arXiv:2301.12028v2 [cs.CC] 6 Feb 2023

多项式时间随机函数的算术理论

M. Antonelli、U. Dal Lago、D. Davoli、I. Oitavem、P. Pistone

2023年2月8日

我们引入一种新的有界理论 RS^1_2, , 并证明其中可由 Σ^b_1表示的函数，恰好是能够在多项式时间内计算的随机函数。具体而言，我们首先研究字符串上的预言机函数类 $\mathcal{POR}$；该类将在第2节中与 RS^1_2一同引入。随后，我们证明，由多项式时间概率图灵机计算的函数可以通过一类概率有界公式进行算术刻画：在第3.2节中，我们证明多项式时间预言机函数类等价于在 RS^1_2, 中可由 Σ^b_1表示的函数类；在第4节中，我们证明逆向结论。

1 概述

有界算术中对多项式时间（确定性）函数的通常刻画，是通过两个“宏观”结果 [1, 7] 得到的。人们引入了某种用于多项式时间函数的 Cobham式代数，并证明它等价于：（1）由在多项式时间内运行的图灵机计算的函数类；（2）在适当有界理论中可由 Σ^b_1 表示的函数类。我们的证明总体上遵循类似路径，其中，一个称为 $\mathcal{POR}$ 的预言机递归函数代数扮演 Cobham 风格函数代数的角色。在我们的情形中，函数由概率图灵机在多项式时间内计算，而理论则是随机化的 RS^1_2。在引入这些类之后，我们证明，在 RS^1_2 中可由 Σ^b_1 表示的随机函数恰好是 $\mathcal{POR}$ 中的函数，并且 $\mathcal{POR}$ 等价于由在多项式时间内运行的概率图灵机计算的函数类（在一种非常具体的意义下）。尽管第一部分可以借助标准论证 [7, 3]，得以确立，但随机性的存在为第二部分引入了一个需要处理的微妙因素。事实上， $\mathcal{POR}$ 中的函数以一种与概率图灵机相当不同的方式访问随机性，而关联这两种模型需要付出一定努力，其中涉及一长串中间模拟。

具体而言，我们首先定义字符串上的预言机函数类，以及深受 [8]，启发、但采用“概率词语言”的新理论 RS^1_2, , 并考虑一种略作修改的 Σ^b_i 可表示性概念，以适应我们特殊预言机函数的定义域。随后，我们分三步证明，多项式时间可计算的随机函数类 RFP，恰好是能在 RS^1_2 中 Σ^b_1 可表示的函数类：

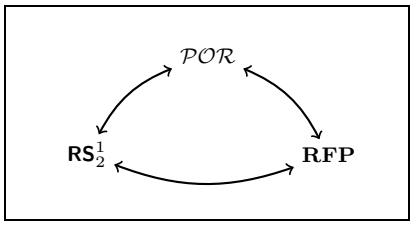


图 1：证明模式

1. 我们通过对预言机函数的结构进行归纳（并依赖 [1, 7] 中介绍的编码机制），证明 $\mathcal{POR}$ 中的函数在 RS_2^1 中是 Σ_1^b 可表示的。2. 我们通过类似于 Cook 和 Urquhart 方法 [3] 的可实现性技术，证明所有在 RS_2^1 中 Σ_1^b 可表示的函数都属于 $\mathcal{POR}$。3. 我们将 Cobham 的结果推广到概率模型，证明 $\mathcal{POR}$ 中的函数恰好就是 RFP 中的函数。

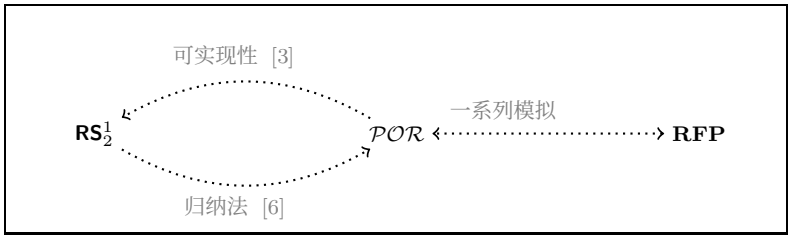


图 2：我们的证明概要

2 引入 $\mathcal{POR}$ 和 RS_2^1

本节将介绍一个用于多项式时间预言机递归函数 $\mathcal{POR}$ 的 Cobham 风格函数代数，以及一种随机有界算术 RS_2^1。与 Ferreira 的体系 [6, 7]，一样，这两个体系都以二进制串而非正自然数为基础： $\mathcal{POR}$ 是定义在比特序列上的预言机函数类，而 RS_2^1 则定义在概率词语言 $\mathcal{RL}$中。字符串具有自然的项大小概念，因此更便于处理界限和时间复杂度。值得注意的是，采用字符串并非关键，下面的所有结果都可以用自然数来表述。事实上，两种表述下都已引入相应的理论——Ferreira 的 Σ_1^b-NIA 和 Buss 的 S_2^1 ——并证明二者等价 [8]。

2.1 函数代数 $\mathcal{POR}$

我们将介绍一个受 Ferreira 的 $\mathcal{PTCA}$ [6, 7] 启发、定义在字符串之上的多项式时间预言机递归函数代数。

记号 2.1。令 $\mathbb{B} = \{\mathbb{0}, \mathbb{1}\}$，$\mathbb{S} = \mathbb{B}^*$ 为有限长度二进制串的集合，$\mathbb{O} = \mathbb{B}^{\mathbb{S}}$ 为无限长度二进制串的集合。元变量η'、η''、.....用于表示 $\mathbb{O}$ 的元素。

令 $|\cdot|$ 表示字符串的长度映射，因此对于任意字符串 x，$|x|$ 表示 x 的长度。给定两个二进制串 x、y，我们用 $x \subseteq y$ 表示 x 是 y 的初始子串或前缀子串，用 $x \frown y$（缩写为 xy）表示连接，并用 $x \times y$ 表示将 x 自连接 $|y|$ 次所得的结果。给定一个无限比特串 η 和一个有限字符串 x，$\eta(x)$ 表示 η 中的一个特定位，即所谓的 x 的第 x 位。

预言机函数与函数代数中的函数之间的一个根本区别在于，后者的形式为 $f : \mathbb{S}^k \times \mathbb{O} \to \mathbb{S}$，并带有一个额外参数，该参数被解释为底层的随机比特源。此外，$\mathcal{PR}$ 包含基本函数查询 $Q(x, \eta) = \eta(x)$，可用于观察 η 中的任意比特。

定义 2.1（类 $\mathcal{POR}$）。类 $\mathcal{POR}$ 是函数 $f : \mathbb{S}^k \times \mathbb{O} \to \mathbb{S}$ 的最小类，包含：

- 空（字符串）函数 $E(x, \eta) = \epsilon$
- 投影（字符串）函数 $P_i^n(x_1, \ldots, x_n, \eta) = x_i$，其中 $n \in \mathbb{N}$ 且 $1 \leq i \leq n$
- 词后继 $S_b(x, \eta) = x\mathbb{b}$，其中 $b = 0$ 当 $\mathbb{b} = \mathbb{1}$ 且 $b = 1$ 当 $\mathbb{b} = \mathbb{1}$
- 条件（字符串）函数

$$C(\epsilon, y, z_0, z_1, \eta) = y$$
$$C(x\mathbb{b}, y, z_0, z_1, \eta) = z_b,$$

  其中 $b = 0$ 当 $\mathbb{b} = \mathbb{0}$ 且 $b = 1$ 当 $\mathbb{b} = \mathbb{1}$
- 查询（字符串）函数 $Q(x, \eta) = \eta(x)$

并在以下模式下封闭：

- 复合，其中 f 由 $g, h_1, \ldots, h_k$ 定义为

$$f(\vec{x}, \eta) = g(h_1(\vec{x}, \eta), \ldots, h_k(\vec{x}, \eta), \eta)$$

- 记号上的有界递归，其中 f 由 g、h_0 和 h_1 定义为

$$f(\vec{x}, \epsilon, \eta) = g(\vec{x}, \eta)$$
$$f(\vec{x}, y\mathbb{0}, \eta) = h_0(\vec{x}, y, f(\vec{x}, y, \eta), \eta)|_{t(\vec{x},y)}$$
$$f(\vec{x}, y\mathbb{1}, \eta) = h_1(\vec{x}, y, f(\vec{x}, y, \eta), \eta)|_{t(\vec{x},y)}$$

并且 t 通过显式定义由 ϵ、1、0、$\frown$ 和 $\times$ 得到，也就是说，t 可以通过对常量 ϵ、0、1 以及变量$\vec{x}$和 y应用 $\frown$ 和 $\times$ 得到。[1]

实际上，条件函数 C 可以通过有界递归来定义。

注 2.1。Ferreira 的刻画中既没有查询函数，也没有条件函数 *[7],*，而是包含“子串条件”函数：

$$S(x,y,\eta) = \begin{cases} \mathbb{1} & if\ x \subseteq y \\ \mathbb{0} & otherwise, \end{cases}$$

它可以通过有界递归在 $\mathcal{POR}$ 中定义。

2.2 随机化有界算术

首先，我们为有界算术引入一种概率词语言及其定量解释。

语言 $\mathcal{RL}$。遵循 [8], ，我们考虑一个以二进制表示法表示自然数的一阶签名，并为其添加一个特殊谓词符号 Flip(·)。因此，公式是在 S 上而非 N 上解释的。

定义 2.2（ $\mathcal{RL}$ 的项和公式）。 $\mathcal{RL}$ 的项和公式由以下语法定义：

$$t := x \mid \epsilon \mid \mathtt{0} \mid \mathtt{1} \mid t \frown t \mid t \times t$$
$$F := \mathtt{Flip}(t) \mid t = s \mid \neg F \mid F \wedge F \mid F \vee F \mid (\exists x)F \mid (\forall x)F.$$

记号 2.2（截断）。为便于阅读，我们采用以下缩写： ts 表示 $t \frown s$， $\mathtt{1}^t$ 表示 $\mathtt{1} \times t$， $t \preceq s$ 表示 $\mathtt{1}^t \subseteq \mathtt{1}^s$，表示 t 的长度小于 s 的长度。给定三个项 t、r 和 s，缩写 $t|_r = s$ 表示以下公式，

$$(\mathtt{1}^r \subseteq \mathtt{1}^t \wedge s \subseteq t \wedge \mathtt{1}^r = \mathtt{1}^s) \vee (\mathtt{1}^t \subseteq \mathtt{1}^r \wedge s = t),$$

这表示 s 是将 t 截断到 r 的长度所得的结果。

每个字符串 $\sigma \in$ S 都可以视为 $\mathcal{RL}$ $\overline{\sigma}$ 的一个项，使得 $\overline{\epsilon} = \epsilon$、 $\sigma\mathtt{b} = \overline{\sigma}\mathtt{b}$，其中 $\mathtt{b} \in$ B 且 $\mathtt{b} \in \{\mathtt{0}, \mathtt{1}\}$，例如 $\overline{\mathbb{0}\mathbb{0}\mathbb{1}} = \mathtt{001}$。

有界算术的一个核心特征是存在有界量词。

记号 2.3（有界量词）。在 $\mathcal{RL}$ 中，有界量化表达式是以下形式之一：$(\forall x)(\mathtt{1}^x \subseteq \mathtt{1}^t \to F)$ 或 $(\exists x)(\mathtt{1}^x \subseteq \mathtt{1}^t \wedge F)$，通常分别简写为 $(\forall x \preceq t)F$ 和 $(\exists x \preceq t)F$。

