenon Sadowski。关于一个 SAT 的最优确定性算法。载于《计算机科学逻辑》，第179–187页，柏林，海德堡，1999年。Springer-Verlag。Sha92 阿迪·沙米尔。IP = PSPACE。《ACM期刊》，39(4)：869–877，1992年10月。Sim77 István Simon。关于某些次递归可归约性。博士论文，斯坦福大学，1977年。Yao85 姚期智。利用预言机分离多项式时间层级。载于《第26届计算机科学基础年度研讨会论文集》，SFCS ’85，第1–10页，美国，1985年。IEEE计算机学会。