arXiv:2301.07123v1 [cs.CC] 17 Jan 2023

多项式时间选择公理与多项式时间基数

谨以此文缅怀 Alan L. Selman

Joshua A. Grochow

2023年1月19日

摘要

不存在单一且规范的多项式时间版本的选择公理（AC）；在策梅洛-弗兰克尔（ZF）集合论中等价的若干选择公理表述，从构造主义的角度看早已并不等价，从复杂性理论的角度看也同样如此。本文表明，将许多经典的选择公理表述以自然的方式限制在多项式时间范围内后，它们便等价于标准的复杂性理论假设，其中包括 Selman 曾关注的若干假设。这为这些假设提供了统一的视角，我们也希望能借此进一步激发人们对本文涉及的一些较不为人知的假设的研究兴趣。

此外，由于若干经典的选择公理形式是用基数来表述的，我们发展了一套多项式时间基数理论。Nerode & Remmel（Contemp. Math. 106, 1990年；Springer Lec. Notes Math. 1432, 1990年）发展了相关理论，但其研究范围仅限于一元集合。Downey（Math. Reviews MR1071525）指出，在更大的字母表上建立这类理论，或许能与更标准的复杂性问题产生有趣的联系；本文将展示其中的一些联系。

选择公理、基数与复杂性问题之间的联系，也使我们得以着重介绍 Selman 的一些研究成果。我们希望本文更像是一个开端，而非终点：引入新的概念，并提出许多有待进一步研究的新问题。

1 引言

> “选择公理显然为真，良序原理显然为假，而谁又说得清佐恩引理呢？”——Jerry L. Bona，[56, 第 145] 页

选择公理（AC）的诸多等价表述之一是：对于每个由非空集合组成的族 $(X_i)_{i\in I}$（其中 I 是任意指标集），都存在一个“选择函数” $x\colon I \to \bigcup_{i\in I} X_i$，使得对所有 i，$x(i) \in X_i$。尽管这一公理并非构造性的，但它在数学的许多领域都极为有用。在经典的策梅洛–弗兰克尔集合论（ZF）中，有许多命题与选择公理等价。关于经典选择公理及其诸多等价形式，我们请读者参阅 Herrlich [38]以及 Rubin 和 Rubin [54, 55] 的著作。然而，尽管这些表述在 ZF 中彼此等价，许多版本给人的“感觉”往往不同，正如 Bona 在上面的引文中所精妙表达的那样。

本文研究了若干在经典意义上与选择公理等价的命题，并提出了若干多项式时间类比；在标准复杂性假设下，这些类比似乎彼此并不等价。我们阐明了它们与一些标准的、以及一些不那么标准的复杂性问题之间的关系，其中大多数问题都与 Alan Selman 的研究有关，这也是我们认为将本文收入这部纪念文集颇为合适的原因之一。

> 非正式定义。多项式时间选择公理是指任何这样一种命题：S 如果从S中删去“多项式时间”、“多项式有界”等类似措辞，那么它在策梅洛-弗兰克尔集合论中将与通常的选择公理等价。

在本文中，我们的总体理念是：“集合”应变为“P 中的语言”，“函数”应变为“FP 中的函数”。当存在多种显而易见的方式来表述某个标准形式所对应的、与其等价的多项式时间版本选择公理时，我们通常会避免采用显然为真或显然为假的表述。

由于若干在经典意义上与选择公理等价的命题是用基数表述的，我们还在第 4 节中发展了“p-基数”的多项式时间理论。基本思路如下：康托尔的基数概念认为，两个集合具有相同的“大小”，当且仅当它们之间存在双射。因此，类比而言，我们称两个语言 $A \subseteq \Sigma^*, B \subseteq \Gamma^*$ 具有相同的 p-基数，如果存在一个多项式时间可计算且多项式时间可逆的双射，将 A 映到 B。这与 p-同构概念的关键区别在于，p-同构 $A \to B$ 必须由一个全函数、p-可计算且 p-可逆的双射 $f\colon \Sigma^* \to \Gamma^*$ 给出，并满足 $f(A) = B$；而在我们的情形中，我们更关注集合本身，只要求双射在限制于集合 A, B时可在多项式时间内计算且可逆。在这些集合之外，它既不必是单射，也不必是满射。

我们的 p-基数概念最终发现与 Selman 的研究中若干值得关注的复杂性理论概念有关，包括 p-可枚举性（观察 4.15 和命题 4.17）、同构猜想（第 4.2 节）、p-可排名性（第 4.3 节）以及免疫性（命题 4.6 和 4.36）。我们怀疑它还与 Selman 关注的其他问题存在进一步联系，包括不相交 NP 对 [23, 24, 17, 22], 有丝分裂性 [20, 19, 18], 分裂 [21], 以及 p-可选择性[60, 59, 49, 34], ，但这些令人兴奋的方向留待未来探索。

1.1 相关工作

选择公理的构造性版本，即便是在可计算性的背景下，也早已有过研究，例如 [8, 13], 但我们尚未发现其他研究多项式时间类比选择公理的工作。

关于 p-基数，最密切相关的工作是 Nerode & Remmel [51, 52, 53, 50] 的研究。他们不仅建立了多项式时间基数的理论，称为“多项式等价类型”或“PET”（类比于此前研究过的递归等价类型 [11], ，见 [10]），还开始发展多项式时间结构的理论，例如向量空间、群等，类比于可计算结构方面的研究（例如见 [9, 3, 48]）。不过，他们的多项式时间理论是针对一元语言建立的。

虽然选择一元语言使得许多与递归情形的类比得以成立，并由此发展出丰富而有趣的理论，但它与 P 与 NP 问题等更标准的复杂性问题大多脱节，因为后者通常是在大小至少为 2 的字母表上表述的。Downey 在其对 [52] 的评论 [12] 中写道：

> “目前尚不清楚复杂性问题（例如 P $\stackrel{?}{=}$ NP）与 [52] 之间是否存在某种关系。例如，如果能够运用这些技术证明 P $\neq$NP 相对于 [直觉主义策梅洛–弗兰克尔集合论]是独立的，类似于 McCarty 的研究 [46, 45]，那将十分令人着迷。或许需要做的是在标准语言 $\subseteq \{0,1\}^*$上发展这套理论。” –R. Downey [12]

在这里（第 4 节），我们致力于在标准语言上，也就是在大小至少为 2 的字母表上，发展这套理论。虽然我们尚未实现 Downey 关于该理论独立于直觉主义策梅洛–弗兰克尔集合论的设想，但我们为这套理论奠定了一些可能的基础。事实上，本文最初聚焦于选择公理，p-基数只是顺带一提；而正是我们发现了 Downey 的这段引述，才促使我们进一步发展 p-基数理论的一些基础。

1.2 Selman 对我工作的影响

我只在少数几次场合亲自见过 Alan——我想，一次是在我拜访波士顿大学的 Steve Homer 时（当时我做了关于复杂性理论研究的第一次演讲），另一次或两次是在计算复杂性会议上。不过，即使只见过这几次，也能看出他为人友善，乐于分享自己的想法和时间，兴趣广泛，而且似乎真心非常喜欢谈论复杂性理论。

不过，他对我工作的影响远不止我们那几次偶然的会面。总体来说，情况是这样的：我刚开始读研究生时，常和 Lance Fortnow 以及芝加哥大学理论组的其他成员交流（当时的成员有：Stuart Kurtz、Ketan Mulmuley、Janos Simon、Laci Babai；我加入后不久，Sasha Razborov 也加入了），那时我对结构复杂性理论简直着迷。复杂性类的性质、（形式）语言的性质、p-同构、复杂性核心、p-可选择性——这些我全都喜欢（现在也依然如此！）。研究生生涯早期，Selman 主编的两本文集 [62, 37] 对我的思想产生了很大影响。[62] 中的每一章都与我人生中某个阶段研究过的内容有关（即使最终没有发表成果）。它们至今仍是我书架上最喜欢的几本高阶复杂性理论著作——没错，我确实拥有这些实体书，就放在实体书架上。

在撰写我的第一篇复杂性论文时， [16], Lance 向我介绍了 Selman 对函数类的分类法 [64, 63, 65], ，从那篇论文中可以看出，NPMV 及其近亲发挥着重要作用。坦白说：直到读了 Selman 关于 NPMV、NPSV 及其相关函数类的研究，我才真正理解 TFNP 的定义。Selman 的一项结果实际上也是 [16] 的研究动机之一（见我的硕士论文 [28, 第 3.2]节）：尽管大多数函数类的表现都与对应的判定类相似，但我们有 $\mathrm{P}^{\mathrm{NP}[log]}=\mathrm{P}_{tt}^{\mathrm{NP}}$ [31, 68, 7] ；而 Selman 表明，对于相应的函数类，这种情况不太可能成立：

定理 1.1（Selman [64]）。$\mathrm{FP}^{\mathrm{NP}[log]}=\mathrm{FP}_{tt}^{\mathrm{NP}}$ 蕴含 NP = RP 且 P = UP。

写完第一篇复杂性论文后，我便深深着迷了（如果此前还没有的话）。我最喜欢的未解决预言机问题之一，至今仍出自 Selman 的研究。NP = UP 是否会导致 PH 塌缩，至今仍是个开放问题。不仅如此，我们甚至不知道解决它是否需要非相对化技术。我们想在这里特别提出这个问题：

开放问题 1.2（民间传说）。构造一个相对预言机，使得 NP =UP，但 PH 是无限的。

Hemaspaandra、Naik、Ogihara 和 Selman [36]证明了一个密切相关的命题确实会使 PH 塌缩到 $\Sigma_2\mathrm{P}$。具体而言，他们证明，假设 $\mathrm{NPMV}_g \subseteq_c \mathrm{NPSV}_g$，即可推出 PH 塌缩。第 2 节会定义所有术语；但现在我们可以说，后一个命题等价于：对于每个属于 P 的语言 $A \subseteq \Sigma^* \times \Sigma^*$，都存在另一个“细化” A 的语言 B，其含义是，对于所有 $x \in \Sigma^*$，若 $(x,y) \in A$，则存在某个 y_x，使得 $(x,y_x) \in A$，且 (x,y_x) 是 B 中第一坐标为 x 的唯一元素。这意味着 NP =UP，在哲学意味上也让人觉得与之非常接近（事实上，不熟悉这个命题的人可能会误以为它就是 NP =UP 的定义）。研究生期间，我在 Lance 的指导下，至少花了一个夏天，甚至可能更久，试图回答问题 1.2。问题在于，要得到 NP =UP 的大多数朴素思路——我当时肯定很天真，现在大概仍然如此——也会推出 $\mathrm{NPMV}_g \subseteq_c \mathrm{NPSV}_g$，进而得到 PH $= \Sigma_2\mathrm{P}$。为了绕开这一障碍，我们起初尝试构造一个预言机，使得相对该预言机，NP =UP，但 PH $\neq \Sigma_2\mathrm{P}$。我们没能做到这一点，不过我提起此事，是因为这引导我们读到了 Selman 的另一项研究。我们没有尝试完全分离 PH 的各层，因为这似乎需要用到 AC^0 电路下界的全部力量；我们只是试图分离它的第二层，而 Baker 和 Selman 已经构造了一个预言机，只分离 PH 的两层 [4], ，所以我们便从他们的工作中寻找灵感。

此时我已经不记得原因了，但大约在同一时期，我还开始阅读 Selman 关于不相交对、有丝分裂性、免疫性和 p-可选择性的研究（例如， [19, 22, 30, 33, 49]）。事实上，

Selman 关于搜索到判定归约的研究激发了我对这一主题的兴趣。十多年前，我在研究生阶段曾与 Youming Qiao 讨论群同构领域中的这类归约；直到最近，我们才在这个问题上取得进展 [29]。

虽然我们没有解决问题 1.2，但那几个月全身心投入 Selman 的研究，实在是一段无比精彩的时光。它影响了我的思考和职业生涯，也将伴随我一生。谢谢你，Alan——你的思想遗产仍在延续，我们都很怀念你。

2 预备知识

在全文中，Σ（有时也包括 Γ）表示一个大小至少为 2、且至少包含符号 0、1 的有限字母表。ϵ 表示空串，即长度为零的唯一字符串。$|x|$ 表示字符串的长度。长度字典序定义如下：若 $|x| < |y|$，则 Σ；或者若 $|x| = |y|$ 且 x 在字典序中先于 y，则 Σ。其中，字典序依据 Σ上的某个固定（但未指定、隐含的）全序定义。Σ^* 表示字母表 Σ上的所有有限字符串构成的集合。

我们可以在 Σ^* 和 $\mathbb{N}$ 之间自由来回转换，具体如下。与 $x \in \Sigma^*$ 关联的自然数就是满足 $\leq_{lex} x$的字符串数量，反之亦然。例如，若 $\Sigma = \{0,1,2\}$，则有如下对应关系

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	$\cdots$
ϵ	0	1	2	00	01	02	10	11	12	20	21	22	000	001	002	010	011	$\cdots$

对于两个字符串 x、y 和一个自然数 n，当我们写作 $x + y$ 或 $x + n$时，先按照上述约定将所有字符串转换为自然数，再将它们相加，最后在需要时转换回相应的字符串。

对于语言 $A \subseteq \Sigma^*$，我们采用一种记号上的简写：写作 $A(x) = 1$ 当且仅当 $x \in A$，写作 $A(x) = 0$ 当且仅当 $x \notin A$。$\overline{A}$ 表示 A的补集，$\overline{A} = \{x \in \Sigma^* : x \notin A\}$。

从 A 到 B 的多项式时间多对一归约，是指一个 p-可计算的全函数 f，满足对所有 $x \in \Sigma^*$都有 $x \in A \Leftrightarrow f(x) \in B$；等价地，$A(x) = B(f(x))$。此时我们记作 $A \leq_m^p B$。若 $A \leq_m^p B$ 且 $B \leq_m^p A$，则记作 $A \equiv_m^p B$，并称 A 和 B 具有相同的多项式时间多对一度（难度）。有界真值表归约，或称 $\leq_{btt}^p$归约，是一种只进行 $O(1)$ 次查询的非自适应图灵归约（我们仅在提及他人的结果时使用 $\leq_{btt}^p$）。若存在一个全函数、多项式时间可计算的双射 $f\colon \Sigma^* \to \Gamma^*$，其逆函数 f^{-1}也可在多项式时间内计算，且满足 $f(A) = B$，则称 $A \subseteq \Sigma^*$和 $B \subseteq \Gamma^*$ 多项式时间同构，记作 $A \cong^p B$。

对于两个语言 $A, B \subseteq \Sigma^*$, $A \oplus B$ 表示“带标签”的不交并 $\{0a : a \in A\} \cup \{1b : b \in B\}$，而 $A \times B$ 表示通常的笛卡尔积。字符串对、元组等使用任意一种标准的多项式时间可计算且多项式时间可逆的双射 $\Sigma^* \to \Sigma^* \times \Sigma^*$ 进行编码。若它们的对称差（$A \backslash B$）$\cup (B \backslash A)$ 是有限的，我们记作 $A =^* B$。

我们沿用 Selman [64, 36] 所提出的部分多值函数记法。一个（可能是）部分多值函数 f 在技术上是一个关系 $\subseteq \Sigma^* \times \Sigma^*$，但我们将该关系的第一个坐标视为输入，第二个坐标视为输出，并使用标准的函数术语和记法。我们不使用关系记法 xfy，而写作 $f(x) \mapsto y$，但请注意，给定一个 x，这样的 y 可能不止一个（因此，除非对于 $f(x)$ 恰好只有一个输出，否则我们会谨慎地不写作 $f(x) = y$）。我们记作

$$set\text{-}f(x) = \{y : f(x) \mapsto y\} \qquad \text{and} \qquad \mathrm{dom}(f) = \{x : set\text{-}f(x) \neq \emptyset\}.$$

非确定性图灵机转换器——带有独立输出带的机器——自然地计算部分多值函数。给定这样一台机器 M，我们定义 $f_M(x) \mapsto y$当且仅当存在 M 的某个接受计算，该计算停止时其输出带上有 y；我们称 f_M 由 M计算。还有一个与 M 相关但略有不同的函数也很有用，即 $acc_M(x) \mapsto y$ 当且仅当 y 是 M某个接受分支上所作非确定性选择的有序列表；注意，$\mathrm{dom}(f_M) = \mathrm{dom}(acc_M) = L(M)$，即 M 所接受的语言。

稍微滥用通常的函数记号，对于两个部分多值函数 f、g，我们可以写成例如 $f(x, g(x))$，表示部分多值函数 $c(x)$，其中 $c(x) \mapsto z$ 当且仅当存在一个输出 $g(x) \mapsto y$，使得 $f(x, y) \mapsto z$。（这也对应于关系复合。）

我们将非确定性多项式时间机 M 称为“NP 机”。

NPMV 是由 NP 机器计算的（可能是）部分多值函数的类。NPSV 是 NPMV 的子类，由实际上为单值的函数组成，不过它们仍可能是部分函数，也可能有多个接受分支（只要这些分支都产生相同的输出）。PF 是由不使用非确定性的 NP 机器计算的函数的类，不过这些函数仍可能是部分函数（也就是说，它们可能会拒绝某些输入）。FP 是由确定性多项式时间机计算的全函数的类。

若多值函数 f 是多值函数 g 的细化，则对于所有 x，$\mathrm{dom}(f) = \mathrm{dom}(g)$ 且 $set\text{-}f(x) \subseteq set\text{-}g(x)$（第二个条件等价于 $f(x) \mapsto y$ 意味着 $g(x) \mapsto y$）。若 $\mathcal{F}_1, \mathcal{F}_2$ 是两个函数类，我们记作 $\mathcal{F}_1 \subseteq_c \mathcal{F}_2$，表示每个 $f \in \mathcal{F}_1$ 在 $\mathcal{F}_2$ 中都有一个细化。

对于任意函数 f——无论它是否为单射、是否为单值、是否为全函数、是否为满射——我们将 f^{-1} 定义为由 $f^{-1}(y) \mapsto x$ 当且仅当 $f(x) \mapsto y$ 定义的部分多值函数。给定一个函数类 $\mathcal{F}$，若 f 在 $\mathcal{F}$ 中有细化，则称 f 在 $\mathcal{F}$ 中可逆。根据我们的符号约定，请注意，尽管 f^{-1} 可能是部分且多值的，我们始终有 $f^{-1}(f(x)) \mapsto x$。此外，$f(f^{-1}(x)) \mapsto x$ 当且仅当 x 属于 f 的像。

若存在一个多项式 p，使得对于每个输入 x，都存在某个输出 y 满足 $|x| \leq p(|y|)$，则称函数 f 是（多项式）诚实的。请注意，诚实是 f^{-1} 存在某个可在多项式空间中计算的细化（更不用说在多项式时间内计算）所必需的条件。

对于这些函数类，有若干下标可用于表示其子类：

- 下标 t 表示全函数构成的子类，也就是说，其定义域为 Σ^* 的全体
- 下标 h 表示诚实函数构成的子类
- 下标 g 表示图为 $\{(x, y) : f(x) \mapsto y\}$ 的函数所构成的子类，该图可在多项式时间内判定。