[1]请注意，这与 $\mathcal{RL}$ 中定义 2.5 的项语法有着明显的对应关系。

记号 2.4。我们将形式为 $(\forall x \subseteq^* t)F$ 和 $(\exists x \subseteq^* t)F$ 的量词称为子词量词，分别简写为 $(\forall x)\big((\exists w \subseteq t)(wx \subseteq t) \rightarrow F\big)$ 和 $(\exists x)(\exists w \subseteq t)(wx \subseteq t \wedge F)$。此外，我们将所谓的初始子词量词 $(\forall x)(x \subseteq t \rightarrow F)$ 简写为 $(\forall x \subseteq t)F$，并将 $(\exists x)(x \subseteq t \wedge F)$ 简写为 $(\exists x \subseteq t)F$。

出于复杂度方面的考虑，有界量化与子词量化之间的区别十分重要。若 $\sigma \in$S 是长度为 k 的字符串，则子词存在量化公式（$\exists x \subseteq^* \overline{\sigma}$）$F$的见证需要在所有可能的 σ子串中寻找，也就是说，搜索空间大小为 $\mathcal{O}$（k）。相反，有界公式（$\exists x \preceq \overline{\sigma}$）$F$ 的见证需要在所有长度为 k 的可能字符串中寻找，即搜索空间大小为 $\mathcal{O}$（2^k）。

备注 2.2. 为避免误解，我们简要总结一下子词关系中使用的不同概念和符号。我们用 $\subseteq$ 表示字符串之间的关系，也就是说，$x \subseteq y$ 表示 x 是 y 的初始子串或前缀子串。我们在语言 $\mathcal{RL}$ 中使用 $\subseteq$ 作为关系符号。我们在语言 $\mathcal{RL}$ 中使用$\preceq$ 作为辅助符号；特别是，如前所见，$t \preceq s$ 是 $1^t \subseteq 1^s$的语法糖。我们在语言$\mathcal{RL}$ 中使用 $\subseteq^*$ 作为辅助符号来表示子词量化。我们还将（$\exists w \subseteq t$）F 作为（$\exists w$）（$w \subseteq t \wedge F$）的缩写，类似地，也将（$\forall w \subseteq t$）作为缩写。

定义 2.3（Σ_1^b-公式）。Σ_0^b-公式是一个带子词量词的公式，即属于满足以下条件的最小类 $\mathcal{RL}$：包含原子公式，并且在布尔运算和子词量词运算下封闭。若一个公式具有形式 $(\exists x_1 \preceq t) \ldots (\exists x_n \preceq t_n)F$，且 F 中的唯一量词是子词量词，则称该公式为 Σ_1^b-公式。我们将包含所有且仅包含 Σ_1^b-公式的类称为 Σ_1^b。

扩展的 Σ_1^b-公式是指 $\mathcal{RL}$ 中的任意公式，它可以通过有限步构造得到，构造从子词量词和有界存在量词开始，并从有界存在量词开始。

有界理论 RS_2^1。我们引入有界理论 $\mathrm{RS}_{2,}^1$，它可以看作 Ferreira 的 Σ_1^b-NIA [6] 的概率版本。它用语言 $\mathcal{RL}$ 表述。

定义 2.4（理论 RS_2^1）。理论 RS_2^1 由属于两个类的公理定义：

- 基本公理：

  1. $x\epsilon = x$2. $x(y$b$) = (xy)$
  b 3. $x \times \epsilon = \epsilon$4. $x \times x$b $=$
  $(x \times y)x$5. $x \subseteq \epsilon \leftrightarrow x = \epsilon$
  6. $x \subseteq y$b $\leftrightarrow x \subseteq y \vee x = y$
  b

7. $x\mathsf{b} = y\mathsf{b}$
$\to x = y$8. $x\mathsf{0} \neq y\mathsf{1}$,
9. $x\mathsf{b} \neq \epsilon$

其中 $\mathsf{b} \in \{\mathsf{0}, \mathsf{1}\}$

- 记法归纳公理模式,

$$B(\epsilon) \wedge (\forall x)\big(B(x) \to B(x\mathsf{0}) \wedge B(x\mathsf{1})\big) \to (\forall x)B(x),$$

其中 B 是 $\mathcal{RL}$ 中的一个 Σ^b_1-公式。

记法归纳将皮亚诺算术的常规归纳模式调整为适用于二进制表示。当然，与 Buss 和 Ferreira 的方法一样，将此模式限制为 Σ^b_1-公式，对于刻画使用有界资源计算的算法至关重要。事实上，该模式更一般的实例会将可表示性扩展到并非可由多项式时间（概率）计算的随机函数。

命题 2.1（[6]）。在 RS^1_2 中，任意扩展的 Σ^b_1-公式在逻辑上都等价于一个 Σ^b_1-公式。[2]

$\mathcal{RL}$ 中公式的语义。我们为 $\mathcal{RL}$ 中的公式引入一种定量语义，其深受 MQPA 语义的启发。具体而言， $\mathcal{RL}$ 的函数符号以及谓词符号“=”和“⊆”在典范模型 $\mathscr{W} = (\mathsf{S} \frown \times)$ 中均有作为 S 上关系的标准解释；而正如我们将看到的，Flip(t) 可以采用标准方式解释，也可以按照定义 ?? 进行解释。

定义 2.5（ $\mathcal{RL}$中的项的语义）。给定一组项变量 $\mathcal{G}$，环境 $\xi : \mathcal{G} \to \mathsf{S}$ 是一种映射，它为每个变量分配一个字符串。给定 $\mathcal{RL}$ 中的一个项 t 和一个环境 ξ， ξ 中 t 的解释是字符串 $[\![t]\!]_\xi \in \mathsf{S}$，按归纳式定义如下:

$$\begin{aligned} [\![\epsilon]\!]_\xi &:= \boldsymbol{\epsilon} & [\![x]\!]_\xi &:= \xi(x) \in \mathbb{S} \\ [\![\mathsf{0}]\!]_\xi &:= \mathbb{0} & [\![t \frown s]\!]_\xi &:= [\![t]\!]_\xi [\![s]\!]_\xi \\ [\![\mathsf{1}]\!]_\xi &:= \mathbb{1} & [\![t \times s]\!]_\xi &:= [\![t]\!]_\xi \times [\![s]\!]_\xi . \end{aligned}$$

如第 ?? 章所述，我们为规范模型 $\mathscr{W}$ 配备概率空间 $\mathscr{P}_\mathscr{W} = (\Omega, \sigma(\mathscr{C}), \mu_\mathscr{C})$，其中 $\sigma(\mathscr{C}) \subseteq \mathcal{P}(\Omega)$ 是由柱集 $\mathsf{C}^{\mathsf{b}}_\sigma = \{\eta \mid \eta(\sigma) = \mathsf{b}\}$（其中 $\mathsf{b} \in \mathsf{B}$）生成的 Borel σ-代数，并且满足 $\mu_\mathscr{C}(\mathsf{C}^{\mathsf{b}}_\sigma) = \frac{1}{2}$。为了形式化定义 $\mathsf{B}^\mathbb{S}$ 上的柱集，我们对 Billingsley 的秩为 n 的柱集概念作了略微修改。

[2]事实上，Ferreira 在论文第 148-149], 页中为理论 Σ^b_1-NIA [6, 证明了这一结果，但显然它对 $\mathcal{RL}$ 也成立。

定义 2.6（关于 S 的柱集）。对于任意可数集 S、有限 $K \subset S$ 和 $H \subseteq \mathsf{B}^K$,

$$\mathsf{C}(H) = \{\eta \in \mathbb{B}^S \mid \eta|_K \in H\},$$

是 S 上的柱集。

接着，$\mathscr{C}$和 $\sigma(\mathscr{C})$ 按标准方式定义，其上的概率测度定义如下：[3]

定义 2.7（柱测度）。对于任意可数集 S、 $K \subseteq S$ 和 $H \subseteq \mathsf{B}^K$，使得 $\mathsf{C}(H) = \{\eta \in \mathsf{B}^S \mid \eta|_K \in H\}$,

$$\mu_{\mathscr{C}}(\mathsf{C}(H)) = \frac{|H|}{2^{|K|}}.$$

这是 $\sigma(\mathscr{C})$ 上的一个测度。

$\mathcal{RL}$ 的公式被解释为可测集。

定义 2.8（ $\mathcal{RL}$ 中公式的语义）。给定一个项 t、一个公式F和一个环境 ξ：$\mathcal{G} \to \mathsf{S}$，其中 $\mathcal{G}$ 是项变量集， F 在 ξ 下的解释是序列集合 $[\![F]\!]_\xi \in \sigma(\mathscr{C})$, 该集合按以下方式归纳定义：

$$[\![\mathtt{Flip}(t)]\!]_\xi := \{\eta \mid \eta([\![t]\!]_\xi) = \mathbb{1}\}$$

$$[\![t = s]\!]_\xi := \begin{cases} \mathbb{O} & \text{if } [\![t]\!]_\xi = [\![s]\!]_\xi \\ \emptyset & \text{otherwise} \end{cases}$$

$$[\![t \subseteq s]\!]_\xi := \begin{cases} \mathbb{O} & \text{if } [\![t]\!]_\xi \subseteq [\![s]\!]_\xi \\ \emptyset & \text{otherwise} \end{cases}$$

$$[\![\neg G]\!]_\xi := \mathbb{O} - [\![G]\!]_\xi$$
$$[\![G \vee H]\!]_\xi := [\![G]\!]_\xi \cup [\![H]\!]_\xi$$
$$[\![G \wedge H]\!]_\xi := [\![G]\!]_\xi \cap [\![H]\!]_\xi$$
$$[\![G \to H]\!]_\xi := (\mathbb{O} - [\![G]\!]_\xi) \cup [\![H]\!]_\xi$$
$$[\![(\exists x)G]\!]_\xi := \bigcup_{i \in \mathbb{S}} [\![G]\!]_{\xi\{x \leftarrow i\}}$$
$$[\![(\forall x)G]\!]_\xi := \bigcap_{i \in \mathbb{S}} [\![G]\!]_{\xi\{x \leftarrow i\}}.$$

正如预期，这种语义是定义良好的。事实上，集合 $[\![\mathsf{Flip}(t)]\!]_\xi$、 $[\![t = s]\!]_\xi$ 和 $[\![t \subseteq s]\!]_\xi$ 都是可测的，而且可测性在所有逻辑算子下都得以保持。

通常意义下，语言 $\mathcal{RL}$ 的一种解释由一个环境 ξ 以及对 $\mathsf{Flip}(x)$ 的一种解释 η 给出。

定义 2.9（ $\mathcal{RL}$中公式的标准语义）。给定一个 $\mathcal{RL}$-公式F以及一个解释 $\rho = (\xi, \eta^{\text{FLIP}})$，其中 ξ: $\mathcal{G} \to \mathsf{S}$ 和 $\eta^{\text{FLIP}} \subseteq \mathsf{O}$， F 在 ρ $[\![F]\!]_\rho$中的解释归纳式地定义如下：

[3]如需了解更多详情，请参阅 [5]。

$$[\![\texttt{Flip}(t)]\!]_\rho := \begin{cases} 1 & \text{if } \eta^{\text{FLIP}}([\![t]\!]_\rho) = \mathbb{1} \\ 0 & \text{otherwise} \end{cases} \qquad [\![\neg G]\!]_\rho := 1 - [\![G]\!]_\rho$$

$$[\![t = s]\!]_\rho := \begin{cases} 1 & \text{if } [\![t]\!]_\rho = [\![s]\!]_\rho \\ 0 & \text{otherwise.} \end{cases} \qquad \begin{aligned} [\![G \wedge H]\!]_\rho &:= min\{[\![G]\!]_\rho, [\![H]\!]_\rho\} \\ [\![G \vee H]\!]_\rho &:= max\{[\![G]\!]_\rho, [\![H]\!]_\rho\} \\ [\![G \to H]\!]_\rho &:= max\{(1 - [\![G]\!]_\rho), [\![H]\!]_\rho\} \end{aligned}$$

$$[\![t \subseteq s]\!]_\rho := \begin{cases} 1 & \text{if } [\![t]\!]_\rho \subseteq [\![s]\!]_\rho \\ 0 & \text{otherwise} \end{cases} \qquad \begin{aligned} [\![(\forall x)G]\!]_\rho &:= min\{[\![G]\!]_{\rho\{x \leftarrow \sigma\}} \mid \sigma \in \mathbb{S}\} \\ [\![(\exists x)G]\!]_\rho &:= max\{[\![G]\!]_{\rho\{x \leftarrow \sigma\}} \mid \sigma \in \mathbb{S}\}. \end{aligned}$$

记号 2.5。为便于阅读，我们将 $[\![\cdot]\!]_\rho$ 简写为 $[\![\cdot]\!]_\eta$，将 $[\![\cdot]\!]_\xi$简写为 $[\![\cdot]\!]$。

注意到，$\mathcal{RL}$ 的定量语义与定性语义彼此相关，这一点可通过对公式 [5]的结构进行归纳来证明。

命题 2.2. 对于 $\mathcal{RL}$中的任意公式 F、环境 ξ、函数 $\eta \in$O 和 $\rho = (\eta, \xi)$,

$$[\![F]\!]_{\xi,\eta} = 1 \quad \textit{iff} \quad \eta \in [\![F]\!]_\rho.$$

3 RS_2^1 刻画 $\mathcal{POR}$

如前所述，我们的证明遵循一条可以说是标准的路径 [1, 6]。第一步是证明，$\mathcal{POR}$ 中的函数恰好是那些在 RS_2^1中可由 Σ_1^b表示的函数。为此，我们扩展 Buss 的可表示性条件，加入一项约束，将 RS_2^1 中公式的定量语义与预言机递归函数的附加函数参数 η 联系起来。

定义 3.1（Σ_1^b-可表示性）。函数 $f : \mathrm{S}^k \times \mathrm{O} \to \mathrm{S}$ 在 RS_2^1 中是 Σ_1^b-可表示的，当且仅当存在一个属于 $\mathcal{RL}$ 的 Σ_1^b-公式 $F(\vec{x}, y)$，使得:

1. $\mathrm{RS}_2^1 \vdash (\forall \vec{x})(\exists y)F(\vec{x}, y)$ 2. $\mathrm{RS}_2^1 \vdash (\forall \vec{x})(\forall y)(\forall z)\big(F(\vec{x}, y) \wedge F(\vec{x}, z) \to y = z\big)$3. 对所有 $\sigma_1, \ldots, \sigma_j, \tau \in \mathrm{S}$ 和 $\eta \in \mathrm{O}$,

$$f(\sigma_1, \ldots, \sigma_j, \eta) = \tau \quad \text{iff} \quad \eta \in [\![F(\overline{\sigma_1}, \ldots, \overline{\sigma_j}, \overline{\tau})]\!].$$

我们回顾一下，语言 $\mathcal{RL}$ 允许我们为公式 F 关联定性解释——即处理 1. 和 2. 时——以及定量解释——即处理 3. 时。接着，在第 3.1 节中，我们证明以下定理。

定理 3.1（$\mathcal{POR}$ 和 RS_2^1）。对于任意函数 $f : \mathrm{S}^k \times \mathrm{O} \to \mathrm{S}$, f 在 $f \in \mathcal{POR}$ 时可在 RS_2^1 中表示为 Σ_1^b-。

特别是，任何属于 $\mathcal{POR}$ 的函数都可在 RS_2^1 中由 Σ_1^b 表示，这一点在第 3.1 节中通过对概率预言机函数的结构进行直接归纳证明。反方向则在第 3.2 节中通过一种与 [3] 中提出的论证非常接近的可实现性论证得以确立。

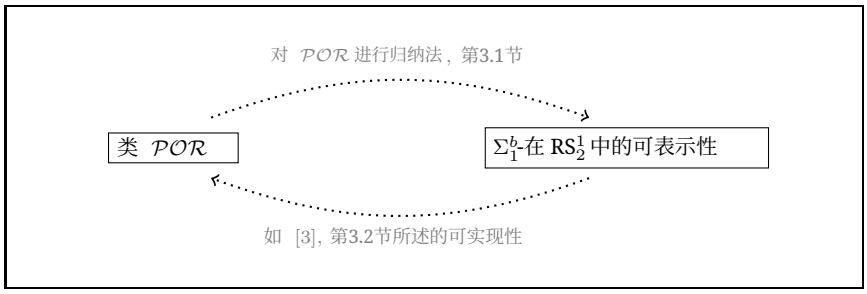


图3：关联 $\mathcal{POR}$ 与 RS_2^1

3.1 $\mathcal{POR}$ 中的函数在 RS_2^1 中可由 Σ_1^b 表示

我们通过对预言机函数的结构进行归纳，构造所需的公式，从而证明任何属于 $\mathcal{POR}$ 的函数都可在 RS_2^1 中由 Σ_1^b 表示。首先请注意，例如，条件 1 中出现的公式 $(\forall\vec{x})(\exists y)G(\vec{x},y)$ 不属于 Σ_1^b，因为其中的存在量词没有界定。因此，为了证明定理 3.3 的归纳步骤——即复合和记号上的有界递归——我们需要将 Parikh定理 [10] 调整到 RS_2^1。[4]

命题 3.2（“Parikh” [10]）。设 $F(\vec{x},y)$ 是 $\mathcal{RL}$ 中的有界公式，使得 $\mathrm{RS}_2^1 \vdash (\forall\vec{x})(\exists y)F(\vec{x},y)$。那么，存在一项 t，使得，

$$\mathbf{RS}_2^1 \vdash (\forall\vec{x})(\exists y \preceq t(\vec{x}))F(\vec{x},y).$$

定理 3.3。每个 $f \in \mathcal{POR}$ 都可在 RS_2^1 中由 Σ_1^b 表示。

证明概要。证明使用归纳法，依据 $\mathcal{POR}$ 中函数的结构。[5]

基例。每个基本函数都可在 RS_2 中由 Σ_1^b 表示。共有五种可能的子情况：[1]

- 空（字符串）函数。 $f = E$ 在 RS 中由公式[12] Σ_1^b 表示：

$$F_E(x,y) : x = x \wedge y = \epsilon.$$

1. 考虑 $y = \epsilon$ 可证明存在性。对于恒等式的自反性，$\mathrm{RS}_2^1 \vdash x = x$ 和 RS $_2^1 \vdash \epsilon = \epsilon$ 成立。因此，根据合取规则，我们得到 $\mathrm{RS}_2^1 \vdash x = x \wedge \epsilon = \epsilon$，并得出结论：

$$\mathbf{RS}_2^1 \vdash (\forall x)(\exists y)(x = x \wedge y = \epsilon).$$

[4]该定理通常在 Buss 有界理论的上下文中表述如下：给定 $\mathcal{L}_{\mathbb{N}}$ 中的一个有界公式 F，使得 $\mathrm{S}_2^1 \vdash (\forall\vec{x})(\exists y)F$，则存在一个项 $t(\vec{x})$，使得 $\mathrm{S}_2^1 \vdash (\forall\vec{x})(\exists y \leq t(\vec{x}))F(\vec{x},y)$ [1, 2] 也成立。此外，由于 [8], Buss 的句法证明可以很自然地改编为 Σ_1^b-NIA。同一结果也适用于 RS_2^1,，它不包含任何关于 `Flip(·)` 的特定规则。[5]更多详情请见附录 [?]。

2. 假设 $\mathbf{RS}_2^1 \vdash x = x \wedge z = \epsilon$ 可证明唯一性。根据合取规则，特别是 RS $\frac{1}{2} \vdash z = \epsilon$，并且由于 $\mathbf{RS}_2^1 \vdash y = \epsilon$，根据恒等关系的传递性，我们得出结论

$$\mathbf{RS}_2^1 \vdash y = z.$$

3. 假设 $E(\sigma, \eta^*) = \tau$。如果 $\tau = \boldsymbol{\epsilon}$，那么：

$$\begin{aligned}\llbracket \overline{\sigma} = \overline{\sigma} \wedge \overline{\tau} = \epsilon \rrbracket &= \llbracket \overline{\sigma} = \overline{\sigma} \rrbracket \cap \llbracket \overline{\tau} = \epsilon \rrbracket \\ &= \mathbb{O} \cap \mathbb{O} \\ &= \mathbb{O}.\end{aligned}$$

因此，在这种情况下，对于任意 η^*、$\eta^* \in \llbracket \overline{\sigma} = \overline{\sigma} \wedge \overline{\tau} = \epsilon \rrbracket$，显然 $\eta^* \in \mathsf{O}$。如果 $\tau \neq \boldsymbol{\epsilon}$，那么

$$\begin{aligned}\llbracket \overline{\sigma} = \overline{\sigma} \wedge \overline{\tau} = \epsilon \rrbracket &= \llbracket \overline{\sigma} = \overline{\sigma} \rrbracket \cap \llbracket \overline{\tau} = \epsilon \rrbracket \\ &= \mathbb{O} \cap \emptyset \\ &= \emptyset.\end{aligned}$$

因此，对于任意 η^*、$\eta^* \notin \llbracket \overline{\sigma} = \overline{\sigma} \vee \overline{\tau} = \epsilon \rrbracket$，显然 $\eta^* \notin \emptyset$。

- 投影（字符串）函数。 $f = P_i^n$ 对于 $1 \leq i \leq n$，可由以下公式在 RS$_{12}$ 中表示：

$$F_{P_i^n}(x, y) : \bigwedge_{j \in J} (x_j = x_j) \wedge y = x_i,$$

其中 $J = \{1, \ldots, n\} \setminus \{i\}$。

- 词后继函数。 $f = S_b$ 可由以下公式在 RS$_{12}$ 中表示：

$$F_{S_b}(x, y) : y = x\mathtt{b}$$

其中，若 $b = 0$，则 $\mathtt{b} = \mathtt{0}$；若 $b = 1$，则 $\mathtt{b} = \mathtt{1}$。

- 条件（字符串）函数。 $f = C$ 在 RS$_{12}$ 中由以下公式表示为 Σ_1^b：

$$\begin{aligned}F_C(x, v, z_0, z_1, y) : (x = \epsilon \wedge y = v) \vee (\exists x' \preceq x)(x = x'\mathtt{0} \wedge y = z_0) \\ \vee (\exists x' \preceq x)(x = x'\mathtt{1} \wedge y = z_1).\end{aligned}$$

- 查询（字符串）函数。 $f = Q$ 在 RS$_{12}$ 中由以下公式表示为 Σ_1^b：

$$F_Q(x, y) : (\mathtt{Flip}(x) \wedge y = \mathtt{1}) \vee (\neg \mathtt{Flip}(x) \wedge y = \mathtt{0}).$$

请注意，在这种情况下，证明的关键依赖于这样一个事实：预言机函数恰好调用一个预言机。

1. 存在性通过分类讨论来证明。若 $\mathrm{RS}_2^1 \vdash \mathrm{Flip}(x)$，令 $y = 1$。根据恒等式的自反性，RS $^1_2 \vdash 1 = 1$ 成立，因此 $\mathrm{RS}_2^1 \vdash \mathrm{Flip}($ $x \wedge 1 =)$ 也成立。根据析取规则，
1 $^1_2 \vdash$ $x \wedge 1 =$
我们得出 RS (Flip( ) 1) $\vee (\neg\mathrm{Flip}(x) \wedge 1 = 0)$，因此，

$$\mathbf{RS}_2^1 \vdash (\exists y)\big((\mathtt{Flip}(x) \wedge y = 1) \vee (\neg\mathtt{Flip}(x) \wedge y = 0)\big).$$