这些下标可以任意组合使用，例如 NPMV$_{ght}$。

Selman [64] 以及 Hemaspaandra、Naik、Ogihara 和 Selman [36] 证明了

$$\mathrm{NPSV}_t = \mathrm{FP}^{\mathrm{NP} \cap \mathrm{coNP}}.$$

定理/定义 Q。([14, 定理 2]) 假设 Q 是以下任一等价陈述 s

Q1 对所有接受 Σ^* 的 NP 机 M，都存在一个多项式时间可计算函数 g_M，使得对于所有 x, $g_M(x)$ 都输出 x 上 M 的一条接受计算。

Q2 所有多项式时间可计算的满射诚实函数在多项式时间多值函数类中均可逆。

Q3 NPMV$_t \subseteq_c$FP。

Q4 对所有满足 $S \subseteq$SAT 的 $S \in$ P，都存在一个多项式时间可计算的 g，使得对于所有 $x \in S$, $g(x)$ 都输出 x 的一个满足赋值。

Q5 P $=$ NP $\cap$ coNP 和 NPMV$_t \subseteq_c$ NPSV$_t$。

Q6 对于所有满足 $L(M) =$ SAT 的 NP 机 M，存在一个 $f_M \in$ 多项式时间多值函数，使得对于所有 $\varphi \in$ SAT，$\varphi(f_M(\varphi, acc_M(\varphi))) = 1$；也就是说，$f_M$ 接收 φ 以及 M 在 φ 上的任意一个接受计算，并至少输出一个 φ 的满足赋值，且所有此类输出都满足 φ。

Q7 对于所有满足 $L(M) \subseteq L(N)$ 的 NP 机 M, N，存在一个 $f_M \in$多项式时间多值函数，使得对于所有$x \in L(M)$，$f_M(x, acc_M(x))$ 都会产生某个输出，且其所有输出都是 $N(x)$ 的接受计算。

Q8 对所有 $L \in$ P 和所有接受 L 的 NP 机 M，都存在一个多项式时间多值函数 $f_M \in$，使得 $f_M($ $x)$ 是 $M(x)$ 的接受计算。

3 多项式时间选择公理

本节中的表述大多基于语言集合族的选择函数。如果 $S = \{S_i : i \in I\}$ 是一个集合族（其中 I 是任意指标集），那么 S 的选择函数是一个函数 f，满足对所有 $i \in I$，$f(i) \in S_i$。

定义 3.1（语言集合族、诚实非空、选择函数）。给定一个复杂性类 $\mathcal{C}$，一个 $\mathcal{C}$ 语言集合族是一个单一语言 $L \in \mathcal{C}$，满足每个 $L_x := \{y : (x, y) \in L\}$ 也属于 $\mathcal{C}$。

语言集合族 L 是诚实非空的，如果存在正次数多项式 p、q，使得对每个 x，L_x 至少包含一个长度为 $p(|x|) \leq |y| \leq q(|x|)$ 的字符串 y。我们称 p、q 为 L 的“诚实性（分别为下界和上界）”。

部分多值函数 f 是语言集合 L 的选择函数，当且仅当：(1) 对所有 x，$set\text{-}f(x) \subseteq L_x$；并且 (2) 对每个非空的 L_x，$set\text{-}f(x)$ 非空。

备注 3.2。此时，诚实非空定义中的多项式上界很容易说明：至少应该存在一个 y 属于 L_x，且无需耗费超多项式空间就能写出（因此，例如，如果 $L \in$ 是 PSPACE，那么多项式空间机器就能找到这样的 y）。但多项式下界可能不那么直观。事实证明，在多个地方它都是一种非常自然且有用的条件，例如观察 3.6 和命题 3.8(1)。

经典选择公理 1（参见 [54, AC1，第 5] 页）。每个非空集合族都有一个选择函数。

多项式时间选择公理（PAC）1：每个由诚实非空语言组成的 P 集合族都存在一个属于 FP 的选择函数。

命题 3.3：PAC1 成立，当且仅当 $\text{NPMV}_{gt} \subseteq_c \text{FP}$。

证明。（⇒）假设 PAC1 成立。设 f 是一个 NPMV_{gt} 函数，且 L 是 f 的图。根据 NPMV_g 的定义，f 的图属于 P，因此 $L \in$P。由于 f 是全函数，每个 L_x 都非空。由于 f 的每个分支都在多项式时间内运行，$f(x)$ 的每个输出 y 都满足 $|y| \leq \text{poly}(|x|)$。为了得到一个ˆ ˆ 多项式下界，我们还要对 f 作如下修改，得到 f：定义 $f(x) \mapsto (x, y) \Leftrightarrow f(x) \mapsto y$，使得现在每个输出都满足 $|x| \leq |\hat{f}(x)|$。设ˆ L 为ˆ f 的图；此时，ˆL 是一个由诚实非空ˆ语言组成的 P 集合族。因此，根据假设，存在一个针对 L 的多项式时间选择函数ˆg。根据ˆ L 的构造，ˆ$g(x)$ 总是具有 (x, y) 的形式。最后，定义 $g(x) = y \Leftrightarrow \hat{g}(x) = (x, y)$。显然，$g$ 也属于 FP，且细化了 f。

(⇐) 反过来，假设 $\text{NPMV}_{gt} \subseteq_c$ FP，且令 L 为一个由诚实非空语言构成的 P 集合族，其诚实性界为 p、q。定义 f 如下：

$$set\text{-}f(x) = \{y : p(|x|) \leq |y| \leq q(|x|) \text{ and } (x, y) \in L\}$$

由于 $L \in$ P，f 的图属于 P：使用 L 的多项式时间判定器，并验证 x 与 y 之间的长度关系。此外，由于对于每个 x，L_x 都是诚实非空的，因此 f 是全函数，所以 f 属于 NPMV_{gt}。根据假设，f 有一个 FP 细化，显然这是 L 的多项式时间选择函数。

□

通过改变 PAC1 中的约束，可以轻松地将同样的论证调整为适用于其他几种标准复杂性假设。这里给出其中两种：

命题 3.4. 每个由诚实非空语言组成的 NP 集合族都有……

1. ……一个 NPSV$_t$ 选择函数，当且仅当 NPMV$_t$ $\subseteq_c$NPSV$_t$。
2. ……一个 FP 选择函数，当且仅当 NPMV$_t$ $\subseteq_c$FP；注意，后者就是假设 Q3。

由此可见，假设 Q 等价于选择公理的一个混合非确定性/确定性多项式时间版本。我们将在下文看到，多项式时间 AC 7 也等价于 Q。

证明。令 $\mathcal{F} \in$ {NPSV$_t$,FP}。

($\Rightarrow$) 假设每个由诚实非空语言构成的 NP 集合族都有一个 $\mathcal{F}$ 选择函数。^^^ 设 f属于 NPMV$_t$。如前所述，令 $f(x) \mapsto (x,y) \Leftrightarrow f(x) \mapsto y$，并令 L为 f的图。由于每个 NPMV 函数的图都属于 NP，因此 L属于 NP。与上文一样， L是一个诚实非空的语言集合族。根据假设，存在一个适用于 L的选择函数^$g \in \mathcal{F}$。定义 $g(x)$为$g(x) = y \Leftrightarrow$ ^$g(x) = (x,y)$；对于 $\mathcal{F}$的任一种选择，显然有^$g \in \mathcal{F} \Leftrightarrow g \in \mathcal{F}$。与上文一样，显然 g是 f的细化，因此 NPMV$_t$ $\subseteq_c \mathcal{F}$。

($\Leftarrow$) 反过来，假设 NPMV$_t$ $\subseteq_c \mathcal{F}$，并设 L 是一个由诚实非空语言构成的 NP 集合族，其诚实性界为 p、q。定义 f 如下：

$$set\text{-}f(x) = \{y : p(|x|) \leq |y| \leq q(|x|) \text{ and } (x,y) \in L\}.$$

由于 $L \in$ NP， f 的图属于 NP：使用针对 L的多项式时间验证器，并验证 x与 y之间的长度关系。此外，由于对于每个x， L_x 都是诚实非空的，因此 f 是全函数，所以 f 属于 NPMV$_t$。根据假设， f 有一个 $\mathcal{F}$ 细化，显然它是 L的一个 $\mathcal{F}$ 选择函数。 □

经典 AC 2（参见 [54, AC2, 第 5], [38, 页，命题 2.1]）。给定任意一组两两不相交的非空集合 X ，存在一个集合 C ，它从 X中的每个集合恰好包含一个元素。

定义 3.5（横截集）。给定一组语言 L， L的横截集是一个语言C ，使得对于每个满足 L_x 非空的 x ，$C \cap L_x$ 恰好包含一个元素。

多项式时间 AC (PAC) 2。每个由诚实非空、两两不相交的语言组成的多项式时间集合，都有一个属于 P 的横截集。

虽然我们还无法为此类集合的横截集给出多项式时间上界，但可以给出 PH 第二层内的上界。更具体地说，回忆一下，DP $= \{L \subseteq \Sigma^* : L = L_1 \backslash L_2 \text{ for some } L_1, L_2 \in \text{NP}\}$。DP 包含于 P^{NP}，甚至包含于 $\text{P}^{\text{NP}[2]}$（该机器在长度为 n 的输入上只进行 2 次查询）。对于任意语言 L，我们将 DP 相对化为 DP^L：将前述定义中的 NP 替换为 NP^L。

观察 3.6。每个由 L 个两两不相交的诚实非空语言组成的集合，在DP^{L}中都有一个横截集。

证明。令 p, q 为 L的诚实性界，因此每个 L_x 都包含某个 y，满足 $p(|x|) \leq |y| \leq q(|x|)$。令 C 由 L_x 中按字典序最先且长度至少为 $p(|x|)$ 的元素组成，对每个 $x \in \Sigma^*$各取一个。由于 L_x 两两不相交， C 中每个 L_x至多包含一个元素，因此它恰好包含一个元素，是一个横截集。

现在我们证明，可以在 DP^L 中判定属于 C。令 $L_1 = \{y : (\exists x)[q^{-1}(|y|) \leq |x| \leq p^{-1}(|y|)$ 和 $(x, y) \in L\}$，并令 $L_2 = \{y : (\exists y' <_{lex} y)(\exists x)[\max\{q^{-1}(|y'|), q^{-1}(|y|)\} \leq |x| \leq \min\{p^{-1}(|y|), p^{-1}(|y'|)\}$ 和 $(x, y) \in L$ 以及 $(x, y') \in L\}$。注意， L_1 和 L_2 均属于 NP^L，且我们有 $C = L_1 \backslash L_2$。 □

因此，对于 P 中的集合族，总是存在一个 DP 横截集。

开放问题 3.7。是否存在一个由两两不相交、诚实非空的多项式时间语言组成的 P 集合族，使得 L 的每个横截集都是 NP-困难的？NP 完全的？DP-完全的？

虽然我们尚未在 PAC2 与更标准的复杂性假设之间得到简洁的等价关系，但我们确实在更标准的假设与 PAC2 的某些 NP 版本之间得到了这样的简洁等价关系。

命题 3.8。1. $\text{NPMV}_{gt} \subseteq_c \text{NPSV}_t$ 当且仅当

(*) 每个由诚实非空、两两不相交的语言组成的 P 集合族都有一个属于 NP 的横截集。

2. $\text{NPMV}_t \subseteq_c \text{NPSV}_t$ 当且仅当

（*′）每个由诚实非空、两两不相交的语言组成的 NP 集合族在 NP 中都有一个横截集。

证明。（1）假设（*）成立，并令 $f \in \text{NPMV}_{gt}$。令 L 为 $\{(x, (x, y) : x \in \Sigma^*, f(x) \mapsto y\}$，它是 f的图的一个修改版本。根据定义，f 的图属于 P，因此 L 也属于 P。由于f 是全函数，并且每个非确定性分支至多使用多项式时间，每个 L_x 都是诚实非空的。由于 L_x 中的每个元素都具有 $(x, *)$ 的形式，当 $x \neq y$时，L_x 和 L_y 不相交。因此存在一个 $C \in$NP，它恰好从每个 L_x中包含一个元素。我们定义一个 NPSV_{gt}函数 g：在输入 x时，非确定性地猜测 y 和 w，使用 w 作为见证来验证 $(x, y) \in C$，并输出 y。这个 g是 f的一个 NPSV_t 细化。

反过来，假设 $\text{NPMV}_{gt} \subseteq_c \text{NPSV}_t$，并令 L 为一个由诚实非空、两两不相交的语言组成的 P 集合族，其诚实性界为 p, q。定义 f 如下：

$$set\text{-}f(x) = \{y : p(|x|) \leq |y| \leq q(|x|) \text{ and } (x, y) \in L\}.$$

由于 $L \in$ P，f 的图属于 P。此外，由于对于每个 x，L_x 都是诚实非空的，f 是全函数。因此，f 有一个 NPSV_t 细化 g。令 C 为 g的像。显然，C 与每个 L_x 恰好相交一次。下面的非确定性机说明 C 属于 NP：输入 y时，它猜测一个 x，使得 $p(|x|) \leq |y|$（因此特别有 $|x| \leq \text{poly}(|y|)$），猜测 g的一条接受路径，在该接受路径上模拟 $g(x)$ 的执行，并在该路径上的输出等于 y时接受。

(2) 我们在此说明，对于证明的第二部分，前面的内容如何相应变化。对于$f \in \text{NPMV}_t$，其图（以及如上所述的修改后的图）属于 NP。(*′) 随后使我们能够像之前一样得出存在一个 $C \in$ NP，其余论证仍然成立。对于论证的另一个方向，如果 L 仅属于 NP，那么 f 仍属于 NPMV_t，所以假设 $\text{NPMV}_t \subseteq_c \text{NPSV}_t$ 仍足以得到 NPSV_t 细化，证明的其余部分也仍然成立。

□

我们注意到，似乎只有在证明的最后一步——非确定性机必须猜测原像 $x \in g^{-1}(y)$——才需要非确定性；这也是实现与 PAC2 等价的唯一障碍。

上述结果使我们得以证明，AC 的两个 NP 版本是等价的：

推论 3.9（“NP 选择公理 1=NP 选择公理 2”）。每个由诚实非空语言构成的 NP 集合族都有一个 NPSV 选择函数，当且仅当每个由两两不相交的诚实非空语言构成的 NP 集合族都有一个 NP 横截集。

证明。命题 3.4(1)指出，此处陈述中的第一个条件等价于 NPMV$_t \subseteq_c$ NPSV$_t$，而命题 3.8(2)表明，后者等价于此处陈述中的第二个条件。

□

观察 3.10。PAC2 蕴含命题 3.8 中的条件 (*)。

证明。PAC2 的结论蕴含存在一个 P 横截集，而条件 (*) 的结论只要求存在一个 NP 横截集，但除此之外二者相同。□

经典选择公理 3（参见 [54, AC5，第 5] 页）。对于每个函数 f，都存在一个函数 g，使得 dom(g) = img(f)，并且对于每个 $x \in$ dom(g)，$f(g(x)) = x$。

多项式时间选择公理（PAC）3。对于每个部分多项式时间诚实函数 $f \in$ PF，都存在一个 $g \in$ PF，其 dom(g) = img(f)，且对于每个 $x \in$ dom(g)，$f(g(x)) = x$。

回想一下，（最坏情形下的）单向函数是一个一一对应的诚实函数 $f \in$PF，满足$f^{-1} \notin$ PF，因此 PAC3 简单来说就是单向函数不存在这一命题。这是 Selman 研究过的主题之一：

定理 3.11（Grollman、Selman [30] 和 Ko [40]）。PAC3 成立当且仅当 P = UP。

4 多项式时间基数

4.1 定义和基本性质

选择公理的若干种表述基于基数。在这里，我们发展这些表述的多项式时间类比。这一发展也部分受到第 1 节中 Downey[12] 的引文的启发。

设 Σ、Γ 是两个有限字母表。对于 $A \subseteq \Sigma^*$ 和 $B \subseteq \Gamma^*$，所谓“部分函数 $f\colon A \to B$”，是指满足 $A \subseteq$ dom(f) 且 $f(A) \subseteq B$的部分函数 $f\colon \Sigma^* \to \Gamma^*$。对于输入 $x \notin A$，我们不对 $f(x)$施加任何限制——它可能属于 B，也可能不属于 B，或者未定义。当我们讨论此类部分函数的性质时——例如，是否可在多项式时间内计算、是否为单射、满射、双射等——我们只考虑这些性质在输入属于 A 且输出属于 B时是否成立。例如，部分函数 $f\colon A \to B$ 是单射，当且仅当对于所有互不相同的 x、$y \in A$，$f(x)$ 和$f(y)$ 均互不相同。即使 f 在 A之外的输入上有定义，它在这些输入上也可能不是单射，甚至对于某些 $x \notin A$、$a \in A$，可能有 $f(x) = f(a)$，但仍然可以认为它是一个单射部分函数 $A \to B$。如果部分函数 $f\colon A \to B$ 满足 $f^{-1}\colon f(A) \to A$ 是单值的（等价地，f 是单射的），并且在 $f(A)$ 上可在多项式时间内计算，我们就称其为多项式时间可逆，或 p-可逆。若部分函数 f对所有 $x \in$dom(f) 都满足 $|f(x)| > |x|$，则称其为长度递增。

定义 4.1. 如果存在部分多项式时间可计算函数 $f\colon A \to B$ 和 $g\colon B \to A$，使得 $f \circ g = id_B$和 $g \circ f = id_A$，则两个集合 $A \subseteq \Sigma^*$、$B \subseteq \Gamma^*$ 具有相同的 p-基数，或称为 p-等势。在这种情况下，我们称 f 为一个 p-等势 $A \to B$。

我们用 $||A||_p$ 表示 A 的 p-基数，或者说，它的 p-等势类，因此 $||A||_p = ||B||_p$ 意味着 A 和 B 是 p-等势的。

如果对于某个子集 $B' \subseteq B$，有 $||A||_p = ||B'||_p$，我们就说 A 的 p-基数不大于 B 的 p-基数，记作 $||A||_p \preceq ||B||_p$。$||A||_p \prec ||B||_p$ 表示 $||A||_p \preceq ||B||_p$ 和 $||A||_p \neq ||B||_p$。

p-基数之间的关系 $\preceq$ 具有传递性和自反性，但我们将在命题 4.4 中看到，它并非偏序；也就是说，存在 A, B，使得 $||A||_p \preceq ||B||_p$ 和 $||B||_p \preceq ||A||_p$ 成立，但 $||A||_p \neq ||B||_p$ 不成立；不过，定理 4.10 给出了一个部分的正面结果。因此我们保留

记号 $\preceq$（而不采用例如 $\leq$ 这样的记号，尽管基数通常使用后者）。我们还将在命题 4.39 中看到，它不是全函数（存在不可比较的 p-基数）。

正如处理多对一归约时一样，引入一个由 $||A||_p \preceq ||B||_p$ 和 $||B||_p \preceq ||A||_p$ 定义的等价关系 $||A||_p \equiv ||B||_p$ 是合理的；粗略地说，等价与 p-基数相等之间的关系，类似于 Karp 等价与语言的 p-同构之间的关系。通过构造，p-基数等价类上的商关系 $\leq$ 是一个偏序，但命题 4.39 仍然表明它只是偏序，而非全序。不过我们不会怎么用到 $\equiv$，尽管其中显然还有值得探索的有趣理论。

记号说明。我们尽量始终使用上标^p 表示某个概念的多项式时间版本；但对于基数，我们想用 $||\cdot||$，因为它是基数的标准符号，同时又想避免使用 $||\cdot||^p$，以免它可能被误解为取 p 次幂。