若 RS $^1_2 \vdash \neg$ x $y = 0$ $^1_2 \vdash$ Flip( )，令 。根据恒等式的自反性，RS 成立。
$0 = 0$ $\neg$ x $\wedge$
因此，根据合取规则，RS Flip( ) $0 = 0$ $^1_2 \vdash$ $x \wedge 0 = 1 \vee$；根据析取规则，
我们得出 RS (Flip( )) $(\neg\mathrm{Flip}(x) \wedge 0 = 0)$，于是，

$$\mathbf{RS}_2^1 \vdash (\exists y)\big((\mathtt{Flip}(x) \wedge y = 1) \vee (\neg\mathtt{Flip}(x) \wedge y = 0)\big).$$

2. 唯一性是借助恒等关系的传递性得以确立的。
3. 最后，我们证明对于每个 $\sigma, \tau \in \mathsf{S}$ 和 $\eta^* \in \mathsf{O}$，当 $\eta^* \in [\![F_Q(\overline{\sigma}, \overline{\tau})]\!]$ 时，$Q(\sigma, \eta^*) = \tau$。假设 $Q(\sigma, \eta^*) = \mathbb{1}$，也就是 $\eta^*(\sigma) = \mathbb{1}$，

$$\begin{aligned}
[\![F_Q(\overline{\sigma}, \overline{\tau})]\!] &= [\![\mathtt{Flip}(\overline{\sigma}) \wedge \overline{\tau} = 1]\!] \cup [\![\neg\mathtt{Flip}(\overline{\sigma}) \wedge \overline{\tau} = 0]\!] \\
&= ([\![\mathtt{Flip}(\overline{\sigma})]\!] \cap [\![1 = 1]\!]) \cup ([\![\neg\mathtt{Flip}(\overline{\sigma})]\!] \cap [\![1 = 0]\!]) \\
&= ([\![\mathtt{Flip}(\overline{\sigma})]\!] \cap \mathbb{O}) \cup ([\![\neg\mathtt{Flip}(\overline{\sigma})]\!] \cap \emptyset) \\
&= [\![\mathtt{Flip}(\overline{\sigma})]\!] \\
&= \{\eta \mid \eta(\sigma) = \mathbb{1}\}.
\end{aligned}$$

显然，$\eta^* \in [\![(\mathrm{Flip}(\overline{\sigma}) \wedge \overline{\tau} = 1) \vee (\neg\mathrm{Flip}(\overline{\sigma}) \wedge \overline{\tau} = 0)]\!]$。
$Q(\sigma, \eta^*) = \mathbb{0}$ 的情形以及反方向的证明方法类似。

归纳情形。若 f 由Σ_1^b-可表示函数经复合或有界递归定义，则 f 在 RS_2^1 中是Σ_1^b-可表示的：

- 复合。假设 f 由函数$g, h_1, \ldots, h_k$经复合定义，使得

$$f(\vec{x}, \eta) = g(h_1(\vec{x}, \eta), \ldots, h_k(\vec{x}, \eta), \eta)$$

并且 $g, h_1, \ldots, h_k$分别由 Σ_1^b-公式 $F_g, F_{h_1}, \ldots, F_{h_k}$在 RS_2^1 中表示。根据命题 3.2，存在适当的项 $t_g, t_{h_1}, \ldots, t_{h_k}$，使定义 3.1 的条件 1 可以加强为：对每个 $i \in \{g, h_1, \ldots, h_k\}$，都有 $\mathrm{RS}_2^1 \vdash (\forall \vec{x})(\exists y \preceq t_i) F_i(\vec{x}, y)$。由此可知，$f(\vec{x}, \eta)$由以下公式在 RS_2^1 中 Σ_1^b-表示：

$$F_f(x, y) : (\exists z_1 \preceq t_{h_1}(\vec{x})) \ldots (\exists z_k \preceq t_{h_k}(\vec{x}))\big(F_{h_1}(\vec{x}, z_1) \wedge \ldots F_{h_k}(\vec{x}, z_k) \wedge F_g(z_1, ..., z_k, y)\big).$$

事实上，根据归纳假设，F_g、F_{h_1}、.....、F_{h_k}都是 Σ_1^b-公式。那么，F_f也属于 Σ_1^b。稍作修改即可通过标准证明证明条件 1.-3. 成立。

- 有界递归。假设 f 由g、 h_0和 h_1 通过有界递归定义，使得：

$$f(\vec{x}, \epsilon, \eta) = g(\vec{x}, \eta)$$
$$f(\vec{x}, y\mathbb{b}, \eta) = h_i(\vec{x}, y, f(\vec{x}, y, \eta), \eta)|_{t(\vec{x},y)},$$

其中，当 $i \in \{0,1\}$ 且 $\mathsf{b} = \mathbb{0}$ 时 $i = 0$，而当 $i = 1$时 $= \mathbb{1}$，且 b g。令 h_0、 h_1、$\frac{1}{2}$分别由 RS Σ_1^b中的 F_g公式 F_{h_0}、 F_{h_1}和 t_g表示。此外，根据命题 3.2，存在适当的项 t_{h_0}、 t_{h_1}和 f，使得定义 3.1 的条件 1. 可以强化为其“有界版本”。于是可以证明，$\vec{x}(y, \Sigma_1^b)$由下列公式在 RS_2^1 中 表示：

$$F_f(x,y) : (\exists v \preceq t_g(\vec{x})t_f(\vec{x})(y \times t(\vec{x},y)t(\vec{x},y)11))\big(F_{lh}(v, 1 \times y1) \wedge (\exists z \preceq t_g(\vec{x}))(F_{eval}(v,\epsilon,z) \wedge F_g(\vec{x},z)) \wedge (\forall u \subset y)(\exists z)\big(\tilde{z} \preceq t(\vec{x},y)\big)\big(F_{eval}(v, 1 \times u, z) \wedge F_{eval}(v, 1 \times u1, \tilde{z}) \wedge (u0 \subseteq y \to (\exists z_0 \preceq t_{h_0}(\vec{x},u,z))(F_{h_0}(\vec{x},u,z,z_0) \wedge z_0|_{t(\vec{x},u)} = \tilde{z})) \wedge (u1 \subseteq y \to (\exists z_1 \preceq t_{h_1}(\vec{x},u,z))(F_{h_1}(\vec{x},u,z,z_1) \wedge z_1|_{t(\vec{x},u)} = \tilde{z}))\big)\big),$$

其中 F_{lh} 和 F_{eval} 是按 [7]中所述定义的 Σ_1^b公式。直观地说， $F_{lh}(x,y)$ 表示 x 的编码中 1 的数量为 yy；而 $F_{eval}(x,y,z)$ 是一个“解码”公式（与 G¨odel 的 β公式十分相似），表示 x 中编码为其第 y位的“位”为 z。此外， $x \subset y$ 是 $x \subseteq y \wedge x \neq y$的缩写。因此，这个公式 F_f 满足在 RS_2^1 中以 Σ_1^b表示函数 f的所有要求；该函数由 g、 h_0和 h_1通过有界递归得到。具体而言，关于存在性和唯一性的条件 1 和 2 已由 Ferreira [7]证明成立。此外， F_f 表示：给定所需的编码序列 v：(i.) v 的第 ϵ位是（对）满足 $F_g(\vec{x}, z')$ 的 z' 的编码，其中（根据归纳假设） F_g 是表示函数 g的 Σ_1^b公式；(ii.) 已知对每个 $u \subset y$， z 表示 v 在位置 $1 \times u$编码的“位”，类似地， $\tilde{z}$是下一个“位”，编码在 v的位置 $1 \times u1$，那么如果 $u\mathsf{b} \subseteq y$（也就是说，如果我们考虑 y 的初始子串，且其最后一位对应于 b），则存在一个 z_b，使得 $F_{h_b}(\vec{x}, y, z, z_b)$，其中 F_{h_b} Σ_1^b表示函数 f_{h_b}，而 z_b 在 $t(\vec{x},u)$ 处的截断恰好是 $\tilde{z}$；当 $\mathsf{b} = 0$ 时为 $b = 0$，当 $\mathsf{b} = 1$时为 $b = 1$。[6]

□

[6]换言之，如果 $u0 \subseteq y$，则存在一个 z_0，使得 Σ_1^b-公式 $F_{h_0}(\vec{x}, u, z, z_0)$ 表示函数 h_0；在这种情况下， $\tilde{z}$ 对应于 z_0 在 $t(\vec{x},u)$ 处的截断，也就是说， v 在位置 $1 \times u1$（即对应于 $u0 \subseteq y$）所编码的“位”恰好就是这样的 $\tilde{z}$。同样，如果 $u1 \subseteq y$，则存在一个 z_0，使得 Σ_1^b-公式 $F_{h_1}(\vec{x}, u, z, z_1)$ 表示函数 h_1，而 $\tilde{z}$对应于 z_1 在 $t(\vec{x},u)$ 处的截断，也就是说，v 在位置 $1 \times u1$（即对应于 $u1 \subseteq y$）所编码的“位”恰好就是这样的 $\tilde{z}$。更多细节请参见附录 [?]。

3.2 在 RS_2^1 中可由 Σ_1^b 表示的函数属于 $\mathcal{POR}$

这里，我们考虑相反的方向。我们的证明是通过改编 Cook 和 Urquhart 对 IPV^ω [3]的证明得到的。该证明经过对 RS_2^1, 的直觉主义版本（称为 IRS_2^1 ）的可实现性解释，并按如下方式展开：

1. 首先，我们为一种简单类型的 λ-演算定义基本等式理论 $\mathcal{POR}^\lambda$ ，该演算带有与 $\mathcal{POR}$ 的函数相对应的原语。2. 其次，我们引入一阶直觉主义理论 $\mathcal{IPOR}^\lambda$，它在 $\mathcal{POR}^\lambda$ 的基础上扩展了通常的谓词演算以及 NP 归纳模式。我们证明， $\mathcal{IPOR}^\lambda$ 足以证明 IRS_2^1, （RS_2^1 的直觉主义版本）的所有定理。3. 接着，我们在 $\mathcal{IPOR}^\lambda$ 内部发展其可实现性解释，证明对于 $(\forall x)(\exists y)F(x, y)$ 的任意推导（其中 F 是一个 Σ_0^b-公式），都可以提取一个 $\mathcal{POR}^\lambda$ 的 λ-项 t，使得 $(\forall x)F(x, \mathrm{t}x)$ 可在 $\mathcal{IPOR}^\lambda$ 中证明。由此我们推得，每个在 IRS_2^1 中可由 Σ_1^b 表示的函数都属于 $\mathcal{POR}$。4. 最后，我们将这一结果扩展到经典 RS_2^1，证明任何在 $\mathcal{IPOR}^\lambda + $ 中可由排中律（EM，简称 EM）证明的 Σ_1^b-公式，都已经可以在 $\mathcal{IPOR}^\lambda$ 中证明。

3.2.1 System $\mathcal{POR}^\lambda$

我们为简单类型的 λ 演算定义一个等式理论，并加入用于 $\mathcal{POR}$ 函数的原语。实际上，这些原语与 $\mathcal{POR}$ 中的原语并不完全对应，不过，最终得到的函数代数已被证明与之等价。[7]

$\mathcal{POR}^\lambda$ 的语法。我们先来考察 $\mathcal{POR}^\lambda$ 的语法。

定义 3.2（$\mathcal{POR}^\lambda$ 的类型）。 $\mathcal{POR}^\lambda$ 的类型由以下文法定义：

$$\sigma := s \mid \sigma \Rightarrow \sigma.$$

定义 3.3（$\mathcal{POR}^\lambda$ 的项）。 $\mathcal{POR}^\lambda$ 的项是标准的简单类型

[7]我们的选择遵循这样一条原则：除递归算子外，其他函数的定义方程不应依赖于递归算子。

λ-项，以及以下常量：

$0、1、\epsilon：s$

$\circ：s \Rightarrow s \Rightarrow s$ Tail：$s \Rightarrow s$ Trunc：$s \Rightarrow s \Rightarrow s$ 条件函数：
$s \Rightarrow s \Rightarrow s \Rightarrow s \Rightarrow s$ Flipcoin：$s \Rightarrow s$ 归约函数：$s \Rightarrow$ （
$s \Rightarrow s \Rightarrow s$）（$s \Rightarrow s \Rightarrow s$）（$s \Rightarrow s$）$\Rightarrow s \Rightarrow s$.

直观地说，Tail(x) 计算删除 x 的首位数字后得到的字符串；Trunc(x, y) 计算将 x 截断至 y 的长度后得到的字符串；条件函数(x, y, z, w) 计算这样一个函数：当 $x = \epsilon$ 时输出 y，当 $x = x'\mathbb{0}$ 时输出 z，当 $x = x'\mathbb{1}$ 时输出 w；Flipcoin(x) 表示一个随机 $\mathbb{0}/\mathbb{1}$ 生成器；递归算子是记号上的有界递归算子。

记法 3.1。我们通常将 $x \circ y$ 简写为 xy。此外，为了便于阅读，设 T 是任意一个元数为 n 的常量 Tail、Trunc、条件函数、Flipcoin 或递归算子，我们将 Tu_1、...、u_n 记作 $\mathsf{T}(\mathsf{u}_1, \ldots, \mathsf{u}_n)$。

$\mathcal{POR}^\lambda$ 与 Cook 和 Urquhart 提出的 PV^ω 颇为相似 [3]，但不包含我们不需要的归纳规则 (R5)。主要区别在于常量 Flipcoin；如前所述，直观而言，它表示一个函数，该函数读取字符串时会随机生成 0 或 1。[8]

备注 3.1. 下文中，我们经常使用记号上的有界递归来隐式定义项。换句话说，我们通过如下形式的方程来定义新项，例如 $\mathsf{F}：s \Rightarrow \ldots \Rightarrow s$：

$$\begin{aligned} \mathsf{F}\vec{x}\epsilon &:= \mathsf{G}\vec{x} \\ \mathsf{F}\vec{x}(y0) &:= \mathsf{H}_0\vec{x}y(\mathsf{F}\vec{x}y) \\ \mathsf{F}\vec{x}(y1) &:= \mathsf{H}_1\vec{x}y(\mathsf{F}\vec{x}y), \end{aligned}$$

其中 G,H_0,H_1 是已定义的项，第二个和第三个方程满足由某个项 K 给出的长度界（通常为 $\lambda\vec{x}\lambda y.0$）。项 F 可以显式定义如下：

$$\mathsf{F} := \lambda\vec{x}.\lambda y.\mathsf{Rec}(\mathsf{G}\vec{x}, \lambda yy'.\mathsf{H}_0\vec{x}yy', \lambda yy'.\mathsf{H}_1\vec{x}yy', \mathsf{K}\vec{x}, y).$$

我们还引入以下复合函数的缩写：

- B(x) := 条件函数(x, ϵ, 0, 1) 表示计算 x最后一位的函数，即将 x 强制转换为布尔值
- BNeg(x) := Cond(x, ϵ, 1, 0) 表示对 B(x) 进行布尔取反的函数

[8]下面的定义 3.6 将阐明这些解释。

• BOr(x, y) := Cond(B(x), B(y), B(y), 1) 表示将 x 和 y 强制转换为布尔值，然后执行或运算的函数
• BAnd(x, y) := Cond(B(x) ϵ, 0, B(y)) 表示先将 x和 y 强制转换为布尔值，然后执行与运算的函数
• Eps(x) := Cond(x, 1, 0, 0) 表示谓词"$x = \epsilon$"的特征函数

• Bool(x) := BAnd(Eps(Tail(x)), BNeg(Eps(x))) 表示谓词"$x = 0 \vee x = 1$"的特征函数
• Zero(x) := Cond(Bool(x),0,Cond(x, 0,0,1),0) 表示谓词"$x = 0$"的特征函数

• Conc(x, y) 表示由下列方程定义的连接函数：

$$\mathsf{Conc}(x, \epsilon) := x \qquad \mathsf{Conc}(x, y\mathsf{b}) := \mathsf{Conc}(x, y)\mathsf{b},$$

其中 $\mathsf{b} \in \{0, 1\}$。
• Eq(x, y) 表示谓词"$x = y$"的特征函数，并由下面的方程通过双重递归定义：

$$\begin{aligned} \mathsf{Eq}(\epsilon, \epsilon) &:= 1 \qquad \mathsf{Eq}(\epsilon, y\mathsf{b}) := 0 \\ \mathsf{Eq}(x\mathsf{b}, \epsilon) = \mathsf{Eq}(x0, y1) = \mathsf{Eq}(x1, y0) &:= 0 \qquad \mathsf{Eq}(x\mathsf{b}, y\mathsf{b}) := \mathsf{Eq}(x, y), \end{aligned}$$

其中 $\mathsf{b} \in \{0, 1\}$
• Times(x, y) 表示用于自连接的函数 $x, y \mapsto x \times y$，并由下面的方程定义：

$$\mathsf{Times}(x, \epsilon) := \epsilon \qquad \mathsf{Times}(x, y\mathsf{b}) := \mathsf{Conc}(\mathsf{Times}(x, y), x),$$

其中 $\mathsf{b} \in \{0, 1\}$。
• Sub(x, y) 表示初始子串函数 $x, y \mapsto S(x, y)$，并按如下方式通过有界递归定义：

$$\mathsf{Sub}(x, \epsilon) := \mathsf{Eps}(x) \qquad \mathsf{Sub}(x, y\mathsf{b}) := \mathsf{BOr}(\mathsf{Sub}(x, y), \mathsf{Eq}(x, y\mathsf{b})),$$

其中 $\mathsf{b} \in \{0, 1\}$。

定义 3.4（ $\mathcal{POR}^\lambda$的公式）。 $\mathcal{POR}^\lambda$ 的公式是方程 $\mathsf{t} = \mathsf{u}$，其中 t 和 u 是类型为 s 的项。

理论 $\mathcal{POR}^\lambda$。现在我们引入理论 $\mathcal{POR}^\lambda$。

定义 3.5（理论 $\mathcal{POR}^\lambda$）。 $\mathcal{POR}^\lambda$ 的公理如下：

- $\mathcal{POR}^{\lambda}$中常量的定义方程：

$$\epsilon x = x\epsilon = x \qquad x(y\mathsf{b}) = (xy)\mathsf{b}$$

$$\mathsf{Tail}(\epsilon) = \epsilon \qquad \mathsf{Tail}(x\mathsf{b}) = x$$

$$\mathsf{Trunc}(x, \epsilon) = \mathsf{Trunc}(\epsilon, x) = \epsilon$$
$$\mathsf{Trunc}(x\mathsf{b}, y\mathsf{0}) = \mathsf{Trunc}(x\mathsf{b}, y\mathsf{1}) = \mathsf{Trunc}(x, y)\mathsf{b}$$

$$\mathsf{Cond}(\epsilon, y, z, w) = y \qquad \mathsf{Cond}(x\mathsf{0}, y, z, w) = z \qquad \mathsf{Cond}(x\mathsf{1}, y, z, w) = w$$

$$\mathsf{Bool}(\mathsf{Flipcoin}(x)) = \mathsf{1}$$

$$\mathsf{Rec}(x, h_0, h_1, k, \epsilon) = x$$
$$\mathsf{Rec}(x, h_0, h_1, k, y\mathsf{b}) = \mathsf{Trunc}(h_b y(\mathsf{Rec}(x, h_0, h_1, k, y)), ky),$$

其中 $\mathsf{b} \in \{0, 1\}$ 和 $b \in \{0, 1\}$.[9]

- (β)-公理和 (ν)-公理：

$$\mathsf{C}\big[(\lambda x.\mathsf{t})\mathsf{u}\big] = \mathsf{C}\big[\mathsf{t}\{\mathsf{u}/x\}\big] \tag{β}$$
$$\mathsf{C}\big[\lambda x.\mathsf{t}x\big] = \mathsf{C}\big[\mathsf{t}\big]. \tag{ν}$$

其中 $\mathsf{C}\big[\,\cdot\,\big]$ 表示一个上下文，其中空位 $\big[\,\big]$唯一出现，因此 $\mathsf{C}\big[\mathsf{t}\big]$ 表示在 $\mathsf{C}\big[\,\big]$中用 t 替换 $\big[\,\big]$ 时进行变量捕获。

$\mathcal{POR}^{\lambda}$ 的推理规则如下：

$$\mathsf{t} = \mathsf{u} \vdash \mathsf{u} = \mathsf{t} \tag{R1}$$
$$\mathsf{t} = \mathsf{u}, \mathsf{u} = \mathsf{v} \vdash \mathsf{t} = \mathsf{v} \tag{R2}$$
$$\mathsf{t} = \mathsf{u} \vdash \mathsf{v}\{\mathsf{t}/x\} = \mathsf{v}\{\mathsf{u}/x\} \tag{R3}$$
$$\mathsf{t} = \mathsf{u} \vdash \mathsf{t}\{\mathsf{v}/x\} = \mathsf{u}\{\mathsf{v}/x\}. \tag{R4}$$

正如预期的那样，$\vdash_{\mathcal{POR}^{\lambda}} \mathsf{t} = \mathsf{u}$ 表示方程 $\mathsf{t} = \mathsf{u}$ 可通过使用上述公理的实例以及推理规则 (R1)-(R4) 推导出来。类似地，给定任意一组方程 T，$\mathsf{T} \vdash_{\mathcal{POR}^{\lambda}} \mathsf{t} = \mathsf{u}$ 表示方程 $\mathsf{t} = \mathsf{u}$ 可通过使用上述公理和规则的实例以及 T 中的方程推导出来。

关联 $\mathcal{POR}$ 和 $\mathcal{POR}^{\lambda}$。对于任意字符串 $\sigma \in \mathsf{S}$，令 $\overline{\sigma}$：s 表示 $\mathcal{POR}^{\lambda}$ 中与之对应的项，也就是说：

$$\overline{\epsilon} = \epsilon \qquad \overline{\sigma\mathbb{0}} = \overline{\sigma}\mathsf{0} \qquad \overline{\sigma\mathbb{1}} = \overline{\sigma}\mathsf{1}.$$

[9]当 if $\mathsf{b} = 0$，则 $b = 0$ 且 $\mathsf{b} = 1$，则 $b = 1$.