命题 4.2。对于语言 $A \subseteq \Sigma^*$、$B \subseteq \Gamma^*$，若 $||A||_p = ||B||_p$，则 $A \equiv_m^p B$，除非 $A = \Sigma^*$ 或 $B = \Gamma^*$。在后一种情况下，A 和 B 都属于 P。

证明。假设 $||A||_p = ||B||_p$，并且先进一步假设 $A \neq \Sigma^*$ 和 $B \neq \Gamma^*$。我们将证明 $B \leq_m^p A$；反向结论由对称性可得。令 $a_0 \in \overline{A}$。

令 $f\colon A \to B$ 是一个 p-等势。令 p 为一个多项式，M、N 为图灵机转换器，使得 M 在多项式时间内对属于 A 的输入计算 f，而 N 在时间 $\leq p(n)$ 内对属于 B 的输入计算 f^{-1}。以下函数 r 是从 B 到 A 的多项式时间归约：对于输入 x，运行 $N(x)$ 共 $p(|x|)$ 步。如果 N 拒绝，或在此时间内没有输出，则 $r(x) := a_0$。对于 $B \subseteq \mathrm{dom}(f^{-1}) \subseteq \mathrm{dom}(N)$。如果 $N(x)$ 在运行 $p(|x|)$ 步后 $= y$，则检查 $M(y) = x$。若不是，则输出 a_0（因为如果 x 属于 B，那么我们就有 $M(N(x)) = f(f^{-1}(x)) = x$）。若是，则令 $r(x) = y$，因为此时 $x \in B$ 当且仅当 $r(x) \in A$。（注意，$\mathrm{dom}(N)$ 可能严格大于 B，且 $\mathrm{dom}(M)$ 可能严格大于 A，并且对于某个 x，$M(N(x)) = x$ 可能成立，而该 x 不属于 B，因此需要进行最后的检查 $r(x) \in A$。）

如果 $A = \Sigma^*$，那么就没有可用的 a_0，但在这些情况下，上述归约可以直接判定输入 x 是否属于 B，因此我们得到 $B \in$P。 □

请注意，在上述证明中，我们实际用到了这样一个事实：我们能够访问彼此互为逆函数的（部分）多项式时间可计算函数。如果仅使用多项式时间的双射诚实函数，而不要求存在多项式时间逆函数（即使要求两个方向上都存在这样的函数，但不要求它们互为逆函数），试图将 Nerode & Remmel 的理论 [51, 52] 从一元语言推广到更大的字母表，其结果似乎不太可能成立。

我们注意到，前述结果无法以自然的方式推广到 $||A||_p \preceq ||B||_p$：

命题 4.3. 存在无限且余无限的集合 A, B，使得 $||A||_p \preceq ||B||_p$，但 $A \not\leq_T^p B$。

证明。设 A 是一个 EXP 完全集，且 $B = 0\Sigma^*$（前缀 0 只是为了确保 B 是余无限的）。那么 $0A = \{0a\colon a \in A\}$ 是 EXP 完全集，且 $0A \subseteq B$，因此 $||A||_p = ||0A||_p \preceq ||B||_p$。但是根据时间层次定理，$A \not\leq_T^p B$，否则就会有 $A \in$P。 □

我们可以用命题 4.2 证明 $\preceq$ 不是偏序：

命题 4.4（$\preceq$ 在 p-基数上不是偏序）。存在语言 A、$B \subseteq \Sigma^*$，使得 $||A||_p \preceq ||B||_p$ 且 $||B||_p \preceq ||A||_p$（我们可以将它们合称为 $||A||_p \equiv ||B||_p$），但是 $||A||_p \neq ||B||_p$。

证明。设对于某个 $B' \notin$ P，有 $A = 1\Sigma^*$，$B = 1(\Sigma^* \oplus B')$。首先，我们有 $||A||_p = ||10\Sigma^*||_p$，并且对任意 B'，$10\Sigma^* \subseteq 1(\Sigma^* \oplus B')$，因此得到 $||A||_p \preceq ||B||_p$。反过来，由于 $B \subseteq A$，我们得到 $||B||_p \preceq ||A||_p$。但是，如果 $||A||_p = ||B||_p$，那么命题 4.2 将推出 $A \equiv_m^p B$（因为二者都不是 Σ^*），这意味着 $B \in$P，与 $B \equiv_m^p B' \notin$ P 这一事实矛盾。 □

4.2 与 p-同构的比较

请注意，先验而言，具有相同的 p-基数是比多项式时间同构更弱的条件，因为 p-基数所要求的双射不必是全函数，也不必是 Σ^* 上的双射。我们在这一方向上的前两个结果有助于阐明二者之间的关系。

命题 4.5. 如果 $A \cong^p B$，那么 $||A||_p = ||B||_p$ 和 $||\overline{A}||_p = ||\overline{B}||_p$。若 A 属于 P，则逆命题也成立。

事后我们发现，这里逆命题的论证与 Goldsmith、Hemachandra 和 Kunen 的一个论证非常相似，但更一般；该论证转载如下，作为推论 4.19(2)。

证明. 假设 $f\colon \Sigma^* \to \Gamma^*$ 是一个 p-同构 $A \to B$。那么 $f|_A\colon A \to B$ 是一个 p-等势，类似地，$f|_{\overline{A}}\colon \overline{A} \to \overline{B}$ 也是一个 p-等势。

反过来，假设 $f\colon A \to B$ 是一个 p-等势（在 A 上），且 $g\colon \overline{A} \to \overline{B}$ 是一个 p-等势，并且 $A \in$ 属于 P。那么以下是一个 p- 双射 $\phi\colon \Sigma^* \to \Gamma^*$，它是一个 p- 同构，见证了 $A \cong^p B$。对于输入 x，我们首先使用多项式时间机器判断 $x \in A$ 是否成立。若成立，则输出 $f(x)$；否则，输出 $g(x)$。由于 Σ^* 是 A 和 $\overline{A}$ 的不交并，ϕ 是一个全函数多项式时间双射。

以下算法可在多项式时间内计算 ϕ^{-1}。设 $t(n)$ 是计算 $f^{-1}|_B$ 的某个算法以及计算 $g^{-1}|_{\overline{B}}$ 的某个算法的运行时间的多项式上界。输入 $x \in \Gamma^*$ 时，尝试分别运行 $f^{-1}(x)$ 和 $g^{-1}(x)$，每个运行 $t(n)$ 步。如果其中只有一个在规定时间内完成，那么我们就知道 x 属于 B 还是 $\overline{B}$，并将其作为输出。不过请注意，计算 f^{-1} 的算法的定义域可能大于 B，而计算 g^{-1} 的算法的定义域可能大于 $\overline{B}$，因此 $f^{-1}(x)$ 和 $g^{-1}(x)$ 都有可能在 $t(|x|)$ 步内分别输出字符串 y、z。如果 $y = z$，那么算法可以明确地输出 y，而无需确定 $x \in B$ 是否成立。如果 $y \neq z$，那么我们计算 $\phi(y)$ 和 $\phi(z)$。由于 ϕ 是双射且 $y \neq z$，因此 $\phi(y) \neq \phi(z)$，所以它们中至多只有一个等于 x。（而且其中至少一个必须等于 x，因为 x 必须属于 B、$\overline{B}$ 中至少一个。）如果 $\phi(y) = x$，则输出 y；如果 $\phi(z) = x$，则输出 z。 □

命题4.6。1. 存在一个包含无穷多个不同 p-同构类的 p-基数。

2. 存在具有相同 p-基数的非 p-同构集合 A、B，其中 $\overline{A}$、$\overline{B}$ 均为无限集合且属于 EXP。

请注意，当 A、B 为有限集合时，不存在此类例子，因为此时 $||A||_p = ||B||_p$ 蕴含 $A \cong^p B$。

证明。1. 对每个 $n \in \mathbb{N}$，令 S_n 为按字典序排列的前 n 个字符串的集合。定义 $A_n := \Sigma^* \setminus S_n$。于是，所有 A_n 都与 $A_0 = \Sigma^*$ p-等势：p-等势 $A_0 \to A_n$ 只需根据相应的 $|\Sigma|$ 进制数，将每个字符串向“上 n”移动即可。但是，如果 $n \neq n'$，那么 $\overline{A_n}$ 和 $\overline{A_{n'}}$ 是大小不同的有限集合，因此它们不 p-等势。由于在这种情况下 $||\overline{A_n}||_p \neq ||\overline{A_{n'}}||_p$，它们不可能 p-同构，因此 A_n 和 $A_{n'}$ 也不可能 p-同构。

2. 我们给出一个例子，其中 $\overline{A}$、$\overline{B}$ 都是无限集合且属于 EXP。回顾一下，如果集合 A 是无限的，但不包含任何属于 P 的无限子集，那么它就是 P-免疫的。设 A 为任意余-P-免疫集，也就是说，$\overline{A}$ 是无限的，但不包含任何属于 P 的无限子集。例如，Ko 和 Moore [41] 证明了 EXP 中存在 P-双免疫集，即 A 及其补集都是 P-免疫的。令 $B = \{1x : x \in A\}$。那么，一个 p-等势由 $A \ni a \mapsto 1a \in B$给出，其逆映射为 $B \ni 1x \mapsto x \in A$。但我们声称 $A \not\cong^p B$。简而言之：P-免疫性在同构下保持不变，但 $\overline{B}$ 包含一个属于 P 的无限子集 $0\Sigma^*$，即

一个属于 P 的无限子集。更具体地说：假设存在一个多项式时间可计算双射$f\colon\ \Sigma^* \to \Gamma^*$，使得 $f(A) = B$，并且 $f^{-1} \in$也属于 FP。由于 $f^{-1}(\overline{B}) = \overline{A}$，我们有$f^{-1}(0\Sigma^*) \subseteq \overline{A}$。但 $f^{-1}(0\Sigma^*)$ 属于 P，因为 $x \in f^{-1}(0\Sigma^*)$ 当且仅当 $f(x)$ 以 0 开头，而这很容易验证。由于 $0\Sigma^*$ 是无限的，且 f^{-1} 是一个双射，这与 $\overline{A}$的 P-免疫性矛盾。

□

观察 4.7。设 $L \notin$ P。若 $L \equiv_m^p L'$ 蕴含 $L \cong^p L'$，则 L 的 p-同构类等于其 p-等势类。

证明。由于 $L \notin$ P，$\Sigma^* \not\equiv_m^p L$，因此 L 的 p-同构类不包含 Σ^*。由于 p-同构蕴含 p-等势，而 p-等势（避开 Σ^*）蕴含 $\equiv_m^p$（命题 4.2），故得证。

□

推论 4.8（参见 Kurtz、Mahaney、Royer [42]）。对每个集合 A，都存在一个集合 $B \geq_m^p A$，使得 B 的 p-同构类等于其 p-等势类。存在一个集合，它是 EXP 的$\leq_{btt}^p$-完全集合，且其 p-同构类等于其 p-等势类。

证明。Kurtz、Mahaney 和 Royer [42] 证明，对于每个 A，都存在一个集合 $B \geq_m^p A$，使得 B 的多项式时间多对一度等于其多项式时间同构类。这样的 B 必然不属于 P，因为 P 是其自身的多项式时间多对一度，但其中包含彼此不同构的集合对。因此，我们可以应用观察 4.7。他们还证明了 EXP 的某个 $\leq_{btt}^p$- 完全集合的坍缩结果；根据时间层次定理，该集合不属于 P，因此我们同样可以应用观察 4.7。

□

在命题 4.6 中，我们展示了一个 p-基数（即 Σ^*的 p-基数），其中包含无限多个 p-同构类；我们认为，更一般的结论应当成立。事实上，我们预计这类基数在$\leq_m^p$ 序中是稠密的：

猜想 4.9。对于每个集合 A，都存在一个集合 $B \geq_m^p A$，使得 $||B||_p$ 包含无限多个不同的 p-同构类。

接下来我们注意到，Berman 和 Hartmanis 的康托尔–伯恩斯坦式证明可推广到 p-基数：

定理 4.10。设 $A \subseteq \Sigma^*$、$B \subseteq \Gamma^*$，以及 $p\colon\ A \to B$和 $q\colon\ B \to A$ 是长度递增的、p-可逆的部分多项式时间单射函数。则 A 和 B 具有相同的 p-基数。

与 [5, 定理 1] 中几乎完全相同的证明同样适用；为便于说明，我们沿用 [15, 第 2] 节中所述的术语和证明。

证明。定义如下图 $G_{p,\ q}$ 其顶点集为 $0A \cup 1B$：对于每个 $x \in A$，存在一条边$0x \to 1p(x)$；对于每个 $y \in B$，存在一条边 $1y \to 0q(y)$。根据构造，该图显然是二部图。由于 p 和 q 是函数，且 dom(p) $\supseteq A$ 、 dom(q) $\supseteq B$，每个顶点的出度恰好为 1。由于 p 和 q 是可逆的，每个顶点的入度至多为 1。$G_{p,\ q}$ 的连通分量称为链。若一个顶点的入度为 0，则称其为源点。因此，该图是不交并的链，每条链属于以下类型之一：有限环、双向无限路径、源点位于 $0A$ 中的单向无限路径，或源点位于$1B$中的单向无限路径。由于 p 和 q 是长度递增的，不可能存在有限环。也不可能存在双向无限路径，因为沿链向后追溯时，字符串的长度必须永远递减。由于每个顶点的出度均为 1，每个顶点都属于某条链。

令 C_A 为属于源点在 $0A$ 的链的顶点，令 C_B 为属于源点在 $1B$ 的链的顶点。我们定义

$$\phi(x) = \begin{cases} p(x) & \text{if } 0x \in 0A \cap C_A \\ q^{-1}(x) & \text{if } 0x \in 0A \cap C_B \end{cases} \qquad \psi(y) = \begin{cases} p^{-1}(y) & \text{if } 1y \in 1B \cap C_A \\ q(y) & \text{if } 1y \in 1B \cap C_B \end{cases}$$

如同我们 与此类证明中的通常情况一样，很容易验证 ϕ 和 ψ 互为逆映射 r.

由于 p^{-1} 的定义域不一定是 B 的全部，且 q^{-1} 的定义域不一定是 A 的全部，因此仍需验证 ϕ（分别地，ψ）能否在定义域 A（分别地，B）上由多项式时间多值函数计算。我们给出 ϕ 的证明，ψ 的证明类似。设 $t(n)$ 是一个多项式，使得对于 A 中的输入，p^{-1} 可在 $t(n)$ 时间内计算；对于 B 中的输入，q^{-1} 可在 $t(n)$ 时间内计算。对于 A 中的输入，我们将 q^{-1} 修改为函数 q^{-1}，使得当 $x \in q(B)$ 时，$q^{-1}(x) = q^{-1}(x)$；否则，$q^{-1}(x)$ 输出特殊符号 $\perp$。后者可在 $O(t(n)\log t(n))$ 时间内计算：运行一个计算 q^{-1} 的 $t(n)$ 时间机器，并加上一个时钟；若时钟达到 $t(n)$，便停止并输出 $\perp$。同样，我们将 p^{-1} 修改为 p^{-1}。

高效计算 ϕ 的关键在于确定 $0x \in C_A$ 还是 $0x \in C_B$。它通过交替应用 q^{-1} 和 p^{-1}，直到得到 $\perp$，从而找到链的源点，并因此知道顶点 $0x$ 属于 C_A 还是 C_B。由于 p^{-1} 和 q^{-1} 都是长度递减的，这一过程所需时间至多为关于 $|x|$ 的多项式时间。

□

注释 4.11。从证明中可以看出，长度递增条件的主要作用是保证任意一列 p^{-1}、q^{-1} 都会在 poly($|x|$) 步后终止。因此，这个论证可以推广到任意满足以下条件的 p-良序（见定义 6.1）：$\prec_A$ 在 A 上，$\prec_B$ 在 B 上，并且对所有 $x \in A$、$y \in B$，$q(p(x)) \succ_A x$ 且 $p(q(y)) \succ_B y$。

事实上，还可以进一步推广。如果一个序列 p^{-1}, q^{-1} 构成长度有 p-界的环，就可以检测到并轻松处理。上述证明真正的问题在于这样的环或链：多项式时间算法无法识别某个字符串何时属于这类环或链。（一个必要条件是，这样的环或链长度超多项式，但仍可能存在非常长、却因其他原因而容易识别的此类链/环。）

4.3 p-可 数性：密度、可排序性、可枚举性与可压缩性 y

自然可以考虑将 Σ^* 作为 $\aleph_0$的 p-基数类比，即 $\mathbb{N}$的基数，因此这里我们考察与 Σ^*具有相同 p-基数的集合。

定义 4.12（p-可数）。如果一个集合是有限集，或者其 p-基数与Σ^*相同，则称它为 p-可数。

在讨论有趣的联系之前，我们先确保我们的探究不依赖于字母表：

观察 4.13. 设 Σ, Γ 是两个大小至少为 2 的有限字母表。那么 $||\Sigma^*||_p = ||\Gamma^*||_p$。

证明. 设 $k = |\Sigma|, \ell = |\Gamma|$。以下是一个 p-等势 $\Sigma^* \to \Gamma^*$。给定 $x \in \Sigma^*$，考虑与之关联的自然数 N（见第 2 节），然后令 y 为 Γ^* 中与 N 关联的 ℓ 进制字符串，并输出 y。我们有 $|x| \sim \log_k N$ 和 $|y| \sim \log_\ell N$（因为两者都 $k, \ell \geq 2$），所以 $|y| = \Theta(|x|)$。显然，这些计算可以在多项式时间内完成。

□

由于每种语言都是 Σ^* 的子集，每个 A 都有 $||A||_p \preceq ||\Sigma^*||_p$，因此似乎 Σ^* 是“最大的” p-基数。但请记住，$\preceq$ 只是一个预序，而非偏序；在命题 4.4 的证明中，我们看到，对于 $B' \notin \mathrm{P}$，$||\Sigma^*||_p \prec ||\Sigma^* \oplus B'||_p$（尽管我们也有 $||\Sigma^* \oplus B'||_p \preceq ||\Sigma^*||_p$），但这两个基数并不相等。因此，$||\Sigma^*||_p$ 的 $\equiv$-等价类确实是商偏序集中的极大元，但 p-基数本身在 $\preceq$ 预序中并非极大元。

4.3.1 可枚举性

Selman 引入了 p-可枚举性的概念：

定义 4.14（p-可枚举，Selman [57]）。如果存在函数$f \in$FP，使得 img(f) $= L$，并且对所有 $y \in L$，存在 x，使得 $f(x) = y$以及$|x| \leq$poly($|y|$)，则语言 L 是 p-可枚举的。

注意，在 Selman 的定义中，f 不必是单射。

观察 4.15。p-可数集是 p-可枚举的。

证明。对于有限集，这是显然的。对于无限 p-可数集 L，令 $f\colon \Sigma^* \to L$ 为一个 p-等势。于是，L 通过 f是 p-可枚举的；诚实性条件由 f^{-1}的 p-可计算性保证。 □

这也可由以下事实推出：p-可枚举集合恰好是 NP 中的集合 [57, 推论 2]，而 p-可数集合属于 P（根据命题 4.2）。这一简单观察将在我们讨论 p-基数算术时带来一个有趣的推论（命题 4.36）。