对于任意 $\eta \in \mathsf{O}$，令 T_η 为所有形式为 $\mathsf{Flipcoin}(\overline{\sigma}) = \eta(\sigma)$ 的方程所组成的集合。

定义 3.6。项 $f \times^j \to s \Rightarrow \ldots \Rightarrow s$ 可证明地表示 $\mathcal{POR}$ 的查询函数 $\sigma_1 \ldots \sigma_j \sigma \in$（可证明表示性）。设 $\mathsf{O}\ \mathsf{S}\ \mathsf{S}$。若项 t : 对所有字符串 , , , S 和 $\eta \in$O 都满足以下条件，则称 t 可证明地表示 f,

$$f(\sigma_1, \ldots, \sigma_j, \eta) = \sigma \quad \text{iff} \quad T_\eta \vdash_{\mathcal{POR}^\lambda} \mathsf{t}\overline{\overline{\sigma_1}} \ldots \overline{\overline{\sigma_j}} = \overline{\overline{\sigma}}.$$

例 3.1。项 Flipcoin : $s \Rightarrow s$ 可证明地表示 $\mathcal{POR}$ 的查询函数 $Q(x, \eta) = \eta(x)$，因为对于任意 $\sigma \in \mathsf{S}$ 和 $\eta \in \mathsf{O}$,

$$\mathsf{Flipcoin}(\overline{\overline{\sigma}}) = \overline{\overline{\eta(\sigma)}} \vdash_{\mathcal{POR}^\lambda} \mathsf{Flipcoin}(\overline{\overline{\sigma}}) = \overline{\overline{Q(\sigma, \eta)}}.$$

现在我们来考察上文描述的一些项，并证明它们表示预期的函数。令 $Tail(\sigma, \eta)$ 表示通过截去 σ 的第一位所得的字符串，并令 $Trunc(\sigma_1, \sigma_2, \eta) = \sigma_1|_{\sigma_2}$。

引理 3.4。项 Tail、Trunc 和 Cond 分别可证明地表示函数 $Tail$、$Trunc$ 和 C。

证明概要。对于 Tail 和 Cond，该结论可直接由相应常量的定义公理推出。例如，若 $\sigma_1 = \sigma_2\mathbb{0}$，则 $Tail(\sigma_1, \eta) = \sigma_2$（且 $\overline{\overline{\sigma_1}} = \overline{\overline{\sigma_2\mathbb{0}}} = \overline{\overline{\sigma_2}}$0）。利用 Tail 的定义公理,

$$\vdash_{\mathcal{POR}^\lambda} \mathsf{Tail}(\overline{\overline{\sigma_1}}) = \mathsf{Tail}(\overline{\overline{\sigma_2\mathbb{0}}}) = \overline{\overline{\sigma_2}}.$$

对 $Trunc$ 关于 σ_1 进行双重归纳后，我们得出：$\sigma_2 \in \mathsf{S}$

$$\vdash_{\mathcal{POR}^\lambda} \mathsf{Trunc}(\overline{\overline{\sigma_1}}, \overline{\overline{\sigma_2}}) = \overline{\overline{\sigma_1}|_{\overline{\sigma_2}}}.$$

□

我们通过下面的定理 3.5 将这一结果推广。

定理 3.5。1. 任意函数 $f \in \mathcal{POR}$ 都可以由一个项 $\mathsf{t} \in \mathcal{POR}^\lambda$ 可证明地表示。

2. 对于任意项 $\mathsf{t} \in \mathcal{POR}^\lambda$，存在一个函数 $f \in \mathcal{POR}$，使得 f 可以由 t 可证明地表示。

证明概要。1. 证明通过对 $f \in \mathcal{POR}$ 的结构进行归纳得出：

基例。每个基本函数都可以被可证明地表示。我们只考虑两个例子：

- 空函数。$f = E$ 可证明由项 $\lambda x.\epsilon$ 表示。对于任意字符串 $\sigma \in \mathsf{S}$，$E(\sigma, \eta) = \overline{\epsilon} = \epsilon$ 成立。此外，$\vdash_{\mathcal{POR}^\lambda} (\overline{\lambda}x.\epsilon)\overline{\sigma} = \epsilon$ 是（β）公理的一个实例。因此，我们得出：

$$\vdash_{\mathcal{POR}^\lambda} (\lambda x.\epsilon)\overline{\overline{\sigma}} = \overline{\overline{E(\sigma, \eta)}}.$$

• 查询函数。 $f = Q$ 可证明由项 Flipcoin 表示，正如上文例 3.1 所示。

归纳情形。由可证明表示的函数通过复合或有界递归定义的每个函数，也都是可证明表示的。我们考虑有界递归的情形。设 f 定义如下：

$$\begin{aligned} f(\sigma_1,\ldots,\sigma_n,\epsilon,\eta) &= g(\sigma_1,\ldots,\sigma_n,\eta)\\ f(\sigma_1,\ldots,\sigma_n,\sigma\mathbb{0},\eta) &= h_0(\sigma_1,\ldots,\sigma_n,\sigma,f(\sigma_1,\ldots,\sigma_n,\sigma,\eta),\eta)|_{k(\sigma_1,\ldots,\sigma_n,\sigma)}\\ f(\sigma_1,\ldots,\sigma_n,\sigma\mathbb{1},\eta) &= h_1(\sigma_1,\ldots,\sigma_n,\sigma,f(\sigma_1,\ldots,\sigma_n,\sigma,\eta),\eta)|_{k(\sigma_1,\ldots,\sigma_n,\sigma)}. \end{aligned}$$

根据归纳假设， g、 h_0、 h_1 和 k 分别由对应的项 $\mathsf{t_g}$、$\mathsf{t_{h_1}}$、$\mathsf{t_{h_2}}$、$\mathsf{t_k}$ 可证明地表示。因此，对于任意 σ_1、.....、 σ_{n+2}、 $\sigma \in \mathsf{S}$ 和 $\eta \in \mathsf{O}$，我们可推出：

$$T_\eta \vdash_{\mathcal{POR}^\lambda} \mathsf{t_g}\overline{\overline{\sigma_1}}\ldots\overline{\overline{\sigma_n}} = \overline{\overline{g(\sigma_1,\ldots,\sigma_n,\eta)}} \qquad (\mathsf{t_g})$$

$$T_\eta \vdash_{\mathcal{POR}^\lambda} \mathsf{t_{h_0}}\overline{\overline{\sigma_1}}\ldots\overline{\overline{\sigma_{n+2}}} = \overline{\overline{h_0(\sigma_1,\ldots,\sigma_{n+2},\eta)}} \qquad (\mathsf{t_{h_0}})$$

$$T_\eta \vdash_{\mathcal{POR}^\lambda} \mathsf{t_{h_1}}\overline{\overline{\sigma_1}}\ldots\overline{\overline{\sigma_{n+2}}} = \overline{\overline{h_1(\sigma_1,\ldots,\sigma_{n+2},\eta)}} \qquad (\mathsf{t_{h_1}})$$

$$T_\eta \vdash_{\mathcal{POR}^\lambda} \mathsf{t_k}\overline{\overline{\sigma_1}}\ldots\overline{\overline{\sigma_n}} = \overline{\overline{k(\sigma_1,\ldots,\sigma_n,\eta)}}. \qquad (\mathsf{t_k})$$

我们可以对 σ 使用归纳法证明：

$$T_\eta \vdash_{\mathcal{POR}^\lambda} \mathsf{t_f}\overline{\overline{\sigma_1}}\ldots\overline{\overline{\sigma_n\sigma}} = \overline{\overline{f(\sigma_1,\ldots,\sigma_n,\eta)}},$$

其中

$$\mathsf{t_f} : \lambda x_1\ldots\lambda x_n.\lambda x.\mathsf{Rec}(\mathsf{t_g}x_1\ldots x_n, \mathsf{t_{h_0}}x_1\ldots x_n, \mathsf{t_{h_1}}x_1\ldots x_n, \mathsf{t_k}x_1\ldots x_n, x).$$

那么，

• 若 $\sigma = \epsilon$，则 $f(\sigma_1$、.....、 σ_n、 σ、 $\eta) = g(\sigma_1$、.....、 σ_n、 $\eta)$。利用 (β)-公理，我们可推出：

$$\vdash_{\mathcal{POR}^\lambda} \mathsf{t_f}\overline{\overline{\sigma_1}}\ldots\overline{\overline{\sigma_n\sigma}} = \mathsf{Rec}(\mathsf{t_g}\overline{\overline{\sigma_1}}\ldots\overline{\overline{\sigma_n}}, \mathsf{t_{h_0}}\overline{\overline{\sigma_1}}\ldots\overline{\overline{\sigma_n}}, \mathsf{t_{h_1}}\overline{\overline{\sigma_1}}\ldots\overline{\overline{\sigma_n}}, \mathsf{t_k}\overline{\overline{\sigma_1}}\ldots\overline{\overline{\sigma_n}}, \overline{\overline{\sigma}})$$

并使用递归公理 $\mathsf{Rec}(\mathsf{t_g}x_1\ldots x_n, \mathsf{t_{h_0}}x_1\ldots x_n, \mathsf{t_{h_1}}x_1\ldots x_n, \mathsf{t_k}x_1\ldots x_n, \epsilon) = \mathsf{t_g}x_1\ldots x_n$，我们得到，

$$\vdash_{\mathcal{POR}^\lambda} \mathsf{t_f}\overline{\overline{\sigma_1}}\ldots\overline{\overline{\sigma_n\sigma}} = \mathsf{t_g}\overline{\overline{\sigma_1}}\ldots\overline{\overline{\sigma_n}},$$

根据（R2）和（R3）。结合（$\mathsf{t_g}$）与（R2），我们得出结论。

• 如果 $\sigma = \sigma_m\mathbb{0}$，那么 $f(\sigma_1,\ldots,\sigma_n,\sigma,\eta) = h_0(\sigma_1,\ldots,\sigma_n,\sigma_m,f(\sigma_1,\ldots,\sigma_n,\sigma,\eta),\eta)|_{k(\sigma_1,\ldots,\sigma_n,\sigma_m)}$。根据归纳假设，我们假设，

$$T_\eta \vdash_{\mathcal{POR}^\lambda} \mathsf{t_f}\overline{\overline{\sigma_1}}\ldots\overline{\overline{\sigma_n\sigma_m}} = \overline{\overline{f(\sigma_1,\ldots,\sigma_n,\sigma',\eta)}}.$$

然后，利用 (β)-公理 $\mathsf{t_f}\overline{\sigma_1}\ldots\overline{\sigma_n\sigma}$ = 递归算子($\mathsf{t_g}$ $\overline{\sigma_1}\cdots\overline{\sigma_n}$, $\mathsf{t_{h_0}}\overline{\sigma_1}\ldots\overline{\sigma_n}$, $\mathsf{t_{h_1}}\overline{\sigma_1}\ldots\overline{\sigma_n}$, $\mathsf{t_k}\overline{\sigma_1}\ldots\overline{\sigma_n,\sigma}$)、递归公理 $(g, h_0, h_1, k, x0)$ = 截断 $(h_0 x($ 递归算子 $(g, h_0, h_1, k, 0))$ $kx)$ 以及归纳假设，我们推得，

$$\vdash_{\mathcal{POR}^\lambda} \mathsf{t_f}\overline{\sigma_1}\ldots\overline{\sigma_n\sigma} = \text{截断}(\mathsf{t_{h_0}}\overline{\sigma_1}\ldots\overline{\sigma_n\sigma_m} f(\overline{\sigma_1, \ldots, \sigma_n, \sigma_m, \eta}), \mathsf{t_k}\overline{\sigma_1}\ldots\overline{\sigma_n})$$

由 (R2) 和 (R3) 得出。利用 ($\mathsf{t_{h_0}}$) 和 ($\mathsf{t_k}$)，结合 (R3) 和 (R2)，我们得出：

$$\vdash_{\mathcal{POR}^\lambda} \mathsf{t_f}\overline{\sigma_1}\ldots\overline{\sigma_n\sigma} = \overline{h_0(\sigma_1, \ldots, \sigma_n, \sigma_m, f(\sigma_1, \ldots, \sigma_n, \sigma_m, \eta))|_{k(\sigma_1,\ldots,\sigma_n,\sigma_m)}}.$$

- 情形 $\sigma = \sigma_m\mathbb{1}$ 以类似方式得证。

2. 这是简单类型λ-演算的规范化性质的一个推论： β-范式项 t : $s \Rightarrow \ldots \Rightarrow s$ 不可能包含高阶类型的变量。通过穷举检查可能的范式，可以验证这些范式都表示 $\mathcal{POR}$ 中的函数。 □

推论 3.1. 对于任意函数 $f\colon \mathsf{S}^j \times \mathsf{O} \to \mathsf{S}$， $f \in \mathcal{POR}$ 当 f 由某个项 t : $s \Rightarrow \ldots \Rightarrow s \in \mathcal{POR}^\lambda$ 可证表示时。

3.2.2 理论 $\mathcal{IPOR}^\lambda$

我们引入一种称为 $\mathcal{IPOR}^\lambda$ 的一阶直觉主义理论，它通过基本谓词演算和受限归纳原理扩展了 $\mathcal{POR}^\lambda$ 。我们还定义了 IRS_2^1 ，它是 RS_2^1 的一个变体，其逻辑基础采用直觉主义而非经典谓词演算。 $\mathcal{POR}^\lambda$ 和 IRS_2^1 中的所有定理都可在 $\mathcal{IPOR}^\lambda$ 中证明。事实上， $\mathcal{IPOR}^\lambda$ 可视为 $\mathcal{POR}^\lambda$ 的扩展，并提供了一种语言，用于将 IRS_2^1 中的推导与多项式时间可计算函数（对应于 $\mathcal{IPOR}^\lambda$ 的项）联系起来。

$\mathcal{IPOR}^\lambda$ 的语法。等式理论 $\mathcal{POR}^\lambda$ 相当弱。特别是，连简单的方程（例如 $x = \mathsf{Tail}(x)\mathsf{B}(x)$ 也无法在其中证明。事实上，这需要归纳法：

$$\begin{aligned} &\vdash_{\mathcal{POR}^\lambda} \epsilon = \epsilon\epsilon = \mathsf{Tail}(\epsilon)\mathsf{B}(\epsilon) \\ x = \mathsf{Tail}(x)\mathsf{B}(x) &\vdash_{\mathcal{POR}^\lambda} x0 = \mathsf{Tail}(x0)\mathsf{B}(x0) \\ x = \mathsf{Tail}(x)\mathsf{B}(x) &\vdash_{\mathcal{POR}^\lambda} x1 = \mathsf{Tail}(x1)\mathsf{B}(x1). \end{aligned}$$

由此，我们希望通过归纳法推出 $x =$Tail(x)B(x)。因此，我们引入 $\mathcal{IPOR}^\lambda$，其语言在 $\mathcal{POR}^\lambda$ 的基础上扩展而来，并包含 RS_2^1 的所有表达式（及其翻译）。特别地，$\mathcal{IPOR}^\lambda$ 的项的语法与定义 3.3 完全相同，而公式的语法则定义如下。

定义 3.7（ $\mathcal{IPOR}^\lambda$的公式）。 $\mathcal{IPOR}^\lambda$ 的公式定义如下：(i.) $\mathcal{POR}^\lambda$ 中所有形如 $\mathsf{t} = \mathsf{u}$ 的方程，都是 $\mathcal{IPOR}^\lambda$的公式；(ii.) 对于 $\mathcal{POR}^\lambda$中任意（可能是开放的）项，例如 t 和 u，$\mathsf{t} \subseteq \mathsf{u}$ 和 Flip(t) 都是 $\mathcal{IPOR}^\lambda$的公式；(iii.) $\mathcal{IPOR}^\lambda$ 的公式在 $\wedge$、$\vee$、$\to$、$\forall$、$\exists$ 下封闭。

记号 3.2。我们采用标准约定： $\bot :=0=1$ 和 $\neg F :=F\to\bot$。

Σ_0^b公式和 Σ_1^b公式的概念，对于 $\mathcal{IPOR}^\lambda$ 而言，正是定义 2.3 中为 RS_2^1, 引入的概念。

注记 3.2. RS_2^1 中的任意公式都可以视为 $\mathcal{IPOR}^\lambda$的公式，其中每个符号 0 都替换为 0，1 替换为 1，$\frown$ 替换为 $\circ$（通常省略），$\times$ 替换为 Times。在下文中，我们假定 RS_2^1 中的任意公式都是 $\mathcal{IPOR}^\lambda$的公式，除非涉及上述替换。

定义 3.8（理论 $\mathcal{IPOR}^\lambda$）。 $\mathcal{IPOR}^\lambda$ 的公理包括直觉主义一阶谓词演算的标准规则、等号符号的通常规则，以及以下公理：

1. $\mathcal{POR}^\lambda$的所有公理 2. $x\subseteq y\leftrightarrow \mathrm{Sub}(x,y)=1$3. $x=\epsilon\vee x=\mathrm{Tail}(x)$ $0\vee x=\mathrm{Tail}(x)1$ 4. $0=1\to x=\epsilon$5. $\mathrm{Cond}(x,y,z,w)=w'\leftrightarrow($ $x=\epsilon\wedge w'=y)\vee(x=\mathrm{Tail}(x)0\wedge w'=z)\vee(x=\mathrm{Tail}(x)1\wedge w'=w)$ 6. $\mathrm{Flip}(x)\leftrightarrow\mathrm{Flipcoin}(x)=1$7. 任何形如以下形式的公式，

$$\big(F(\epsilon)\wedge(\forall x)(F(x)\to F(x0))\wedge(\forall x)(F(x)\to F(x1))\big)\to(\forall y)F(y),$$

其中 F 的形式为 $(\exists z\preceq \mathrm{t})\mathrm{u}=\mathrm{v}$，且 t 只包含一阶自由变量。

记号 3.3（NP 谓词）。我们将形式为 $(\exists z\preceq \mathrm{t})\mathrm{u}=\mathrm{v}$ 且 t 只包含一阶自由变量的公式称为 NP 谓词。

将 $\mathcal{IPOR}^\lambda$ 与 $\mathcal{POR}^\lambda$ 及 IRS_2^1联系起来。现在 $\mathcal{IPOR}^\lambda$ 已经引入，我们将证明， $\mathcal{POR}^\lambda$ 以及 RS_2^1 的直觉主义版本中的定理都可以在其中导出。首先，检查 $\mathcal{POR}^\lambda$ 的所有规则即可轻松证明命题 3.6。

命题 3.6。 $\mathcal{POR}^\lambda$ 的任何定理都是 $\mathcal{IPOR}^\lambda$ 的定理。

接着，我们考察 IRS_2^1，并证明其中的每个定理都可在 $\mathcal{IPOR}^\lambda$ 中推导出来。为此，我们证明了若干关于 $\mathcal{IPOR}^\lambda$ 的性质。特别是，它的递归模式不同于 IRS_2^1 的递归模式，因为它处理的是形如 $(\exists y\preceq \mathrm{t})\mathrm{u}=\mathrm{v}$ 的公式，而非所有 Σ_1^b 公式。根据命题 3.7，这两个模式彼此相关；该命题通过对公式结构进行归纳法证明。[10]

[10]有关更多详情，请参阅附录 [?]。

命题 3.7. 对于 $\mathcal{RL}$ 中任意的 Σ_0^b-公式 $F(x_1, \ldots, x_n)$，都存在 $\mathcal{IPOR}^\lambda$ 的一个项 $\mathsf{t}_F(x_1, \ldots, x_n)$，使得：

1. $\vdash_{\mathcal{IPOR}^\lambda} F \leftrightarrow \mathsf{t}_F = 0$2.
   $\vdash_{\mathcal{IPOR}^\lambda} \mathsf{t}_F = 0 \vee \mathsf{t}_F = 1$.

由此我们得到以下推论，并得以证明定理 3.8，该定理联系了 $\mathcal{IPOR}^\lambda$ 与 IRS_2^1。

推论 3.2。i. 对任意 Σ_0^b-公式 F， $\vdash_{\mathcal{IPOR}^\lambda} F \vee \neg F$。

ii. 对于 $\mathcal{RL}$ F 和 $\eta \in$O 中任意闭合的Σ_0^b-公式，要么 $\mathrm{T}_\eta \vdash_{\mathcal{IPOR}^\lambda} F$，要么 $\mathrm{T}_\eta \vdash_{\mathcal{IPOR}^\lambda} \neg F$。

定理 3.8。IRS_2^1 的任何定理都是 $\mathcal{IPOR}^\lambda$的定理。

证明。首先注意到，根据命题 3.7，对于 $\mathcal{RL}$中的任意 Σ_1^b-公式 $F = (\exists x_1 \preceq t_1)$。...
...$(\exists x_n \preceq t_n)G$，

$$\vdash_{\mathcal{IPOR}^\lambda} F \leftrightarrow (\exists x_1 \preceq \mathsf{t}_1) \ldots (\exists x_n \preceq \mathsf{t}_n)\mathsf{t}_G = 0,$$

IRS_2^1 的任意 Σ_1^b-递归模式实例都可以从 NP 归纳模式在 $\mathcal{IPOR}^\lambda$ 中导出。因此，只需检查 IRS_2^1 的所有基本公理能否在 $\mathcal{IPOR}^\lambda$ 中得到证明。 □

这一结果还带来了以下显而易见的推论。

推论 3.3. 对任意闭合的 Σ_0^b-公式 F 和 $\eta \in$O，要么 $\mathrm{T}_\eta \vdash_{\mathcal{IPOR}^\lambda} F$，要么 $\mathrm{T}_\eta \vdash_{\mathcal{IPOR}^\lambda} \neg F$。

借助推论 3.3，我们甚至可以证明以下引理 3.9。

引理 3.9. 设 F 是 $\mathcal{RL}$ 和 $\eta \in$O 中的一个闭合 Σ_0^b-公式，则：

$$\mathrm{T}_\eta \vdash_{\mathcal{IPOR}^\lambda} F \quad \textit{iff} \quad \eta \in [\![F]\!].$$

证明. ($\Rightarrow$) 这一可靠性结果通过对 $\mathcal{IPOR}^\lambda$ 的规则结构进行归纳而得到。

($\Leftarrow$) 根据推论 3.3，我们知道 $\mathrm{T}_\eta \vdash_{\mathcal{IPOR}^\lambda} F$ 或 $\mathrm{T}_\eta \vdash_{\mathcal{IPOR}^\lambda} \neg F$。因此，如果 $\eta \in [\![F]\!]$，那么它不可能是 $\mathrm{T}_\eta \vdash_{\mathcal{IPOR}^\lambda} \neg F$ （根据可靠性）。所以，我们得出结论 $\mathrm{T}_\eta \vdash_{\mathcal{IPOR}^\lambda} F$。 □

3.2.3 可实现性

这里，我们将可实现性作为 $\mathcal{IPOR}^\lambda$ 的内部概念引入。由此可得一个推论：对于 IRS_2^1 （实际上是 $\mathcal{IPOR}^\lambda$ ）中关于形如 $(\forall x)(\exists y)F(x, y)$ 的公式的任意推导，都可以提取出一个 $\mathcal{POR}^\lambda$ f：$s \Rightarrow s$ 的函数项，使得 $\vdash_{\mathcal{IPOR}^\lambda} (\forall x)F(x, \mathrm{f}x)$。因此我们可以得出结论：如果一个函数 $f$is Σ_1^b-representable in IRS_2^1, then $f \in \mathcal{POR}$。