定义 4.16（迭代 p-可枚举 [32]）。如果存在一台图灵机 M 和一个多项式 p，使得对所有 $x \in L$，$M(x)$ 都在 $p(|x|)$ 步内停机，且存在某个 $x_0 \in L$，使得 $L = \{x_0, M(x_0)\ M(M(x_0))\ M(M(M(x_0)))\ \dots\}$，则称语言 L 为迭代 p-可枚举。若 L 按上述方式迭代 p-可枚举，且由 M 计算出的函数在其像上有一个多项式时间逆函数，则称其为可逆迭代 p-可枚举。

Hemachandra、Hoene、Siefkes 和 Young [32, 第 5] 节等人，举出了若干可逆迭代 p-可枚举语言的例子，其中包括可计算可枚举的 P-圆柱，以及具有各种形式自归约性的集合。这里我们再补充一类例子：

命题 4.17. 若 L 是 p-可数的，则 L 是可逆迭代 p-可枚举的。反之并非总是成立。

证明. 对有限的 L，这显然成立；枚举器会遍历 L的所有元素，形成一个有限循环。

对于无限的 L，设 $f\colon L \to \Sigma^*$是一个 p-等势。令 $x_0 = f^{-1}(\epsilon)$，并对 $x \in L$定义 $M(x)$，使得 $M(x) = f^{-1}(f(x) + 1)$. 由于 f、f^{-1}和加常数运算都是 p-可逆的，因此 M也是 p-可逆的。

Hemachandra 等人 [32] 给出了迭代 p-可枚举、但不属于 P 的语言示例；然而，根据命题 4.2，p-可数语言属于 P。 □

4.3.2 可压缩性

Goldsmith、Hemachandra 和 Kunen [27] 将语言 L 定义为 P-可压缩的，当且仅当存在一个$f \in$FP，$f\colon \Sigma^* \to \Sigma^*$，使得 $f|_L\colon L \to \Sigma^*$是一个双射。

观察 4.18. 若 L 是 p-可数无限的，则 L 可由一个 p-可逆函数压缩为 P-可压缩。

ˆ 证明。给定一个 p-等势 $f\colon L \to \Sigma^*$，定义 $f\colon \Sigma^* \to \Sigma^*$ 如下：

$$\hat{f}(x) = \begin{cases} x & x \notin L \\ f(x) & x \in L. \end{cases}$$

ˆ 由于 $f \in$PF 具有 $f|_L\colon L \to \Sigma^*$一个双射，而 $L \in$P（因为它是 p-可数的），显然 $f \in$FP，且 ˆ$f|_L\colon L \to \Sigma^*$仍然是一个双射。此外，$f^{-1}\colon \Sigma^* \to L$是 ˆ f的逆映射，而后者属于 FP。 □

因此，Goldsmith、Hemachandra 和 Kunen 的若干结果与技术对 p-可数集合具有直接的意义；我们在此记录其中一个特别有趣的结果。

推论 4.19（参见 Goldsmith、Hemachandra、Kunen [27, 命题 3.18]）。如果 A、$\overline{A}$、B、$\overline{B}$ 都是 p-可数无限的，那么 $A \cong^p B$。

证明。Goldsmith–Hemachandra–Kunen [27, 命题 3.18] 使用了 Grollman 和 Selman 的结果：P =UP 当且仅当单向函数不存在 [30]。这里我们转而利用这样一个事实：根据定义，具有 Σ^* 的 p-等势映射都有逆映射。不过，除此之外，以下构造与 [27] 相同。为确保完备性并便于查阅，我们在此给出该构造。

令 $f_1 : A \to \Sigma^*$ 和 $f_2 : \overline{A} \to \Sigma^*$ 为 p-等势映射，其扩展 $\hat{f}_1$、$\hat{f}_2$ 均为全函数 FP 函数。定义

$$f(x) = \begin{cases} 0\hat{f}_1(x) & x \in A \\ 1\hat{f}_2(x) & x \notin A. \end{cases}$$

于是我们有

$$f^{-1}(by) = \begin{cases} f_1^{-1}(y) & b = 0 \\ f_2^{-1}(y) & b = 1. \end{cases}$$

由于 $\hat{f}_1$、$\hat{f}_2$、f_1^{-1}、f_2^{-1} 以及 A 的示性函数都可在多项式时间内计算（后者依据命题 4.2），因此 f 和 f^{-1} 也可在多项式时间内计算。此外，f、f^{-1} 是全双射 $\Sigma^* \to \Sigma^*$。

对 B 类似地定义 g。那么 $h(x) = f^{-1}(g(x))$ 是一个全函数、p-等势的 $\Sigma^* \to \Sigma^*$，满足 $h(B) = f^{-1}(g(B)) = f^{-1}(0\hat{}g_1(B)) = f^{-1}(0g_1(B)) = f^{-1}(0\Sigma^*) = f_1^{-1}(\Sigma^*) = A$，因此 h 就是所需的 p-同构 $B \to A$。 □

4.3.3 可排序性

假设 $L \subseteq \Sigma^*$ 是 p-可数无限的。那么存在一个多项式时间可计算且可逆的双射 $f : L \to \Sigma^*$。对于无限语言，排名函数 [25, 1] 是到 Σ^* 的双射映射这一特殊情形：

定义 4.20（排名函数，p-可排序性 [25, 1]）。语言 L 的（强）排名函数是映射 $rk_L(x) = |\{y \in L : y \leq_{lex} x\}|$。若语言 L 的强排名函数可在 FP 中计算，则称其为强 p-可排序；若排名函数可在实际属于 L 的那些输入上通过多项式时间多值函数计算，则称其为弱 p-可排序。

由 p-可数性，我们还不能完全推出 p-可排名性；不过，如果允许将排序 $\leq_{lex}$ 替换为具有许多相同性质的另一种排序 $\leq_{lex}$，就能得到一个相应的版本。我们将可排序性推广到任意全序 $\prec$。我们定义 L 相对于 $\prec$ 的强排名函数为$rk_{L,\prec}(x) = |\{y \in L : y \preceq x\}|$；若$rk_{L,\prec}$ 属于 FP（分别地，在 L上的输入上属于 PF），则称 L 相对于 $\prec$ 是强 p-可排序的（分别地，弱 p-可排序的）。

定义 4.21（长度相关 [47]）。若全序 $\prec$ 在 Σ^* 上满足：$x \prec y$ 蕴含$|x| \leq$poly($|y|$)，则称其为长度相关的。

观察 4.22。若 L 是 p-可数的，则在某个长度相关的全序（在 L上）$\prec \in$PF 下，L 是弱 p-可排序的。

证明。对于有限集合，这显然成立。设 L 是一个无限 p-可数集，且 $f : L \to \Sigma^*$ 是一个 p-等势。定义 $x \prec y$，使得 $f(x) <_{lex} f(y)$。显然，$\prec$ 在 L 上可由多项式时间多值函数计算。由于字典序在 Σ^* 上是全序，$\prec$ 在 L 上也是全函数。由于 f 是 p-可逆的，因此它是诚实的，所以我们有 $|x| \leq$ poly($|f(x)|$) $\leq$ poly($|f(y)|$) $\leq$ poly($|y|$)，其中最后一个不等式源于 f 可在多项式时间内计算这一事实。 □

接下来我们指出，p-基数在多项式变换下保持密度。回忆一下，语言 L 的计数函数是 $c_L(n) = |L \cap \Sigma^{\leq n}|$。若存在多项式 p、q，使得对所有 n，都有 $f(n) \leq g(p(n))$ 且 $g(n) \leq f(q(n))$，则称两个函数 f、g: $\mathbb{N} \to \mathbb{N}$ 多项式相关。

引理 4.23. 如果 $||A||_p = ||B||_p$，那么 $c_A(n)$ 与 $c_B(n)$ 多项式相关。

证明. 设 f： $A \to B$ 是见证 $||A||_p = ||B||_p$的 p-等势。设 p 是一个多项式，它给出了 f 在 A中的输入上的运行时间上界；类似地，设 q 是 $f^{-1}|_B$运行时间的多项式上界。那么我们有

$$f(A \cap \Sigma^{\leq n}) \subseteq B \cap \Sigma^{\leq p(n)} \qquad \text{and} \qquad f^{-1}(B \cap \Sigma^{\leq n}) \subseteq A \cap \Sigma^{\leq q(n)}.$$

前者推出 $c_A(n) \leq c_B(p(n))$，后者推出 $c_B(n) \leq c_A(q(n))$. □

推论 4.24. 如果 L 是 p-可数无限的，那么 L 是指数稠密的，也就是说， L 至少有$2^{\Omega(n^c)}$ 个长度为 $\leq n$ 的字符串，其中 $c > 0$。

由于 p-同构保持 p-基数，而 p-可排名性不是 p-同构不变量，我们回顾一下 Goldsmith 与 Homer 提出的可扩展性概念 [26]。如果一个语言与某个强 p-可排名集合 p-同构，则称其为 p-可扩展。（我们想引入显而易见的弱 p-可扩展概念，并称 p-可数性蕴含弱 p-可扩展性，但我们仍不知道后者是否确实成立！）

结合前面的结果，我们得到

定理 4.25。对于任意指数稠密语言 L,

$$\textit{strongly } p\textit{-rankable} \implies p\textit{-scalable} \implies p\textit{-countable} \implies \textit{weakly } p\textit{-rankable } w.r.t.\ \prec,$$

存在某种长度相关的全序 $\prec$，定义在 L 上，且可由多项式时间多值函数 PF 计算。

因此，指数密度是与 Σ^* 具有相同 p-基数的必要条件；而在指数稠密语言中，具有 Σ^* 的 p-基数，其位置介于强 p-可排序性和弱 p-可排序性之间（对于某些全序而言）。我们认为这些蕴含关系的逆命题不成立。

证明。我们证明第二个箭头，其余箭头已在上文或此前证明。Goldberg 与 Sipser [25] 指出，如果一个语言具有强 p-可排序性，那么 rk_L^{-1}: $\Sigma^* \to L$ 可通过二分查找在关于其输出长度的多项式时间内计算。因此，只需证明 rk_L 是诚实的。根据假设，我们有 $rk_L(x) \geq 2^{|x|^c}$。对两边取位长，得到 $|rk_L(x)| \geq |x|^c - 1$，所以 $|x| \leq |rk_L(x)|^{1/c}$，因此 rk_L 是诚实的。 □

例 4.26。这使我们能够再举出一类有趣的语言，它们体现了 p-同构类与 p-基数之间的差异。具体而言， Σ^* 的任何 p-可扩展稠密真子集都与 Σ^*具有相同的 p-基数，但与 Σ^*不同构。后者的原因是，同构集合的补集也同构；然而， Σ^* 的补集为空，而根据假设，另一个语言的补集非空。

4.3.4 有限差异。

现在我们证明，有限差异保持 P-可数性（当然，这里指无限集合）。下一个结果的第一部分涉及可排序性，这一点想必早已为人所知，但我们找不到相关参考资料；其证明也可作为第二部分的良好预热。我们认为第二部分是新的。我们采用标准记号 $A =^* B$，表示 A 和 B 至多相差一个有限集合。

定理 4.27. 若 $A =^* B$，则

1. A是强（分别地，弱）p-可排序，当且仅当 B 是；
2. A 是 p-可数的，当且仅当 B 是。

证明。假设 $A =^* B$。如果它们是有限的，那么它们都是强 p-可排序的，也都是 p-可数的，因此现在我们可以假设它们是无限的。

(1) 我们将定义一个“移位函数” $\sigma(x)$，它告诉我们从 A移到 B时应移动多少。我们归纳地定义 σ：

$$\sigma(x) = \sigma(x-1) + B(x) - A(x)$$

其中，$x-1$表示 x在长度字典序中的直接前驱；而在 $x = \epsilon$（空串）的情况下，我们按惯例简单地定义为 σ（“$\epsilon - 1$”）：$= 0$。

写作 $B = (A \cup P) \backslash N$，其中 P是与 A不相交的有限集合，而 N是 A的有限子集。令 $\{z_1, \ldots, z_{s+t}\} = P \cup N$满足 $z_1 \leq_{lex} z_2 \leq_{lex} \cdots \leq_{lex} z_{s+t}$。首先，$\sigma$在每个范围$[\epsilon, z_1)$ $[z_1, z_2) \ldots,$ $[z_{s+t-1}, z_{s+t})$ $[z_{s+t}, \infty)$上都是常数。其次，σ可以在多项式时间内计算：可以将 z_i以及 σ 在上述每个范围上的取值硬编码，因此输入 x 时，算法只需判断它属于这些 $O(1)$个范围中的哪一个 x，然后输出相应的（硬编码）值。根据构造，对于所有字符串 x，都有 $rk_B(x) = rk_A(x) + \sigma(x)$，由此得到第一个结论。

(2) 假设 A 是 p-可数无限的（有限情形已在第一段中处理），且$A =^* B$。令 $f\colon \mathbb{N} \to A$ 为一个 p-等势映射。我们将通过平移f来定义一个 p-等势映射 $g\colon \mathbb{N} \to B$，方法与上文类似。令 $B = (A \cup P) \backslash N$，其中 P是与 A不相交的有限集合，而 N是 A的有限子集。

首先，我们证明 $B' = A \cup P$是 p-可数的。思路是先枚举 P，然后将 A的枚举整体上移 $|P|$。更正式地说，我们定义 $g'(0)$ $g'(1) \ldots, g'(|P|-1)$，使其双射地枚举 P，然后对所有 $i \geq s$，令 $g'(i) = f(i-s)$。不难验证，$g'\colon \mathbb{N} \to B'$是一个 p-等势（要验证 p-可计算性和 p-可逆性，注意到前 $|P|$ 个值可以硬编码）。

接下来，我们证明 $B = B' \backslash N$是 p-可数的。设 $N = \{g'(j_1) \ldots, g'(j_t)\}$，其中 $j_1 < j_2 < \cdots < j_t$。思路是使用同一个 p-等势 g'，但在适当的位置对其进行平移，以跳过 $g'(j_1) \ldots, g'(j_t)$。令 $h\colon \mathbb{N} \to \mathbb{N} \backslash \{j_1, \ldots, j_t\}$ 为满足以下条件的双射：$h(i)$ 是 $\mathbb{N} \backslash \{j_1, \ldots, j_t\}$中的第 i 小元素。不难验证，$g = g' \circ h$ 是一个等势 $\mathbb{N} \to B$。要证明它是 p-可计算且 p-可逆的，只需证明 h满足这两个性质，因为 g' 已经是 p-等势。对于这两点，注意到 h是分段线性的，且只有有限多个断点。将这些断点及其跳跃值硬编码（注意：如果某些 j_k 是连续整数，它可能会跳过多个整数），即可使 h 成为 p-可计算的。由于 h 也严格递增，计算其逆映射相当于确定输入落在哪个线性区间内，然后对该区间上的线性函数求逆。同样，由于这样的区间只有有限多个，所需信息可以硬编码，其余计算也就很简单了。 □

这引出了一个问题：对于无限集，两个具有有限差异的集合是否必定总是 p-等势？我们感谢一位匿名审稿人提出的构造；对该构造稍作修改后，我们得以对此问题作出否定回答：

定理 4.28。存在一个无限语言 $A \in \mathrm{P}$，使得

1. A 与它的任何真子集都不 p-等势（它是戴德金 p-有限的，见定义 6.2）；
2. 对于任意两个与 A 有限差异的语言 B、B'，我们有 $||B||_p = ||B'||_p$ 当且仅当 $|B \backslash A| - |A \backslash B| = |B' \backslash A| - |A \backslash B'|$。特别地，并非所有与 A 有限差异的集合都与 A p-等势；并且

3. 对于任意两个与 A 有限差异的语言 B、B'，我们有 $||B||_p \preceq ||B'||_p$ 当且仅当 $|B\backslash A| - |A\backslash B| \leq |B'\backslash A| - |A\backslash B'|$。

特别地，对于这个 A，与 A 有限差异的集合的 p-基数上的预序 $\preceq$ 实际上是一个与整数具有相同序型的全序。尽管定理的第 (1) 部分已经回答了有限差异是否保留 p-基数这一问题，但另外两部分的证明也类似，并且将在下文得出一个有趣的推论（推论 4.48）。

证明。令 $A = \{1^{2^{2^{2^k}}} : k \in \mathbb{N}\}$。注意，如果 $\ell = 2^{2^{2^k}}$ 是 A中某个字符串的长度，那么下一个最长字符串的长度恰好是 $\ell^{\log_2 \ell}$（这就是我们使用三重指数塔的原因；如果只使用双重指数塔，那么这里得到的不是 $\ell^{\log \ell}$，而是 ℓ^2）。

(1) 假设 f: $A \to A'$ 是到真子集 $A' \subsetneq A$的一个 p-等势。令 n_0 满足：对于所有 $n \geq n_0$，f 在长度为 ℓ 的字符串上的运行时间严格小于 $\ell^{\log \ell}$。那么，f 不可能将 A 中长度至多为 n_0 的任何字符串映射到长度为 $> n_0$的字符串，因此我们必须有，f 给出了 $A \cap \Sigma^{\leq n_0}$ 与 $A' \cap \Sigma^{\leq n_0}$之间的一个双射；又因为 $A' \subseteq A$，实际上 A' 必须在$\Sigma^{\leq n_0}$上与 A 一致。

但对于长度为 $\geq n_0$, f 的字符串，必须是长度不增的，因为对于这样的字符串，$f(x)$ 没有足够的时间在 A 中写出更长的字符串。但由于 f 已经是从 A 中长度为 $\leq n_0$ 的字符串到其自身的双射，任何长度为 $\geq n_0$ 的 $x \in A$ 都只能映射到自身。因此，对于长度为 $\geq n_0$ 的字符串，f 必须是恒等映射。因此 $A' = A$。

(2) 设 B 与 A 有限差异于 B'。

($\Rightarrow$) 假设 $||B||_p = ||B'||_p$；令 f: $B \to B'$ 为一个 p-等势。令 n_0 表示比满足以下条件的任意字符串 x 的最大长度大 1 的数：$B(x) \neq A(x)$ 或 $B'(x) \neq A(x)$。注意，长度超过 n_0 时，B、B' 与 A 一致，因此它们的元素之间有相同的 $\ell^{\log \ell}$ 间隔。因此，如上所述，存在某个 $n_1 \geq n_0$，使得 f 和 f^{-1} 都无法将任何长度为 $\leq n_1$ 的字符串映射到长度为 $> n_1$ 的字符串。但这样一来，f 必须将 $B \cap \Sigma^{\leq n_1}$ 双射到 $B' \cap \Sigma^{\leq n_1}$（将逆映射 f^{-1} 限制在 $B' \cap \Sigma^{\leq n_1}$ 上）。

现在，令 $P = B\backslash A$、$N = A\backslash B$，并类似地用 B' 替换 B 来定义 P'、N'。那么 $f|_{\Sigma^{\leq n_1}}$ 给出了从 $[(A \cup P)\backslash N] \cap \Sigma^{\leq n_1}$ 到 $[(A \cup P')\backslash N'] \cap \Sigma^{\leq n_1}$ 的一个双射。由于 P、N、P'、$N' \subseteq \Sigma^{\leq n_1}$——这是 n_1 定义的一部分——且它们是有限集，并且 P、P' 与 A 不相交，而 N、N' 是 A 的子集，因此必有 $|P| - |N| = |P'| - |N'|$。

($\Leftarrow$) 令 n_0、P、P'、N、N' 如上所述，并假设 $|P| - |N| = |P'| - |N'|$。下面的映射 f 是一个 p-等势 $B \to B'$。对于长度为 $\leq n_0$ 的字符串，f 实现了一个任意的、硬编码的双射，将 $[(A \cup P)\backslash N] \cap \Sigma^{\leq n_0}$ 映射到 $[(A \cup P')\backslash N'] \cap \Sigma^{\leq n_0}$，因为二者都是基数相同的有限集。对于长度为 $> n_0$ 的字符串，f 是恒等映射。

(3) 与 (2) 类似。对于 ($\Rightarrow$) 方向，设 f: $B \to B'' \subseteq B'$ 是一个 p-等势。如上所述，对于 B 中所有足够长的字符串，f 必须是恒等映射；也就是说，字符串长度大于某个长度 n_1。但这样一来，f 就给出了一个双射 $B \cap \Sigma^{\leq n_1} \to B'' \cap \Sigma^{\leq n_1} \subseteq B \cap \Sigma^{\leq n_1}$。和前面一样，计数这些有限集便可得知 $|B\backslash A| - |A\backslash B| \leq |B'\backslash A| - |A\backslash B'|$。对于 ($\Leftarrow$) 方向，采用与第 (2) 部分类似的构造即可，其中 f 中硬编码的部分现在是一个单射，而非双射。

□

开放问题 4.29。如果 A、B 是无限语言，并且 $A =^* B$ 中长度为$\leq n$ 的字符串至少有 n^c 个（对某个 $c > 1$，且对所有充分大的 n 都成立），那么必有 $||A||_p = ||B||_p$ 吗？如果再加上 $A \subsetneq B$ 且 $B\backslash A$ 有限呢？如果再进一步，$A \in$P 呢？

事实上，定理 4.28 中的集合甚至没有对数密度！

4.4 p-基数的算术

由于许多版本　选择公理的.....涉及基数算术，我们将发展 p-基数算术 .

命题 4.30（p-基数算术）。如果 $||A||_p = ||A'||_p$ 且 $||B||_p = ||B'||_p$，那么 $||A \oplus B||_p = ||A' \oplus B'||_p$ 且 $||A \times B||_p = ||A' \times B'||_p$。如果 $||A||_p \preceq ||A'||_p$ 且 $||B||_p \preceq ||B'||_p$，那么 $||A \oplus B||_p \preceq ||A' \oplus B'||_p$ 且 $||A \times B||_p \preceq ||A' \times B'||_p$。

定义 $||A||_p + ||B||_p = ||A \oplus B||_p$ 和 $||A||_p \times ||B||_p := ||A \times B||_p$，p-基数构成一个预序半环，其加法单位元为 $||\emptyset||_p$，乘法单位元为 $||\{\epsilon\}||_p$。

此外：

1. 对所有 A，$||\emptyset||_p \times ||A||_p = ||\emptyset||_p$。 2. 对所有 A，$||\emptyset||_p \preceq ||A||_p \preceq ||\Sigma^*||_p$。 3. 若 A 为无限，则对任意有限集合 F，$||A||_p \succ ||F||_p$。 4. 对所有 A，B，$||A||_p \preceq ||A||_p + ||B||_p$。 5. 对所有 A，以及所有非空的 B，$||A||_p \preceq ||A||_p \times ||B||_p$。 6. 有限集的 p- 基数构成一个全序子半环，它作为有序半环同构于 $(\mathbb{N}, +, \times, \leq, 0, 1)$。

7. 对于所有有限非空语言 n 和所有语言 A，有 $||n \times A||_p = ||A \oplus A \oplus \cdots \oplus A||_p$，其中后一个求和有 $|n|$ 项。

证明。设 $f\colon\ A \to A''$ 是某个 $A'' \subseteq A'$ 的 p-等势，且 $g\colon\ B \to B''$ 是某个 $B'' \subseteq B'$的 p-等势。那么，定义为

$$(f \oplus g)(bx) = \begin{cases} f(x) & \text{if } b = 0 \\ g(x) & \text{if } b = 1 \end{cases}$$

是一个 p-等势 $A \oplus B \to A'' \oplus B'' \subseteq A' \oplus B'$，其逆映射为 $f^{-1} \oplus g^{-1}$。类似地，定义为 $(f \times g)(x, y) = (f(x)\ g(y))$ 的 $f \times g$ 是一个 p- 等势 $A \times B \to A'' \times B'' \subseteq A' \times B'$，其逆映射为 $f^{-1} \times g^{-1}$。由此得到关于 $\preceq$的所需结论；由于 $\preceq$ 只是一个预序，关于 $=$ 的结论并不能立即推出。然而，如果在证明中取 $A'' = A'$ 和 $B'' = B'$，那么就能得到关于 $=$的所需结论。

最后请注意，$A \oplus \emptyset = \{0x\colon\ x \in A\}$，很容易看出它与$A$具有相同的 p-基数。类似地，$A \times \{b\} = \{(a, b)\colon\ a \in A\}$ 很容易看出也与 A具有相同的 p-基数。其余性质留给读者作为练习。□

备注 4.31。请注意，算术运算和比较在 p-基数的$\equiv$-等价类上也定义良好（其中若 $||A||_p \preceq ||B||_p$ 则 $||A||_p \equiv ||B||_p$ 和 $||B||_p \preceq ||A||_p$），此时所得结构是偏序半环，而不只是预序。

观察 4.32。$||\Sigma^*||_p = ||\Sigma^*||_p + ||\Sigma^*||_p$ 和 $||\Sigma^*||_p = ||\Sigma^*||_p \times ||\Sigma^*||_p$。

证明。令 n_x 表示与 x 关联的自然数（见预备知识），令 σ_n 表示与自然数 n关联的字符串。双射 $\Sigma^* \to \Sigma^* \oplus \Sigma^*$ 定义如下

$$f(x) = \begin{cases} 0\sigma_{n_x/2} & \text{if } n_x \text{ is even} \\ 1\sigma_{(n_x-1)/2} & \text{if } n_x \text{ is odd} \end{cases}$$

其逆映射为

$$f^{-1}(by) = \begin{cases} \sigma_{2n_y} & \text{if } b = 0 \\ \sigma_{2n_y+1} & \text{if } b = 1 \end{cases}.$$

对于直积，我们使用任意一种标准双射 $\Sigma^* \to \Sigma^* \times \Sigma^*$（例如，使用上面的双射 n、σ 将其转换为 $\mathbb{N}$，并使用标准双射 $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$）。□

推论 4.33. 如果 A 是 p-可数的，那么

$$A \cong^p \overline{A} \qquad \iff \qquad \overline{A} \text{ is } p\text{-countable},$$

并且如果这些条件成立，那么 $A \cong^p A \times \Sigma^*$（即 A 是一个 p-圆柱）。

开放问题 4.34。如果仅有 $||A||_p = ||A \times \Sigma^*||_p$ 和 $||\overline{A}||_p = ||\overline{A} \times \Sigma^*||_p$，能得出什么结论?

证明。假设 A 是 p-可数的。正向由 p-同构保持 p-可数性这一事实得出。反向则利用推论 4.19 和 $A = B$ 得出。

对于最后一个陈述，假设 A、$\overline{A}$ 都是 p-可数的。证明思路与 Goldsmith、Kunen 和 Hemaspaandra [27] 以及推论 4.19 的思路类似。由于 $||A||_p = ||\Sigma^*||_p$ 和 $||\Sigma^*||_p = ||\Sigma^*||_p \times ||\Sigma^*||_p$，我们可以用 A 替换左边和右边其中一个，从而得到 $||A||_p = ||A||_p \times ||\Sigma^*||_p = ||A \times \Sigma^*||_p$。对 $\overline{A}$ 也同样如此。现在令 $f\colon\ A \to A \times \Sigma^*$ 和 $g\colon\ \overline{A} \to \overline{A} \times \Sigma^*$ 为 p-等势映射。那么函数

$$h(x) = \begin{cases} f(x) & x \in A \\ g(x) & x \notin A. \end{cases}$$

是一个 p-可计算双射 $\Sigma^* \to \Sigma^* \times \Sigma^*$，因为 $A \in \mathrm{P}$。要证明它是双射，注意到 $\overline{A \times \Sigma^*} = \overline{A} \times \Sigma^*$。$h$ 的逆映射类似地由以下 p-可计算双射给出

$$h^{-1}(y) = \begin{cases} f^{-1}(y) & y \in A \times \Sigma^* \\ g^{-1}(y) & y \notin A \times \Sigma^*. \end{cases}$$

因此 $A \cong A \times \Sigma^*$，所以 A 是一个圆柱。 □

我们注意到，所有 p-基数组成的集合是不可数无限的：Σ^*有不可数多个子集，而每个 p-基数等价类都只有可数多个代表元，因为能够计算 p-等势映射的图灵机（包括仅部分定义的图灵机）只有可数多个。不过，即使是在有趣的可数 p-基数集合中，我们仍认为:

猜想 4.35。对于任意标准复杂性类 $\mathcal{C} \supseteq \mathrm{P}$（例如 P、NP、PSPACE、EXP 等），其中 $\mathcal{C}$ 语言的 p-基数半环都不是有限生成的。p-基数等价类的半环（见备注 4.31）也同样如此。

对于普通基数，$\aleph_0$ 是最小的无限基数，而每个无限基数 $\mathfrak{c}$ 都满足 $\mathfrak{c} + \aleph_0 = \mathfrak{c}$。然而，对于 p-基数，情况不再如此:

命题 4.36. 若 A 是 P-免疫的，则 $||A||_p \not\succeq ||A||_p + ||\Sigma^*||_p$。

证明。假设 $||A||_p + ||\Sigma^*||_p \preceq ||A||_p$。由于左边等于 $||A \oplus \Sigma^*||_p$，我们有一个从 $A \oplus \Sigma^*$ 到子集 $A' \subseteq A$的 p-等势映射 f。于是，将 f 限制在 $1\Sigma^*$ 上，就得到一个到子集 $A'' \subseteq A' \subseteq A$的 p-等势映射。因此，$A''$ 是 p-可数的，故由命题 4.2 可知它属于 P。所以 A 包含一个无限的 P 子集，这与其 P-免疫性矛盾。 □

命题 4.37（加法的不可消去性，Nerode & Remmel [51, 定理 7]）。存在语言 A, B, C，使得 $||A \oplus B||_p = ||A \oplus C||_p$，但 $||B||_p \neq ||C||_p$。

Nerode & Remmel 对一元语言证明了这一结果，虽然使用的定义略有不同，但他们相同的构造也适用于我们的定义。

Nerode & Remmel [51, 定理 10] 还证明了，对一元字符串的有限集合可以使用乘法消去律。他们的论证采用了往返构造，要求他们

计算字符串所有前驱上的函数。由于他们使用的是一元语言，这样的前驱只有线性多个，因此整个论证都可以在多项式时间内完成。若我们尝试在自己的设定中采用相同方法，例如使用长度字典序，一个字符串就会有指数多个前驱（相对于其长度呈指数增长），所以同样的策略行不通。使用某种 p良基序（见定义 6.1）或许可以奏效，只要其直接前驱能在 FP 中计算出来；但我们尚未能使这一方法奏效，因此将其留作一个问题：

开放问题 4.38（有限 p-基数除法）。对于任意非空有限语言 n 以及任意语言 A, B，$||n \times A||_p = ||n \times B||_p$，是否有 $||A||_p = ||B||_p$?

4.5 基于 p-基数的多项式时间选择公理

经典选择公理 4（参见 [54, CN6 和 CN7，第 52–53] 页）。对于任意基数 $m < n$ 和 $p < q$，$m + p < n + q$ 和 $mp < nq$。

与命题 4.30 比较。

经典选择公理 5（塔斯基定理 [66], 参见 [54, CN 3，第 52] 页）。对于每个无限集 A，A 与 $A \times A$之间存在双射。

多项式时间选择公理（PAC）4。对于每个无限语言 $L \in$ P，$||L||_p = ||L \times L||_p$。

经典选择公理 6（三分律 [54, T，第 9] 页）。对于所有集合 A、B，要么 A 与 B 的某个子集之间存在双射，要么 B 与 A的某个子集之间存在双射。

基于密度考量，这一命题的一个直接的多项式时间版本是错误的：

命题 4.39。P 中存在两个语言，它们的 p-基数不可比较。

证明。令 $tow(0) = 1$和 $tow(n+1) = 2^{tow(n)}$为塔函数。A_0将由所有长度为 $tow(2k) \leq |x| < tow(2k+1)$ 的字符串 x 组成，其中 $k \geq 0$取遍所有值；而 A_1 将由所有长度为 $tow(2k+1) \leq |x| < tow(2k+2)$ 的字符串组成，其中 $k \geq 0$取遍所有值。显然，A_0、A_1 都属于 P。其思路是，它们的密度会无限多次地在 $\Theta(n)$ 和 $2^{\Theta(n)}$ 之间波动，但发生的时机相反。下面来验证这一点。

对于长度范围 $[\frac{1}{2}tow(2k+2)\ tow(2k+2))$，$A_0$中的所有字符串长度均为 $< tow(2k+1)$，因此它们最多有 $2^{tow(2k+1)+1} - 1 \sim tow(2k+2)$ 个。所以在这些范围内，我们有$c_{A_0}(n) \in [n/2, n]$。在同一范围内，所有字符串都存在于 A_1中，因此我们有 $c_{A_1}(n) \geq 2^n$，这几乎是最大的。对于长度范围 $[\frac{1}{2}tow(2k+1)\ tow(2k+1))$，情况则相反。

为了导出矛盾，假设 $B \subseteq A_0$ 具有 $||B||_p = ||A_1||_p$。由于在长度范围 $[tow(2k+1)\ tow(2k+2))$ 内，A_0 为空，B也为空，因此对于范围 $[\frac{1}{2}tow(2k+2)\ tow(2k+2)]$内的 n，B 的密度至多为 $O(n)$。但在此范围内，A_1的密度至少为 2^n，所以对于任意大的长度区间，两者都不是多项式相关的，这就产生了矛盾。交换 A_0 和 A_1 的角色，并改用范围 $[tow(2k)\ tow(2k+1))$，可用类似论证排除 A_1 的某个子集具有与 A_0相同的 p-基数。因此 $||A_0||_p$ 和 $||A_1||_p$ 不可比较。

□

因此，我们提出一种在假设中包含密度的多项式时间形式的选择公理。

多项式时间选择公理（PAC）5. 对于所有密度多项式相关的集合 A、$B \in$ P，要么$||A||_p \preceq ||B||_p$，要么 $||B||_p \preceq ||A||_p$。

如果去掉两个语言都属于 P 这一限制，我们认为该命题就不成立了。

经典选择公理 7（三分律 [54, T’，第 10] 页）。对于任意两个非空集合，都存在一个从其中一个到另一个的满射映射。

多项式时间选择公理（PAC）6. 对任意两个非空语言 A, B，若 $c_A(n) \leq c_B(\text{poly}(n))$，则存在一个诚实的多项式时间满射函数 $A \to B$。

在经典情形中，T 蕴含 T’。对于 p-类比，这种蕴含似乎等同于假设 Q，尽管要将其形式化已被证明颇为棘手。不过，我们确实有：

经典选择公理 8. 每个满射函数都有一个右逆。

多项式时间选择公理（PAC）7. 每个多项式时间可计算、诚实的满射函数都有一个多项式时间逆函数。这是对假设 Q 的精确重述。

经典选择公理 9（参见 [54, 第 6 节，第 52–53] 页）。选择公理的基数形式。全文中，m, n, p, q 表示无限基数。若未注明量词，则默认采用全称量化，例如，第一个条件更准确地说是“对于所有无限基数 m, n，$m \cdot n = m + n$。”

1. $m \cdot n = m + n$。
2. 存在一个基数 n，使得 $m = n^2$。
3. 如果 $m^2 = n^2$，那么 $m = n$。
4. 如果 $m + p < n + p$，那么 $m < n$。
5. 如果 $mp < np$，那么 $m < n$。
6. 每个基数都有一个直接后继（$m < n$，并且如果 $m < p$，那么 $n \leq p$）。
7. 如果 $n < p$，且 n 与 p 之间不存在基数（即 p “覆盖” n），那么 $mn = mp$ 或 mp 覆盖 mn。（如果 p 是 n 的直接后继，那么 p 覆盖 n。反命题等价于选择公理。）
8. 如果 $m < n$，那么存在一个 p，使得 $n = mp$。
9. 如果 $m < n$，那么 n/m（如前一点所述）存在且唯一。
10. 如果 $m < n$，那么 $n/m = n$。
11. 如果 $m + p = m + q$，那么要么 $p = q$，要么 $p \leq m$ 且 $q \leq m$。
12. 如果 $m + m < m + n$，那么 $m < n$。（反命题独立于选择公理。）
13. 若 $m < n$，则 $n - m$ 存在，也就是说，存在且仅存在一个 p，使得 $n = m + p$。（仅存在性与选择公理无关。）
14. 若 $m < n$，则 $n - m = n$。
15. 若 $p < n$、$q < n$，则 $p + q \neq n$。
16. 若 $p < n$、$q < n$，则 $pq \neq n$。
17. $mn = m$ 或 $mn = n$。

许多关于这些命题彼此等价且与标准选择公理等价的论证，都依赖于基数的直接后继这一概念（例如，[54]）。我们通过一个 Ladner 型对角化结果表明，对于（无限）p-基数而言，这样的构造不太可能存在。

在介绍该结果之前，我们当前的证明还使用了一个额外的假设，这主要是因为定理 4.28 所提出的问题。

定义 4.40（小得多的 p-基数）。如果 $||A||_p \prec ||B||_p$，并且对于满足 $||A||_p = ||B'||_p$ 的任意子集 $B' \subseteq B$，差集 $B\backslash B'$ 是无限的，则称 $||A||_p$ 比 $||B||_p$ 小得多，记作 $||A||_p \ll ||B||_p$。

下一个命题表明，$\ll$ 实际上是 p-基数类上的一个定义良好的关系。

命题 4。41. 若 $||A||_p = ||A||_p$ 且 $||B||_p = ||B||_p$，则 $||A||_p \ll ||B||_p$ 当且仅当 $||A||_p \ll ||B||_p$。

证明。假设 $||A||_p \ll ||B||_p$，我们证明 $||A||_p \ll ||B||_p$，反向蕴含可由对称性得出。若 $||A||_p = ||A||_p$，$B' \subseteq B$，$||A||_p = ||B'||_p$，$||A||_p =$，则 $||B'||_p$，$||A||_p \ll ||B||_p$，$||B||_p = ||B||_p$，$B' \subseteq B$ 对于任意子集，我们有 当且仅当，因此有。现在假设，并令 与 具有相同的 p-基数。令 f: $B \to B$ 为一个 p-等势映射，并定义 $B' = f($$B')$。于是我们有$||A||_p = ||B'||_p$，根据假设，$B\backslash B'$ 是无限的。但由于 f^{-1} 在 B 上是单射，$f^{-1}(B\backslash B') = B\backslash B'$ 也必然是无限的。□

显然，对于任意无限的 A，有限集都小得多；不过我们也有一些不那么显然的例子。

命题 4.42. 1.若 $A \subset B$ 和 $A \not\equiv_m^p B$，则 $||A||_p \ll ||B||_p$。

2. 若 $A \not\equiv_m^p B \neq \Sigma^*$，则 $||A||_p \ll ||\Sigma^* \oplus B||_p$。

证明. 1. 若 $A \subset B$，则 $||A||_p \preceq ||B||_p$。若 $A \not\equiv_m^p B$，假设 $B' \subset B$ 与 A 的 p-基数相同。由于 A、B' 都是 B 的真子集，因此它们都不可能是 Σ^*，所以由命题 4.2 可知 $A \equiv_m^p B'$。但由于 $B \not\equiv_m^p A$，我们必有 $B \not\equiv_m^p B'$，因而 $B\backslash B'$ 必须是无限的。

2. 定义 $B = \Sigma^* \oplus B$ 和 $A = 0A$。由于 $B \equiv_m^p B$ 和 $A \equiv_m^p A$，我们仍有 $A \not\equiv_m^p B$，现在 我们有 $A \subseteq B$。第 1 部分意味着 $||A||_p \ll ||B||_p$，而命题 4.41 随即也给出 $||A||_p \ll ||B||_p$。□

警告！“小得多”遗憾的是不具有传递性。假设 $A \not\equiv_m^p B \neq \Sigma^*$。将前一个命题的第 2 部分应用几次，我们得到 $||A||_p \ll ||\Sigma^* \oplus B||_p \ll ||\Sigma^* \oplus A||_p \ll ||\Sigma^* \oplus \Sigma^* \oplus B||_p = ||\Sigma^* \oplus B||_p$。但显然 $||\Sigma^* \oplus B||_p$ 等于自身，因此它不可能比自身小得多。乍看之下，这似乎表明存在某种错误，但实际上，这是 p-基数混合了子集和多对一度这一事实所导致的自然结果，而子集包含偏序集与多对一归约偏序集并不兼容。也就是说，存在语言序列 $L_1 \subset L_2 \subset L_3$，其中 L_2 是 NP 完全的，但 $L_1, L_3 \in$ 属于 P，例如，对于任意 $L_1 \in \in$P，$0L_1 \subseteq \Sigma^* \oplus SAT \subseteq \Sigma^*$。

相比之下，“$\preceq$ 但不是 $\ll$”（“较小，但没有小很多”）这一关系具有传递性。因为如果A 与 B的某个余有限子集 p-等势，且 B 与 C的某个余有限子集 p-等势，那么将这两个 p-等势复合起来，就得到 A 与 C的某个余有限子集之间的 p-等势关系。在下面的证明中，我们将多次使用这一事实（以其逆否命题的形式）。

定理 4.43。设 A、B 为满足 $||A||_p \ll ||B||_p$的语言。则存在一个无限语言C，满足 $||A||_p \prec ||C||_p \prec ||B||_p$。

由于定理 4.28，这里的假设并不等价于 $||A||_p \prec ||B||_p$；我们将在下面的推论 4.48 中看到，定理 4.28 中构造的同一个集合可以用来给出集合 A、B 的一个例子，其中有 $||A||_p \prec ||B||_p$，但两者之间不存在严格的 p-基数。沿着

问题 4.29 的思路，探讨在什么条件下定理 4.43 可以在较弱的假设 $||A||_p \prec ||B||_p$ 下成立，和/或具有较强的结论 $||A||_p \ll ||C||_p \ll ||B||_p$，是很有趣的。就目前情况而言，我们必然有 $||A||_p \prec ||C||_p$ 和 $||C||_p \prec ||B||_p$ 中至少一个可以转化为 $\ll$，否则我们就不可能有 $||A||_p \ll ||B||_p$；但我们的构造无法控制究竟是哪一个。

证明。根据假设，存在一个从 A 到 B 的某个余无限子集的 p-可计算、p-可逆双射，但反过来则不成立。（注意，B 不可能是有限的。）为简化下文的记号，我们将 A 与其在此双射下的像视为同一对象，因此不失一般性，可以假设事实上 $A \subsetneq B$ 和 $B\backslash A$ 是无限的。我们将构造 C，使得 $A \subsetneq C \subsetneq B$ 且 $||A||_p \prec ||C||_p \prec ||B||_p$。由于 $A \subseteq C \subseteq B$，因此有 $||A||_p \preceq ||C||_p \preceq ||B||_p$。所以，只需在 A 与 B 之间构造 C，同时避免 p-可计算、p-可逆双射 $C \to A$ 和 $B \to C$。

令 $M_1, M_2, \ldots$ 是图灵机转换器的一个枚举；对于所有 c，令 M_c 表示由 M_c 得到的机器：将 M_c 限制为对每个长度为 n 的输入运行不超过 $cn^c + c$ 步。如果 $M_c(x)$ 在运行 $c|x|^c + c$ 步后仍未产生输出，那么 $M_c(x)$ 将拒绝 x（即不产生任何输出）。显然，$M_1, M_2, \ldots$ 因此构成了所有部分多项式时间图灵机转换器的一个枚举。

构造。我们分阶段 $s = 0, 1, 2, \ldots$ 构造 C。我们还构造一个字符串集合 E，将其从 C 中排除。对于每个 $s \in \mathbb{N}$，C_s 和 E_s 将分别是 C 和 E 的部分，并在阶段 s 结束时枚举出来。该构造将保证，对于每个 s，$C_s \cap E_s = \emptyset$、$A \subseteq C_s \subseteq C_{s+1} \subseteq B$、$C_s$ 与 A 有限差异，且 E_s 有限。

我们需要满足两组要求；当 $s \equiv 0$（模 3）时，我们会向 C_s 中添加元素，以确保 C 是无限的。当 $s \equiv 1$（模 3）的阶段 $s+1$（相应地，$s \equiv 1$ 同余于 2（模 3）的阶段）将确保第一组（相应地，第二组）要求在该阶段得到满足。为便于下文验证时引用，我们将构造分成编号情形。

阶段 $s = 0$。集合 $C_0 = A$ 和 $E_0 = \emptyset$。

阶段 $s+1$，其中 $s \equiv 0$ (模 3)。令 y 为 $B\backslash(C_s \cup E_s)$ 的最小元素（任意元素均可），并设 $C_{s+1} := C_s \cup \{y\}$ 和 $E_{s+1} := E_s$。（这样的 y 必定存在，因为 $B\backslash A$ 是无限的，C_s 与 A有限差异，且 E_s 是有限的。）

阶段 $s+1$，其中 $s = 3\langle \alpha, \beta \rangle + 1$。（这里我们用 $\langle \bullet, \bullet \rangle$ 表示一个双射 $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$。）

情况1：$M_\alpha|_A$: $A \to M_\alpha(A)$ 不是 p-等势，或者 $M_\alpha(A) \not\subseteq B$，或者 M_β 不是其逆 p-等势 $M_\alpha(A) \to A$。在这种情况下，设 $C_{s+1} := C_s$ 和 $E_{s+1} := E_s$，并继续到下一阶段（$s+2$）。

情况2：否则。注意，在这种情况下，$B\backslash M_\alpha(A)$ 必须是无限的，因为 $||A||_p = ||M_\alpha(A)||_p$，但$|A||_p \ll ||B||_p$。令 $Y = B\backslash E_s$；由于 E_s 是有限的，Y在 B中是余有限的。根据假设，$||A||_p \ll ||B||_p$，但 Y在 B中是余有限的，因此 $||A||_p$ 不可能等于 $||Y||_p$。

子情况2.1：$Y \not\subseteq \text{dom}(M_\beta)$。在此子情况中，令 y为 $Y \setminus \text{dom}(M_\beta)$ 的最小元素（任取一个元素即可），设 $C_{s+1} : = C_s \cup \{y\}$，$E_{s+1} : = E_s$，然后进入下一阶段。

子情况2.2：不属于前一个子情况，且 M_β 在 Y上不是单射。在此子情况中，令 y_1、$y_2 \in Y$为 M_β 映射到同一位置的两个最小的不相同元素（任取两个即可）。设 $C_{s+1} : = C_s \cup \{y_1, y_2\}$ 以及 $E_{s+1} : = E_s$，然后继续进入下一阶段。

子情况2.3：不属于之前的子情况，且 $M_\beta(Y) \not\subseteq A$。在此子情况中，令 y为 Y中满足 $M_\beta(y) \notin A$ 的最小元素（任意一个都可以），设 $C_{s+1} := C_s \cup \{y\}$, $E_{s+1} := E_s$，然后进入下一阶段。

子情形2.4：不属于前面的子情形。在此子情形中，必定存在 $y \in Y$ 使得$M_\alpha(M_\beta(y)) \neq y$；因为此时我们有，$M_\beta|_Y$ 是从Y到 A的单射函数，所以如果 M_α 是其逆映射，我们就会得到 $||A||_p = ||Y||_p$（因为我们已经知道

$(M_\beta \circ M_\alpha)|_A = id_A$），而我们已在上文证明这是不可能的。令 y 为满足条件的最小者（任意一个都可以），设 $C_{s+1} := C_s \cup \{y\}$, $E_{s+1} := E_s$，然后进入下一阶段。

阶段 $s+1$，其中 $s = 3\langle \alpha, \beta \rangle + 2$。

情况1：在以下任一子情形中，令 $C_{s+1} := C_s$、$E_{s+1} := E_s$，然后进入下一阶段。

子情形 1.1：$M_\alpha(C_s) \not\subseteq B$。子情形 1.2：并非 $M_\alpha|_{C_s}$：$C_s \to M_\alpha(C_s)$ 是一个逆映射为 M_β 的 p-等势映射。子情形 1.3：$X := B \backslash (M_\alpha(C_s) \cup E_s)$ 不包含于 $\mathrm{dom}(M_\beta)$ 中。子情形 1.4：不属于上述子情形，且 $M_\beta(X) \subseteq C_s$。

情况2：不属于上述任何子情形。在这种情况下，令 x 为满足 $M_\beta(x) \notin C_s$ 的 X 的最小元素（任取这样的元素即可），令 $E_{s+1} := E_s \cup \{x\}$、$C_{s+1} := C_s$，然后进入下一阶段。（注意，这样的 x 必然存在，因为 E_s 是有限的，且 M_α 是从一个与 A 存在有限差异的集合到 B 的某个子集的 p-等势映射，但 $||A||_p \ll ||B||_p$。）

至此，阶段 $s+1$ 的描述以及整个构造的描述便告完成。

要求。下面我们将证明，除了确保 C 是无限的之外，该构造还满足两组要求，并且这些要求蕴含 C 所需的性质。为陈述这些要求，定义 $E = \bigcup_s E_s = \lim_{s\to\infty} E_s$。关于 (α, β) 的要求如下：

$\mathrm{R}1_{\alpha,\beta}$：以下条件至少有一个成立：(a) $A \not\subseteq \mathrm{dom}(M_\alpha)$ 或 M_α 在 A 上不是单射；(b) $C \not\subseteq \mathrm{dom}(M_\beta)$ 或 M_β 在 C 上不是单射；(c) $M_\alpha(A)$ 不包含于 B（原文如此！）；(d) $M_\beta(C)$ 不包含于 A；(e) 存在 $a \in A$，使得 $M_\beta(M_\alpha(a)) \neq a$，或者存在 $c \in C$，使得 $M_\alpha(M_\beta(c)) \neq c$。$\mathrm{R}2_{\alpha,\beta}$：以下条件至少有一个成立：(a) $C \not\subseteq \mathrm{dom}(M_\alpha)$ 或 M_α 在 C 上不是单射；(b) $B \not\subseteq \mathrm{dom}(M_\beta)$ 或 M_β 在 B 上不是单射；(c) $M_\alpha(C)$ 不包含于 B；(d) $M_\beta(B) \cap E$ 非空；(e) 存在 $c \in C$，使得 $M_\beta(M_\alpha(c)) \neq c$，或者存在 $b \in B$，使得 $M_\alpha(M_\beta(b)) \neq b$。

这些要求已经足够。首先来看，这些要求加上 C 是无限的，足以得到该定理。要求 $\mathrm{R}1_{\alpha,\beta}$ 意味着 M_α 不是一个逆映射为 M_β的 p-等势 $A \to C$，而 $\mathrm{R}2_{\alpha,\beta}$ 意味着 M_α 不是一个逆映射为 M_β 的 p- 等势 $C \to B$（注意，$\mathrm{R}2_{\alpha,\beta}$(d) 确保 $M_\beta(B) \not\subseteq C$，因为 E 与 C 不相交）。由于 (α, β) 遍历了多项式时间图灵机的一个完备列表，这些要求将确保 $||A||_p \prec ||C||_p \prec ||B||_p$。

阶段 $s+1 \equiv 0 \pmod 3$ 会不断向 C添加元素，从而确保 C是无限的，即使 A 是有限的。

要求的验证。首先指出，这是一个“无伤害”论证：一旦某项要求得到满足，它就不会再变得不满足（“不会再受到伤害”）。这是因为每项要求都是一个 $(\Sigma_1^0)^{A\oplus B}$ 语句，也就是说，它的形式为 $(\exists \vec{x})[P(\vec{x})]$，其中$P$是一个谓词，可借助关于 A 和 B 的预言机计算得出。因此，只需证明在阶段 $s+1 = 3\langle \alpha$ 结束时，$\beta\rangle + b$，如果 C'、E'是满足 $C_s \subseteq C' \subseteq B$、$E_s \subseteq E' \subseteq B\backslash C'$的任意两个集合，那么用 C'（分别是 E'）替代 C（分别是 E）后，$\mathrm{R}b_{\alpha,\ \beta}$ 仍然得到满足。

注 4.44。为确保这一 $(\Sigma_1^0)^{A\oplus B}$ 性质，我们注意到，$\mathrm{R}1_{\alpha,\beta}$ 比确保 M_α 不是一个以 M_β 为逆映射的 p-等势映射 $A \to C$ 所需的条件略强；类似地，$\mathrm{R}2_{\alpha,\beta}$ 也比确保 M_α 不是一个以 M_β 为逆映射的 p-等势映射 $C \to B$ 所需的条件略强。特别地，如果 $\mathrm{R}1_{\alpha,\beta}$(c) 仅仅是“$M_\alpha(A) \neq C$”，而 $\mathrm{R}1_{\alpha,\beta}$(d) 是“$M_\beta(C) \neq A$”，那么避免 p-等势映射就足够了；但这些语句在 $A \oplus B$ 中就不会是 Σ_1^0，因为之后加入 C 的元素可能会违反这样的条件。类似地，如果 $\mathrm{R}2_{\alpha,\beta}$(c) 仅仅是“$M_\alpha(C) \neq B$”，而 $\mathrm{R}2_{\alpha,\beta}$(d) 仅仅是“$M_\beta(B) \neq C$”，那么避免 p-等势映射就足够了，但同样无法如此明确地避免未来向 C 添加元素所造成的伤害。

阶段 $s+1$ 通过 $s = 3\langle\alpha,\beta\rangle + 1$ 确保 $\mathrm{R}1_{\alpha,\beta}$ 成立。我们按照构造中的各种情况，将验证分情况进行。

情况1。如果 $M_\alpha|_A\colon A \to M_\alpha(A)$ 与子集 $M_\alpha(A) \subseteq B$ 并非 p-等势，且其逆映射为 M_β，那么构造中的情况1告诉我们转到下一阶段。因此，我们必须证明，在这种情况下，不对 C_s, E_s作任何进一步修改，R1 已经成立。

在这种情况下，以下情况必有一种成立：

(A) $A \not\subseteq \mathrm{dom}(M_\alpha)$ 或 M_α 在 A上不是单射。(B) $M_\alpha(A) \not\subseteq B$。(C) $M_\alpha(A) \not\subseteq \mathrm{dom}(M_\beta)$ (D) M_β 在 $M_\alpha(A)$ 上不是单射 (E) $M_\beta(M_\alpha(A)) \not\subseteq B$(F) M_α 和 M_β 在 $A, M_\alpha(A)$ 上分别互不为逆映射。也就是说，存在某个 $a \in A$，使得 $M_\beta(M_\alpha(a)) \neq a$；或者存在某个 $b \in M_\alpha(A)$，使得 $M_\alpha(M_\beta(b)) \neq b$。后者等价于存在某个 $a \in A$，使得 $M_\alpha(M_\beta(M_\alpha(a))) \neq M_\alpha(a)$。

假设 (A) 成立。(A) 等同于 $\mathrm{R}1_{\alpha,\ \beta}$(a)，因此 $\mathrm{R}1_{\alpha,\ \beta}$ 成立。

假设 (B) 成立。(B) 等同于 $\mathrm{R}1_{\alpha,\ \beta}$(c)。

假设 (C) 成立。那么存在一个 $a \in A$，使得 $M_\alpha(a) \notin \mathrm{dom}(M_\beta)$，因此 $M_\beta(M_\alpha(a)) \neq a$，因为左端项未定义，所以 $\mathrm{R}1_{\alpha,\ \beta}$(e) 成立。

假设 (D) 成立。那么存在互不相同的 a_1、$a_2 \in A$，使得 $M_\beta(M_\alpha(a_1)) = M_\beta(M_\alpha(a_2))$。但这样一来，对于 $i = 1$，2，$M_\beta(M_\alpha(a_i)) = a_i$ 中至少有一个必须不成立，因此 $\mathrm{R}1_{\alpha,\ \beta}$(e) 成立。

假设 (E) 成立。由于 $M_\beta(M_\alpha(A)) \not\subseteq B$，存在某个 $a \in A$，使得 $M_\beta(M_\alpha(a)) \notin B \supseteq A$，所以必有 $M_\beta(M_\alpha(a)) \neq a$，因此 $\mathrm{R}1_{\alpha,\ \beta}$(e) 成立。

假设（F）成立。那么必然存在一个 $a \in A$，使得 $M_\beta(M_\alpha(a)) \neq a$。否则，根据（F）的第二部分，我们可以得到存在一个 a，使得

$$M_\alpha(M_\beta(M_\alpha(a))) \neq M_\alpha(a).$$

但是，如果对于所有 $a \in A$ 都有 $M_\beta(M_\alpha(a)) = a$，那么所显示的方程将简化为 $M_\alpha(a) \neq M_\alpha(a)$，这是荒谬的。因此，$\mathrm{R}1_{\alpha,\beta}$(e) 得到满足。

因此，情况1 确保了 $\mathrm{R}1_{\alpha,\beta}$，正如所声称的那样。

情况2。现在假设我们处于情况2，其中 $M_\alpha|_A\colon A \to M_\alpha(A)$ 是到 B 的某个子集的 p-等势，其逆映射为 M_β。沿用构造中的记号，令 $Y = B \backslash E_s$。

子情况2.1。如果满足子情况2.1的条件（$Y \not\subseteq \mathrm{dom}(M_\beta)$），那么我们向 C中添加一个 $y \in Y \backslash \mathrm{dom}(M_\beta)$，从而满足$\mathrm{R}1_{\alpha,\ \beta}$(b)。

子情况2.2。在子情况2.2中，如果满足相关条件，我们向 C 中添加彼此不同的 y_1、$y_2 \in Y$，使得 $M_\beta(y_1) = M_\beta(y_2)$。这满足了$\mathrm{R1}_{\alpha,\beta}$(b)的第二部分。子情况2.3。在子情况2.3中，如果满足相关条件，我们向 C 中添加一个 $y \in Y$，使得$M_\beta(y) \notin A$，从而满足$\mathrm{R1}_{\alpha,\beta}$(d)。子情况2.4。在子情况2.4中，如果满足相关条件，我们向 C 中添加一个 $y \in Y$，使得$M_\alpha(M_\beta(y)) \neq y$，从而满足$\mathrm{R1}_{\alpha,\beta}$(e)的第二部分。

由于这些情况和子情形涵盖了所有可能性（情况2是情况1的“其他情况”，而根据构造，子情况2.4涵盖了前面各情况未包含的所有情况），因此这一阶段确保满足 $\mathrm{R1}_{\alpha,\beta}$。

阶段 $s+1 = 3\langle\alpha,\beta\rangle + 2$ 确保 $\mathrm{R2}_{\alpha,\beta}$。沿用构造中的记号，令 $X = B\backslash(M_\alpha(C_s) \cup E_s)$。

情况1。我们必须证明，在这种情况下，无需对 C_s, E_s 做任何进一步更改，R2 就已经满足。

子情形 1.1：$M_\alpha(C_s) \not\subseteq B$。因此我们有 $M_\alpha(C) \not\subseteq B$，这正是 $\mathrm{R2}_{\alpha,\beta}$(c)
.
子情形 1.2：$M_\alpha|_{C_s}$：$C_s \to M_\alpha(C_s)$ 不是具有逆映射 M_β 的 p-等势。在此情形下，$\mathrm{R2}_{\alpha,\beta}$(a)、(b) 或 (e) 中必有一项成立（因为它们合起来就是 p-等势的定义），因此 $\mathrm{R2}_{\alpha,\beta}$ 已经成立。

子情形 1.3：$X \not\subseteq \mathrm{dom}(M_\beta)$。由于根据定义 $X \subseteq B$，$\mathrm{R2}_{\alpha,\beta}$(b) 成立
d.
子情形 1.4：不属于上述子情形，且 $M_\beta(X) \subseteq C_s$。在此情形下，我们声称 M_β 在 B 上不是单射。为证明 M_β 在 B 上不是单射，首先注意，由于我们不处于子情形 1.2，因此 M_β 是 p-等势 $M_\alpha(C_s) \to C_s$，它是 $M_\alpha|_{C_s}$ 的逆映射。因此，M_β 将 $M_\alpha(C_s)$ 双射到 C_s。现在令 $x \in X$，并令 $b = M_\alpha(M_\beta(x))$。根据假设，$M_\beta(X) \subseteq C_s$，所以 $b \in M_\alpha(C_s)$。但根据定义，X 与 $M_\alpha(C_s)$ 不相交，因此 $b \neq x$。然而，由于 M_β、M_α 分别是在 $M_\alpha(C_s)$ C_s 上的逆映射，且根据假设 $M_\beta(X) \subseteq C_s$，我们有 $M_\beta(b) = M_\beta(M_\alpha(M_\beta(x))) = (M_\beta \circ M_\alpha)(M_\beta(x)) = (id)(M_\beta(x)) = M_\beta(x)$。因此，$M_\beta$ 在 B 上不是单射，满足 $\mathrm{R2}_{\alpha,\beta}$(b) 的第二部分。

情况2。在这种情况下，通过添加某个 $x \in X$，将 E_s 扩展为 E_{s+1}，使得 $M_\beta(x) \notin C_s$。由于 $X \subseteq B$，这确保了 $M_\beta(B) \cap E$ 非空，从而满足 $\mathrm{R2}_{\alpha,\beta}$(d)。

由于这些情况和子情形涵盖了所有可能性，因此在这一阶段结束时，要求 $\mathrm{R2}_{\alpha,\beta}$ 得以满足。

综上所述，这一构造确实产生了一个无限集 C，使得 $||A||_p \prec |C||_p \prec ||B||_p$，从而完成了该定理的证明。 □

注 4.45。除了 R1 和 R2 强于实际所需之外（见注 4.44），读者可能还会好奇，为什么 R1 和 R2 并非彼此的完美对应。答案是，我们最初写证明时，二者的形式更加对称，随后才将其精简为最终实际用到的要求部分。

最后，我们注意到，该论证关于 C 几乎是单调的。唯一不关于 C 单调的要求是 $\mathrm{R2}_{\alpha,\beta}$(d)，正是这一要求迫使我们跟踪被排除的字符串集合 E（$\mathrm{R2}_{\alpha,\beta}$(d) 关于 E 是单调的）。

既然 $\aleph_0$ 是唯一的最小无限基数，自然会想知道极小无限 p-基数是否存在。下面的推论对此给出了否定的回答：

推论 4.46（不存在极小无限 p-基数）。对于每个无限 $B \subseteq \Sigma^*$，都存在一个无限集合 C，使得 $||C||_p \prec ||B||_p$。

证明。应用定理 4.43，其中 $A = \emptyset$。 □

我们猜想，可以修改上述证明来对以下更强的问题给出否定答案：

开放问题 4.47。在 $\equiv$ 下，是否存在极小（无限）的 p-基数？也就是说，是否存在一个无限语言 $B \subseteq \Sigma^*$，使得如果 $||C||_p \prec ||B||_p$，那么 C 要么是有限的，要么 $||B||_p \preceq ||C||_p$？

我们在本节最后证明，定理 4.43 中的假设 $||A||_p \ll ||B||_p$ 一般不能替换为 $||A||_p \prec ||B||_p$，即使对于无限语言也是如此（对于有限语言，只要 $|B| = |A| + 1$，这显然成立）；证明如下推论，该推论由定理 4.28 得出：

推论 4.48（无限 p-基数可以有直接前驱）。存在无限语言 A、B，满足 $||A||_p \prec ||B||_p$，使得任意满足 $||A||_p \preceq ||C||_p \preceq ||B||_p$ 的语言 C 都与 A 或 B之一 p-等势。

根据定理 4.43，任何这样的有序对必然不能具有 $||A||_p \ll ||B||_p$。

证明。令 A 为定理 4.28 所保证的集合，令 $w \notin A$，并令 $B = A \cup \{w\}$。假设 C满足 $||A||_p \preceq ||C||_p \preceq ||B||_p$，但 C 不与 B p-等势。我们将证明 C 必与 A p-等势。由于根据假设 $||C||_p \preceq ||B||_p$，存在一个 p-等势 f：将 $C \to C'$ 映射到 $C' \subset B$的一个真子集。由于结论和陈述都不依赖于所选 $||C||_p$ 的代表元，不失一般性，我们可以用 C'替换 C。

由于 $B = A \cup \{w\}$ 和 $C' \subseteq B$，C' 要么是 A的子集，要么是 $A' \cup \{w\}$，其中 $A' \subseteq A$是一个子集。但根据假设，存在从 A 到 C'的某个子集的 p-等势。根据定理 4.28(1)，C'不可能是 A的真子集。如果 $C' = A$，那么结论成立。

因此，剩下的只有处理这样的情况：对于某个 $A' \subseteq A$，$C' = A' \cup \{w\}$。如果 $A' = A$，那么 $C' = B$，这与我们的假设 $||C||_p \neq ||B||_p$矛盾。因此 A' 必定是A的真子集。如果 $|A \backslash A'| \geq 2$，那么令 $w_1 \in A \backslash A'$。于是我们有 $||C'||_p = ||A' \cup \{w\}||_p = ||A' \cup \{w_1\}||_p$。但是$A' \cup \{w_1\}$ 是 A的真子集，这与定理 4.28(1)矛盾。因此 $|A \backslash A'| \leq 2$，并且由于 A' 是 A的真子集，我们必有 $|A \backslash A'| = 1$。于是 $|C' \backslash A| - |A \backslash C'| = |\{w\}| - |A \backslash A'| = 1 - 1 = 0$，因此根据定理 4.28(2)，$||C'||_p = ||A||_p$。 □

5 弱于选择公理的命题

这里我们考察一些由 ZF 上的选择公理蕴含、但尚不确定是否等价于选择公理（或已知严格弱于选择公理）的命题，因为它们的多项式时间类比建立了有趣的联系。

经典结果 1：任意可数个可数集的并集都是可数集。

多项式时间类比 1：如果 L 是一个由语言组成的 P 集合族，L_x 其中每个语言都是 p-可数的，那么 L是 p- 可数的。

人们或许希望结合各个 p-等势映射$L_x \to \Sigma^*$ 以及 $||\Sigma^*||_p = ||\Sigma^* \times \Sigma^*||_p$这一事实，来构造一个 p- 等势映射 $L \to \Sigma^*$。然而，这会遇到这样一个问题：如果 f_x：$L_x \to \Sigma^*$ 是一个 p- 等势映射，那么所有 f_x的运行时间可能不存在统一的多项式上界。反过来，L 本身属于 P 这一事实意味着，判定每个 L_x所需的时间存在统一的多项式上界，因此或许仍有希望证明这一点无条件成立。我们将其留作一个开放问题

开放问题 5.1。证明或反驳 PTA1。选择公理的某个多项式时间版本是否蕴含 PTA1?

经典结果 2. 如果 A 是无限的，则存在从 $\mathbb{N} \to A$ 出发的单射。

这一结论的自然 p-类比并不成立：

推论 5.2. 存在一个无限语言 $L \in$P，使得 $||\Sigma^*||_p \not\preceq ||L||_p$.

这是命题 4.39 的证明的一个推论。

证明. 令 L 为命题 4.39 中构造的语言之一。 $||\Sigma^*||_p \preceq L$ 将意味着 L 是指数稠密的，但 L 是无穷多次线性稀疏的，因此结论成立。 □

经典结果 3（一致化公理）。如果 $R \subset X \times Y$ 其中 X 和 Y 是波兰空间，那么存在一个子集 $f \subseteq R$，它是一个部分函数 $f\colon X \to Y$，并且满足 dom(f) $=\{x \in X | \exists y \in Y (x, y) \in R\}$。

多项式时间类比 2。如果 $X, Y \in$ P 且 $R \subseteq X \times Y$ 也属于 P，那么存在 R 的一个细化 f，使得 f 是一个多项式时间可计算的部分函数，其定义域恰好是 dom(f) $= \{x \in X\colon \exists y \in Y (x, y) \in R\}$。

这是对 NPMV$_g \subseteq_c$ PF 的另一种表述。Blass 和 Gurevich 在大约十年前研究过它 [6]，当时 Selman 尚未引入 NPMV 这一记号 [64]。请注意，我们的一些选择公理的多项式时间版本涉及 NPMV$_t$ 或 NPMV$_{gt}$，但通常尚不清楚 NPMV$_t$ 的塌缩是否意味着 NPMV 的塌缩；这与经典的无界情形不同，在那里选择公理蕴含一致化公理。

6 讨论与未来工作

除了已提出的诸多问题和猜想（问题 1.2、3.7、4.29、4.34、4.38、4.47、5.1、围绕定理 4.25 的问题，以及猜想 4.9 和 4.35）之外，我们还提出几个我们认为值得探索的方向。

关于同构猜想。Joseph 和 Young 提出的、作为同构猜想反例的创造集 [39], ，彼此是否 p-等势? 它们是否与 SAT p-等势? （例如，参见 [43] 的引言，其中综述了相关进展。）回顾一下，若 A 满足 $A \cong^p A \times \Sigma^*$，则称语言 A 为圆柱；这等价于 A 是可填充的。更一般地说，圆柱在围绕同构猜想的研究中发挥着重要作用 [5]。Berman 和 Hartmanis 的主要定理之一 [5] 指出，一个 NP 完全集与 SAT 多项式时间同构，当且仅当它是圆柱。注意，若 A 是圆柱，则 $||A||_p = ||A \times \Sigma^*||_p \succeq ||\Sigma^*||_p$。注意，$A$ 是圆柱，当且仅当 $\overline{A}$ 是圆柱。关于圆柱的基数可以得出什么结论? 如果 A 和 $\overline{A}$ 的 p-基数都等于它们与 Σ^* 的乘积，那么 A 是否必定以某种方式类似于圆柱（参见问题 4.34）?

与其他复杂性概念的联系。假设 μ_p(NP) $\neq 0$ [44]，我们能否解决关于 p-基数或多项式时间选择公理的一些开放问题?

p-基数似乎应该与 Selman 的其他一些研究兴趣存在有趣的联系，例如 p-可选择性 [58, 59, 60, 49, 34], 不相交对 [23, 24, 17, 22], 和有丝分裂性 [20, 19, 18]。

选择公理的若干版本使用良序。在研究自归约性的背景下，Meyer 和 Paterson 提出了一些定义，它们可能有助于构建这些版本的选择公理的多项式时间类比：

定义 6.1（Meyer 和 Paterson [47, 定义 4]）。偏序 $\prec$ 在 Σ^* 上是多项式良序的，如果存在一个多项式 p，使得每条有限的 $\prec$-递减链所含元素不超过 $p(|x|)$ 个，其中 $|x|$ 是链中任一元素的最大长度。

若存在一个多项式时间预言机图灵机 $M^{\square}$ 和一个 p-良序、长度相关序 $\prec$，使得 $L(M^L) = L$，并且对于任意输入 x，$M^L(x)$ 只会在严格 $\prec x$的字符串上查询预言机，则称语言 $L \subseteq \Sigma^*$ 是自可归约的。

Selman 在（至少） [61, 33, 60]中研究了自归约性的这一概念。
经典选择公理 10（见 [54, WE1，第 1] 页）。每个集合都可以良序化。
多项式时间选择公理（PAC）8。P 中的每种语言都存在一个可在 P 中计算的 p-良序。

更一般地说，除选择公理相关论述中使用良序之外，一位匿名审稿人建议，我们也同意，发展一套关于 p-序数的理论会很有意思，类似于本文对 p-基数的研究。我们指出，这既可以通过在 Σ^* 上、可在 FP 中计算的全序来实现，也可以通过在子集 $A \subseteq \Sigma^*$ 上的全序来实现，其中序关系可在 $A \times A$ 上由多项式时间多值函数计算。我们目前尚不清楚哪种方式与本文对 p-基数的研究更为契合。

回顾一下，若一个集合与它的任何真子集都不存在双射，则称它为戴德金有限。在经典集合论中，“有限”和“戴德金有限”等价，但在其他情形下未必如此。Dekker [10] 和 Dekker–Myhill [11] 的工作开创了将孤立数作为戴德金有限集合模型的研究。

定义 6.2（戴德金 p-有限）。如果一个语言 $L \subseteq \Sigma^*$ 与它的任何真子集的 p-基数都不相同，则称它为戴德金 p-有限。

定理 4.28 中构造的集合是一个无限的戴德金 p-有限集合。戴德金 p-有限集合与 Nerode & Remmel [52, 定义 6]中的 p-有限集合有何关系？戴德金 p-有限集合能让我们对 p-基数有怎样更一般的认识？它们是否拥有一套完善的算术理论？能否用它们实现 Downey 的建议 [12]（见第 1 节中的引文）？

最后，也可以考虑有限选择公理，即从由有限集组成的集合族开始——相应地，这里可以考虑语言 L，其中 L 中的单个元素通过将 x 的二进制编码视为 $\mathbb{N}$的有限子集的示性函数，来表示一个二进制集合。有限选择公理见 [38, 第 2 节2] 和 [67]。

致谢

我们感谢 Lance Fortnow 在我们最初讨论这些问题时（当时我还在读研究生）与我们进行初步讨论并提供了一些初步结果，也感谢他建议我以纪念专文的形式投稿。我们感谢两位匿名审稿人提出的建议，这些建议既改善了论文的阐述和组织，也为论文增添了结果。特别是，推论 4.46 最初被提出为一个开放问题；但由于审稿人建议改进定理 4.43 的证明阐述，因此只需对该定理的原始证明做一行修改即可（原投稿中的定理并未保证 C 是无限的）。定理 4.28 回答了原投稿中提出的一个开放问题，所用方法是对一位审稿人建议的构造进行修改。

本工作的准备工作部分得到了美国国家科学基金会 CAREER 奖项 CCF-2047756 的资助，也可能得到了我读研究生时 Lance 获得的某项资助；不过那是很久以前的事了，我们都不记得了，美国国家科学基金会大概也不再在意了。

当然，我们也要感谢 Alan，他与我们分享了自己无比旺盛的好奇心和深刻见解。

A 关于选择公理其他版本的评论

在本附录中，我们汇总了一些遇到过的选择公理变体。这些变体的多项式时间版本似乎切实可行，也值得研究，但我们尚未对此展开探索。

A.1 代数版本

经典选择公理 11. 每个向量空间都有一个基。

[53] 给出预言机 A_1, A_2，相对于它们，$\mathrm{P}^{A_i} \neq \mathrm{NP}^{A_i}$；相对于 A_1，每个非确定性多项式时间子空间都有一个多项式时间基；而相对于 A_2，则存在没有多项式时间基的非确定性多项式时间子空间。不过，与他们其他研究工作一样，这里的向量都是用一元字母表编码的。

经典选择公理 12. 对于每个非空集合 S，都存在一个定义在 S 上的二元运算，使 S 成为一个群。

这一命题的多项式时间版本似乎与群式见证 [16,第 4.1 节2] 以及群可定义性 [2]的概念有关。

经典选择公理 13（蒂霍诺夫定理，参见 [54, P5，第 69] 页）。紧空间的乘积是紧的。

A.2 模型论版本

经典结果 4。每个博弈 G_S，如果 S 是贝尔空间的博雷尔子集，则都是确定的。

经典选择公理 14（参见 [54, P6，第 69]页）。一个公式若在基数为 n 的集合上有模型，那么当 $\aleph_0 \leq m \leq n$时，它在基数为 m 的集合上也有模型。

经典选择公理 15（参见 [54, P7，第 69] 页）。一个公式若在基数为 $\aleph_0$ 的集合上有模型，那么它在任何大于 $\aleph_0$的基数上都有模型。

经典选择公理 16（参见 [54, P8，第 69] 页）。如果 Q 是一个公式集合，其中个体常元的集合的基数为 m，且 Q 的每个有限子集都有一个模型，那么 Q在某个基数不大于 $m + \aleph_0$的集合中有一个模型。

A.3 序理论版本

经典选择公理 17（豪斯多夫极大原理，参见 [38, 定理 2.2]）。在任意偏序集中，每个全序子集都包含于某个极大全序子集中。等价地：任意偏序集（至少）都有一个极大全序子集。

经典选择公理 18（库雷帕极大反链条件，参见 [38, 定理 2.4(3)]）。每个偏序集都有一个极大反链。

回想一下，集合的一个集族 $\mathcal{S}$ 具有有限特征，是指对于每个集合 $A \in \mathcal{S}$，其每个有限子集$F \subseteq A$ 也属于 $\mathcal{S}$；反过来，也就是说，如果存在一个集合 A，使得其每个有限子集$F \subseteq A$ 都属于 $\mathcal{S}$，那么 A 也属于 $\mathcal{S}$。

经典选择公理 19（图基引理，参见 [38, 定理 2.2], [54, M7，第 13] 页）。每个非空的有限特征集合族都存在一个关于包含关系的极大元。

多项式时间选择公理（PAC）9. 每个由具有有限特征的诚实非空语言组成的 P 集合族，都有一个关于包含关系的极大元。

最后，我们提及几条基于基数幂运算的公理。基数幂运算通常定义为 $|A|^{|B|} := |\{f\colon\ A \to B\}|$。

经典 AC 20（参见 [54, CN23、CN24、CN25，第 53–54] 页）。1. 对每个固定的无限基数m，对于所有无限基数 p, q，若 $p^m < q^m$，则 $p < q$。

2. 存在一个基数 $n > 1$，使得对于所有基数 p, q，都存在一个基数 $1 < m \leq n$，使得 $p^m < q^m$ 蕴含 $p < q$。

3. 对于所有 m, p, q，若 $m^p < m^q$ 且 $m \neq 0$，则 $p < q$。

一方面，当 B 是有限的时，我们应有 $A^B = A \times A \times \cdots \times A$，其中后一个乘积有 $|B|$ 个 A。另一方面，当 B 是无限的时，将 p 次幂 A^B 定义为能够计算部分多项式时间函数 $B \to A$的图灵机（/程序/索引）集合，似乎是自然而然的做法。这会带来两个问题：首先，当 B 是有限的时，这两种定义并不一致。其次，采用后一种定义时，只要 A, B 非空，A^B 便由赖斯定理可知不可计算。尽管如此，我们仍作如下暂定定义：

定义 A.1（p-基数的幂运算）。令 $A \subseteq \Sigma^*$、$B \subseteq \Gamma^*$。我们将 $||A||_p^{||B||_p}$ 定义为满足以下条件的图灵机集合的 p-基数：M 使得 M 计算一个多项式时间部分函数 $B \to A$。

让我们展开诸如 $||A||_p^{||C||_p} \preceq ||B||_p^{||C||_p}$这样的表达式的含义。这意味着存在一个部分多项式时间可计算的、p-可逆函数 f（在 img(f) 上可逆），对于任何计算多项式时间函数 $C \to A$的图灵机 M，该函数输出一台图灵机$f(M)$，计算一个部分多项式时间函数 $C \to B$。这让我们有理由希望，尽管 $||A||_p^{||B||_p}$不可计算，仍可能证明关于它的有意义的陈述。

P多项式时间选择公理（PAC）10。1. 对每个固定的 $C \in \mathsf{P}$，对于所有语言 A、$B \in \mathsf{P}$，若 $||A||_p^{||C||_p} \prec ||B||_p^{||C||_p}$，则 $||A||_p \prec ||B||_p$。2. 存在一个集合 $N \in \mathsf{P}$，满足 $||N||_p \succ 1$，使得对于所有集合 A、$B \in \mathsf{P}$，存在一个集合$1 \prec ||C||_p \preceq ||N||_p$ 属于 P，使得 $||A||_p^{||C||_p} \prec ||B||_p^{||C||_p}$ 蕴含 $||A||_p \prec ||B||_p$。3. 对所有非空 $C \in \mathsf{P}$ 以及所有语言 A、$B \in \mathsf{P}$，若 $||C||_p^{||A||_p} \prec ||C||_p^{||B||_p}$，则 $||A||_p \prec |B||_p$。

A.4 难以提出有趣的多项式时间类比的选择公理形式

这里我们列举一些选择公理的变体。对于这些变体，我们难以提出合理的多项式时间类比，并介绍遇到的困难。

前几个变体都提到了幂集，这给我们带来了麻烦：

经典 AC 21. 对任意集合 A，其幂集（去掉空集后）都有一个选择函数。等价地：对任意集合 A，存在一个函数 f，使得对任意非空子集 $B \subseteq A$，$f(B) \in B$。

经典 AC 2（参见 [38, 定理 2.4(5)]）。每个可良序集的幂集都可以良序化。

一方面，我们希望讨论语言$L \in$P 的“多项式时间幂集”。一种尝试是考虑所有满足 $L' \in$ P 的 $L' \subseteq L$ 的集合；一种自然的方式是用某个多项式时间机器 M_x 写作 $L' = L \cap L(M_x)$，来指称这些子集 L'，然后可以将这些索引 x 用作选择函数或良序函数的输入。但这样一来，我们就遇到了一个问题：给定 x 作为输入，这样的多项式时间函数甚至无法模拟所有 M_x。

其他人提到了单个元素的存在，这似乎不适用于渐近考量，例如，或许最著名的一个例子是：

经典选择公理 23（佐恩引理，参见例如 [38, 定理 2.2]）。每个非空偏序集，只要其中每条链（全序子集）都有上界，就至少包含一个极大元。

参考文献

[1] Eric A. Allender. 可逆函数。博士论文，佐治亚理工学院，1985年。网址：https://people.cs.rutgers.edu/~allender/publications/complete_list.html。[2] V. Arvind 和 N. V. Vinodchandran。群可定义语言的计数复杂性。《理论计算机科学》，242(1-2):199–218，2000年。doi:10.1016/S0304-3975(98)00218-7。[3] C. J. Ash 和 J. Knight。《可计算结构与超算术层级》，《逻辑与数学基础研究》第144卷。北荷兰出版公司，阿姆斯特丹，2000年。[4] Theodore P. Baker 和 Alan L. Selman。迈向多项式层次的第二步。《理论计算机科学》，8(2):177–187，1979年。doi:10.1016/0304-3975(79)90043-4。[5] L. Berman 和 J. Hartmanis。关于 NP 和其他完全集的同构与密度。SIAM 计算杂志，6(2):305–322，1977年。doi:10.1137/0206023。[6] Andreas Blass 和 Yuri Gurevich。等价关系、不变量与标准形，II。载于《逻辑与机器：判定问题与复杂性》，计算机科学讲义第171卷，第24–42页。施普林格，1984年。doi:10.1007/3-540-13331-3_31。[7]Samuel R. Buss 和 Louise Hay。关于对 SAT 的真值表可约性。《信息与计算》，91(1):86–102，1991年。初步版本发表于 1988 年复杂性结构会议。doi:10.1016/0890-5401(91)90075-D。[8] Merlin Carl。广义有效可约性。载于 Arnold Beckmann、Laurent Bienvenu 和 Nataˇsa Jonoska（编），《追寻普适性》，第225–233页，查姆，2016年。施普林格国际出版公司。arXiv 版本：arXiv:1601.01899 [math.LO]。[9] Barbara Csima、Sergey Goncharov、Noam Greenberg、Julia Knight、Antonio Mon- talb´an 和 Ted Slaman。可计算模型论，BIRS 研讨会报告。https://www.birs.ca/workshops/2013/13w5047/report13w5047.pdf，2014年。[10] J. C. E. Dekker。集合类的递归等价类型。《美国数学会通报》，70:628–632，1964年。doi:10.1090/S0002-9904-1964-11215-5。[11] J. C. E. Dekker 和 J. Myhill。递归等价类型。《加州大学数学出版物》，3:67–213，1960年。

[12]Rodney G. Downey。A. Nerode 和 J. B. Remmel 的《多项式隔离集》书评。MathSciNet 对 MR1071525 的评论，1990年。网址：https://mathscinet.ams.org/mathscinet-getitem?mr=1071525。

[13] Damir D. Dzhafarov 和 Carl Mummert。逆向数学与选择公理的等价命题。arXiv:1009.3242 [math.LO], 2010。

[14] Stephen A. Fenner、Lance Fortnow、Ashish V. Naik 和 John D. Rogers。满射函数的求逆。《信息与计算》，186(1)：90–103，2003年。doi:10.1016/S0890-5401(03)00119-6。

[15]Stephen A. Fenner、Stuart A. Kurtz 和 James S. Royer。每个多项式时间 1-度坍缩，当且仅当 P = PSPACE。《符号逻辑杂志》，69(3)：713–741，2004年。doi:10.2178/jsl/1096901763。

[16] Lance Fortnow 和 Joshua A. Grochow。重新审视等价问题的复杂性类。《信息与计算》，209(4):748–763，2011。预印本 arXiv:0907.4775 [cs.CC]。doi:10.1016/j.ic.2011.01.006。

[17]Christian Glaßer、Andrew Hughes、Alan L. Selman 和 Nils Wisiol。不相交的 NP 对与命题证明系统。《SIGACT 新闻》，45(4):59–75，2014。doi:10.1145/2696081.2696095。

[18] Christian Glaßer、Dung T. Nguyen、Alan L. Selman 和 Maximilian Witek。《自归约性与有丝分裂性的介绍》。载于 Adam R. Day、Michael R. Fellows、Noam Greenberg、Bakhadyr Khoussainov、Alexander G. Melnikov 和 Frances A. Rosamond（编），《可计算性与复杂性——献给 Rodney G. Downey 60 岁生日的论文集》，《计算机科学讲义》第 10010 卷，第 56–78 页。施普林格，2017。doi:10.1007/978-3-319-50062-1_5.[19]Christian Glaßer、Mitsunori Ogihara、Aduri Pavan、Alan L. Selman 和 Liyu Zhang。《自归约性、有丝分裂性与免疫性》。《计算机与系统科学杂志》，73(5):735–754，2007。初步版本发表于 MFCS ’05。doi:10.1016/j.jcss.2006.10.020.[20] Christian Glaßer、Aduri Pavan、Alan L. Selman 和 Liyu Zhang。《计算复杂性中的有丝分裂》。载于 Jin-yi Cai、S. Barry Cooper 和 Angsheng Li（编），《计算模型理论与应用》，第三届国际会议 TAMC 2006，2006年5月15–20日，中国北京，会议论文集，《计算机科学讲义》第 3959 卷，第 61–67 页。施普林格，2006。doi:10.1007/11750321_4.[21] Christian Glaßer、Aduri Pavan、Alan L. Selman 和 Liyu Zhang。《NP 完全集的分裂》。《SIAM 计算杂志》，37(5):1517–1535，2008。doi:10.1137/060673886.[22]Christian Glaßer、Alan L. Selman 和 Samik Sengupta。《不相交 NP 对之间的归约》。载于第 19 届年度 IEEE计算复杂性会议（CCC 2004），2004年6月21–24日，美国马萨诸塞州阿默斯特，第 42–53 页。IEEE 计算机学会，2004。doi:10.1109/CCC.2004.1313791.[23]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。初步版本发表于 CCC ’03。doi:10.1137/S0097539703425848.[24]Christian Glaßer、Alan L. Selman、Stephen D. Travers 和 Klaus W. Wagner。《不相交集合之并的复杂性》。《计算机与系统科学杂志》，74(7):1173–1187，2008。doi:10.1016/j.jcss.2008.05.001。

[25] Andrew V. Goldberg 和 Michael Sipser。《压缩与排序》。《SIAM 计算杂志》，20(3):524–536，1991年。doi:10.1137/0220034.[26] Judy Goldsmith 和 Steven Homer。《可扩展性与同构问题》。《信息处理快报》，57(3):137–143，1996年。doi:10.1016/0020-0190(95)00204-9.[27] Judy Goldsmith、Kenneth Kunen 和 Lane A. Hemachandra。《多项式时间压缩》。《计算复杂性》，2:18–39，1992年。doi:10.1007/BF01276437.[28]Joshua A. Grochow。《等价关系的复杂性》。硕士论文，芝加哥大学，2008年12月。网址：https://home.cs.colorado.edu/~jgrochow/Grochow_UofC_Masters_08_Equivalence_Relations.pdf.

[29]Joshua A. Grochow 和 Youming Qiao。《关于 p 群同构：通过张量实现搜索到判定、计数到判定及幂零类归约》。载于 Valentine Kabanets（编），第36届计算复杂性会议（CCC 2021），Leibniz 信息学国际会议论文集（LIPIcs）第200卷，第16:1–16:38页，德国达格施图尔，2021年。Schloss Dagstuhl – Leibniz-Zentrum f¨ur Informatik。doi:10.4230/LIPIcs.CCC.2021.16.[30] Joachim Grollmann 和 Alan L. Selman。《公钥密码系统的复杂性度量》。SIAM 计算杂志，17(2):309–335，1988年。密码学专刊。doi:10.1137/0217018.[31] Lane A. Hemachandra。《结构复杂性理论中的计数》。博士论文，康奈尔大学，1987年。注：L. A. Hemachandra 是 L. A. Hemaspaandra 婚前使用的姓名。[32] Lane A. Hemachandra、Albrecht Hoene、Dirk Siefkes 和 Paul Young。《关于通过迭代多项式可枚举的集合》。理论计算机科学，80(2):203–225，1991年。计算机科学数学基础研讨会 ’89。doi:10.1016/0304-3975(91)90388-I。[33] Edith Hemaspaandra、Ashish V. Naik、Mitsunori Ogihara 和 Alan L. Selman。《P-选择集与将搜索归约为判定和自归约性》。计算机与系统科学杂志，53(2，第1部分):194–209，1996年。第八届年度复杂性理论结构会议（加利福尼亚州圣迭戈，1993年）。doi:10.1006/jcss.1996.0061。[34]Lane Hemaspaandra 和 Leen Torenvliet。《半可行算法理论》。理论计算机科学专著，EATCS丛书。施普林格，2003年。doi:10.1007/978-3-662-05080-4。[35] Lane A. Hemaspaandra、Ashish V. Naik、Mitsunori Ogihara 和 Alan L. Selman。《计算解可唯一地折叠多项式层次》。载于《算法与计算》（北京，1994年），数学讲义第834卷，第56–64页。施普林格，柏林，1994年。可作为 ECCC技术报告 TR96-027 获取。 [36]的预印本。[36] Lane A. Hemaspaandra、Ashish V. Naik、Mitsunori Ogihara 和 Alan L. Selman。《计算解可唯一地折叠多项式层次》。SIAM 计算杂志，25(4):697–708，1996年。最初发表于 [35]。doi:10.1137/S0097539794268315。[37] Lane A. Hemaspaandra 和 Alan L. Selman（编）。《复杂性理论回顾》。第II卷。施普林格出版社，纽约，1997年。doi:10.1007/978-1-4612-1872-2。[38] Horst Herrlich。《选择公理》，数学讲义第1876卷。施普林格出版社，柏林，2006年。doi:10.1007/11601562。

[39]Deborah Joseph 和 Paul Young。《关于 NP 中非多项式且非完全集的见证函数的一些评论》。理论计算机科学，39(2-3):225–237，1985年。doi:10.1016/0304-3975(85)90140-9。[40] Ker-I Ko。《关于一些自然完备算子》。理论计算机科学，37(1):1–30，1985年。doi:10.1016/0304-3975(85)90085-4。[41] Ker-I Ko 和 Daniel Moore。《完备性、近似与密度》。SIAM 计算杂志，10(4):787–796，1981年。doi:10.1137/0210061。[42] Stuart A. Kurtz、Stephen R. Mahaney 和 James S. Royer。《度的折叠》。计算机与系统科学杂志，37:247–268，1988年。doi:10.1016/0022-0000(88)90007-4。[43]Stuart A. Kurtz、Stephen R. Mahaney 和 James S. Royer。《相对于随机预言机，同构猜想不成立》。计算机协会杂志，42(2):401–420，1995年。doi:10.1145/201019.201030。[44] Jack H. Lutz。《复杂性类中的范畴与测度》。SIAM 计算杂志，19(6):1100–1131，1990年。doi:10.1137/0219076。[45] Charles McCarty。《可实现性与递归数学》。博士论文，牛津大学，1980年（1985年）。URL: http://hdl.handle.net/1842/35199。[46] Charles McCarty。《可实现性与递归集合论》。纯粹与应用逻辑年刊，32(2):153–183，1986年。doi:10.1016/0168-0072(86)90050-3。[47] Albert R. Meyer 和 Michael S. Paterson。《表面上难以处理的问题究竟有多大概率是困难的？》麻省理工学院技术报告 MIT/LCS/TM-126，1979年。URL: http://publications.csail.mit.edu/lcs/pubs/pdf/MIT-LCS-TM-126.pdf。[48] Antonio Montalb´án。《可计算结构理论》。逻辑展望。剑桥大学出版社，剑桥；符号逻辑协会，纽约州伊萨卡，2021年。算术中的内容。doi:10.1017/9781108525749。[49] Ashish V. Naik 和 Alan L. Selman。《关于 P-选择集以及对 NP 的自适应与非自适应查询的一则说明》。载于 Steven Homer 和 Jin-Yi Cai（编），第十一届 IEEE 计算复杂性年会论文集，美国宾夕法尼亚州费城，1996年5月24–27日，第224–232页。IEEE 计算机学会，1996年。doi:10.1109/CCC.1996.507684。[50] A. Nerode 和 J. B. Remmel。《复杂性理论代数。II. 布尔代数》。纯粹与应用逻辑年刊，44(1-2):71–99，1989年。第三届亚洲数理逻辑会议（北京，1987年）。doi:10.1016/0168-0072(89)90047-X。[51] A. Nerode 和 J. B. Remmel。《多项式时间等价类型》。载于《逻辑与计算》（宾夕法尼亚州匹兹堡，1987年），当代数学第106卷，第221–249页。美国数学会，罗得岛州普罗维登斯，1990年。doi:10.1090/conm/106/1057825。[52] A. Nerode 和 J. B. Remmel。《多项式隔离集》。载于《递归论周》（奥伯沃尔法赫，1989年），数学讲义第1432卷，第323–362页。施普林格，柏林，1990年。doi:10.1007/BFb0086125。[53] Anil Nerode 和 J. B. Remmel。《复杂性理论代数。I. 有限域上的向量空间》。都灵理工大学数学研讨会论文集，第1–10页（1988年），1987年。逻辑与计算机科学：新趋势与应用会议（都灵，1986年）。

[54] Herman Rubin 和 Jean E. Rubin。《选择公理的等价命题》。北荷兰出版公司，阿姆斯特丹，1963年。[55] Herman Rubin 和 Jean E. Rubin。《选择公理的等价命题》II，逻辑与数学基础研究第116卷。北荷兰出版公司，阿姆斯特丹，1985年。[56] Eric Schechter。《分析及其基础手册》。学术出版社，圣迭戈，1997年。[57] Alan L. Selman。多项式时间枚举可约性。《SIAM 计算杂志》，7(4):440–457，1978年。doi:10.1137/0207035。[58] Alan L. Selman。P-选择集、计数语言以及多项式时间归约在 NP 上的行为。《数学系统理论》，13:55–65，1979年。doi:10.1007/BF01744288。[59] Alan L. Selman。关于 NP、实数和 p-选择集的一些观察。《计算机与系统科学杂志》，23(3):326–332，1981年。doi:10.1016/0022-0000(81)90068-4。[60] Alan L. Selman。NP 和 p-选择集上的归约。《理论计算机科学》，19(3):287–304，1982年。doi:10.1016/0304-3975(82)90039-1。[61]Alan L. Selman。自然自可约集。《SIAM 计算杂志》，17(5):989–996，1988年。doi:10.1137/0217062。[62]Alan L. Selman，编。《复杂性理论回顾》。施普林格出版社，纽约，1990年。谨以此书纪念 Juris Hartmanis 六十寿辰。doi:10.1007/978-1-4612-4478-3。[63] Alan L. Selman。部分函数的复杂性类。载于 Grzegorz Rozenberg 和 Arto Salomaa 编，《理论计算机科学当前趋势——论文与教程》，世界科学计算机科学丛书第40卷，第504–522页。世界科学出版社，1993年。doi:10.1142/9789812794499_0038。[64] Alan L. Selman。函数复杂性类的分类。《计算机与系统科学杂志》，48(2):357–381，1994年。doi:10.1016/S0022-0000(05)80009-1。[65] Alan L. Selman。函数问题上的大惊小怪。载于 Steven Homer 和 Jin-Yi Cai 编，《第十一届 IEEE 计算复杂性年会论文集》，美国宾夕法尼亚州费城，1996年5月24—27日，第198–212页。IEEE 计算机学会，1996年。doi:10.1109/CCC.1996.507682。[66] Alfred Tarski。关于若干等价于选择公理的定理。《数学基础》，5:147–154，1924年。URL：http://matwbn.icm.edu.pl/ksiazki/fm/fm5/fm5118.pdf。[67]John Truss。有限选择公理。《数学逻辑年刊》，6:147–176，1973/74年。doi:10.1016/0003-4843(73)90007-7。[68] Klaus W. Wagner。对数查询类。技术报告TR-145，奥格斯堡大学数学研究所，1987年。