记号 3.4。令 $\mathbf{x}$、$\mathbf{y}$ 分别表示项变量的有限序列 x_1、...,x_n 和 y_1、...,y_k，并令 $\mathbf{x}(\mathbf{y})$ 表示 $y_1(\mathbf{x})\ldots,y_k(\mathbf{x})$ 的缩写。令 Λ 表示空序列，并令 $y(\Lambda) := y$。

定义 3.9。公式 $x \circledR F$ 按如下方式通过归纳法定义：

$$\begin{aligned}
\Lambda \circledR F &:= F \\
\mathbf{x},\mathbf{y} \circledR (G \wedge H) &:= (\mathbf{x} \circledR G) \wedge (\mathbf{y} \circledR H) \\
z,\mathbf{x},\mathbf{y} \circledR (G \vee H) &:= (z = 0 \wedge \mathbf{x} \circledR G) \vee (z \neq 0 \wedge \mathbf{y} \circledR H) \\
\mathbf{y} \circledR (G \to H) &:= (\forall \mathbf{x})(\mathbf{x} \circledR G \to \mathbf{y}(\mathbf{x}) \circledR H) \wedge (G \to H) \\
z,\mathbf{x} \circledR (\exists y)G &:= \mathbf{x} \circledR G\{z/y\} \\
\mathbf{x} \circledR (\forall y)G &:= (\forall y)(\mathbf{x}(y) \circledR G),
\end{aligned}$$

其中，$\mathbf{x}$ 中没有变量在 F 中自由出现。给定项 $\mathbf{t} = \mathbf{t}_1$、.....、$\mathbf{t}_n$，我们定义：

$$\mathbf{t} \circledR F := (\mathbf{x} \circledR F)\{\mathbf{t}/\mathbf{x}\}.$$

我们将这些新公式的可推导性与 $\mathcal{IPOR}^\lambda$ 的公式的可推导性联系起来。下面的证明分别对 $\mathcal{IPOR}^\lambda$-公式的结构以及推导的高度进行归纳。

定理 3.10（可靠性）。若 $\vdash_{\mathcal{IPOR}^\lambda} \mathbf{t} \circledR F$，则 $\vdash_{\mathcal{IPOR}^\lambda} F$。

记号 3.5。给定 $\Gamma = F_1$、.....、F_n，令 $\mathbf{x} \circledR \Gamma$ 表示 $\mathbf{x}_1 \circledR F_1$、.....、$\mathbf{x}_n \circledR F_n$。

定理 3.11（完备性）。若 $\vdash_{\mathcal{IPOR}^\lambda} F$，则存在项 $\mathbf{t}$，使得 $\vdash_{\mathcal{IPOR}^\lambda} \mathbf{t} \circledR F$。

证明概要。我们证明，如果 $\Gamma \vdash_{\mathcal{IPOR}^\lambda} F$，那么存在项 $\mathbf{t}$，使得 $\mathbf{x} \circledR \Gamma \vdash_{\mathcal{IPOR}^\lambda} \mathbf{t}\mathbf{x}_1 \ldots \mathbf{x}_n \circledR F$。证明通过对 $\Gamma \vdash_{\mathcal{IPOR}^\lambda} F$ 的推导进行归纳法来完成。我们仅以规则 $\vee R_1$ 为例：

$$\dfrac{\begin{array}{c}\vdots\\ \Gamma \vdash G\end{array}}{\Gamma \vdash G \vee H} \vee R_1$$

根据归纳假设，存在项 $\mathbf{u}$，使得 $\mathbf{t} \circledR \Gamma \vdash_{\mathcal{IPOR}^\lambda} \mathbf{tu} \circledR G$。由于 $x, y \circledR G \vee H$ 定义为 $(x = 0 \wedge y \circledR G) \vee (x \neq 0 \wedge y \circledR H)$，我们可以取 $\mathbf{t} = 0, \mathbf{u}$。 □

推论 3.4。设 $(\forall x)(\exists y)F(x,y)$ 是 $\mathcal{IPOR}^\lambda$ 的一个闭定理，其中 F 是一个 Σ_1^b-公式。那么，存在 $\mathcal{POR}^\lambda$ 的闭项 $\mathbf{t}$：$s \Rightarrow s$，使得：

$$\vdash_{\mathcal{IPOR}^\lambda} (\forall x)F(x, \mathbf{t}x).$$

证明。由定理 3.11，存在 $\mathbf{t} = \mathbf{t}\ w$ 使得 $\vdash_{\mathcal{IPOR}^\lambda} \mathbf{t} \circledR (\forall x)(\exists y)F(x,y)$。因此，根据定义 3.9，

$$\begin{aligned}
\mathbf{t} \circledR (\forall x)(\exists y)F(x,y) &\equiv (\forall x)(\mathbf{t}(x) \circledR (\exists y)F(x,y)) \\
&\equiv (\forall x)(w(x) \circledR F(x, \mathbf{t}x)).
\end{aligned}$$

由此，根据定理 3.10，我们可推出，

$$\vdash_{\mathcal{IPOR}^\lambda} (\forall x)F(x, \mathsf{t}x).$$

□

在 IRS 中可由 Σ_1^b 表示的函数 $\frac{1}{2}$ 属于 $\mathcal{POR}$。现在，我们已具备所有要素，可以证明：若一个函数按照定义 3.1 的意义可在 IRS 中由 Σ_1^b 表示，则它属于 $\mathcal{POR}$。

推论 3.5. 对任意函数 $f\colon \mathsf{O}\times\mathsf{S}\to\mathsf{S}$，若在 $\mathcal{RL}$ $F(x,y)$ 中存在一个闭 Σ_1^b-公式，使得：

1. $\mathbf{IRS}_2^1 \vdash (\forall x)(\exists! y)F(x,y)$
2. $[\![F(\overline{\overline{\sigma_1}}, \overline{\overline{\sigma_2}})]\!] = \{\eta \mid f(\sigma_1,\eta) = \sigma_2\}$,

则 $f \in \mathcal{POR}$。

证明. 由于 $\vdash_{\mathbf{IRS}_2^1} (\forall x)(\exists! y)F(x,y)$，由定理 3.8 $\vdash_{\mathcal{IPOR}^\lambda} (\forall x)(\exists! y)F(x,y)$可得。接着，由 $\vdash_{\mathcal{IPOR}^\lambda} (\forall x)(\exists y)F(x,y)$，根据推论 3.4，我们推得：对某个闭项 $\mathsf{g} \in \mathcal{POR}^\lambda$，有 $\vdash_{\mathcal{IPOR}^\lambda} (\forall x)F(x, \mathsf{g}x)$。此外，根据定理 3.5.2，存在一个 $g \in \mathcal{POR}$，使得对于任意 σ_1, $\sigma_2 \in \mathsf{S}$ 和 $\eta \in \mathsf{O}$，当 $T_\eta \vdash_{\mathcal{IPOR}^\lambda} \mathsf{g}\overline{\sigma_1} = \overline{\sigma_2}$ 时，$g(\sigma_1,\eta) = \sigma_2$。因此，根据命题 3.6，对于任意 $\sigma_1,\sigma_2 \in \mathsf{S}$ 和 $\eta \in \mathsf{O}$，若 $g(\sigma_1,\eta) = \sigma_2$，则 $T_\eta \vdash_{\mathcal{IPOR}^\lambda} \mathsf{g}\overline{\sigma_1} = \overline{\sigma_2}$，从而 $T_\eta \vdash_{\mathcal{IPOR}^\lambda} F(\overline{\sigma_1}, \overline{\sigma_2})$。根据引理 3.9，当 $\eta \in [\![F(\overline{\sigma_1}, \overline{\sigma_2})]\!]$ 时，$T_\eta \vdash_{\mathcal{IPOR}^\lambda} F(\overline{\sigma_1}, \overline{\sigma_2})$，也就是说 $f(\sigma_1,\eta) = \sigma_2$。但此时 $f = g$，所以由于 $g \in \mathcal{POR}$，$f \in \mathcal{POR}$ 也成立。 □

3.2.4 ∀NP-保守性：$\mathcal{IPOR}^\lambda$ + 排中律 对 $\mathcal{IPOR}^\lambda$

推论 3.5 已经非常接近我们所要寻找的结果。要完成证明，剩下的步骤是将其从直觉主义 IRS_2^1 扩展到经典 RS_2^1，，证明任何在 RS_2^1 中 Σ_1^b-可表示的函数也属于$\mathcal{POR}$。证明通过调整 [3]中的方法得到。我们首先考虑通过排中律对 $\mathcal{IPOR}^\lambda$ 进行扩展，并证明可实现性解释可以扩展到该扩展理论，从而对于其中的任意闭定理 $(\forall x)(\exists y \preceq \mathsf{t})F(x,y)$，由于其是 F一个 Σ_1^b-公式，存在一个闭项 t：$s \Rightarrow s$，使得 $\vdash_{\mathcal{IPOR}^\lambda} (\forall x)F(x, \mathsf{t}x)$。

从 $\mathcal{IPOR}^\lambda$ 到 $\mathcal{IPOR}^\lambda$ +（马尔可夫） 令排中律模式为 EM，$F \vee \neg F$，并将马尔可夫原理定义如下：

$$\neg\neg(\exists x)F \to (\exists x)F, \qquad (\mathbf{Markov})$$

其中 F 是一个 Σ_1^b-公式。

命题 3.12. 对任意 Σ_1^b 公式 F，若 $\vdash_{\mathcal{IPOR}^\lambda + \text{排中律}} F$，则 $\vdash_{\mathcal{IPOR}^\lambda + (\text{马尔可夫})} F$。

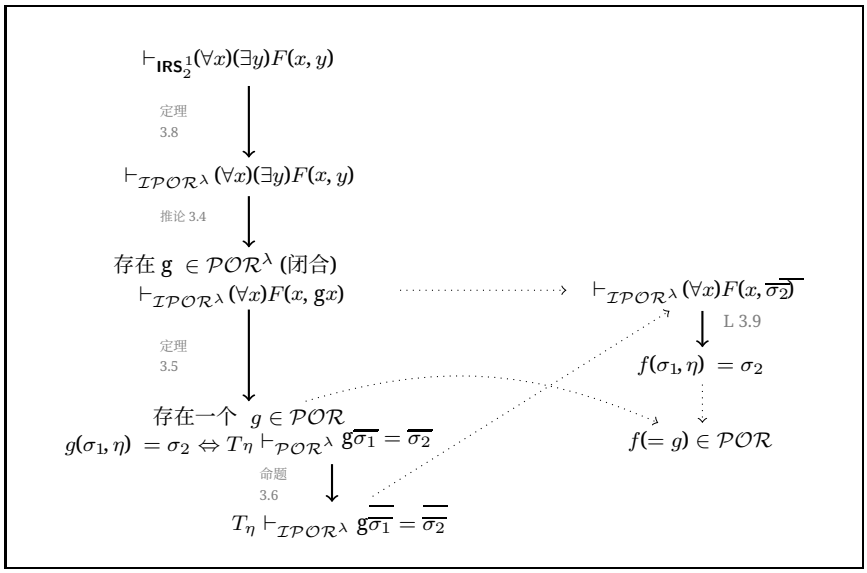


图 4：推论 3.5 的证明模式

证明概要. 该主张通过应用双重否定翻译得证，以下两点值得注意：(1) 对任意 Σ_0^b 公式 $F, \vdash_{\mathcal{IPOR}^\lambda} \neg\neg F \to F$；(2) 利用（马尔可夫），可以证明 NP 归纳的一个实例的双重否定等价于 NP归纳模式的一个实例。 □

最后，我们证明上述定义的可实现性解释可扩展至 $\mathcal{IPOR}^\lambda$ +(马尔可夫)，也就是说，对于 $\mathcal{IPOR}^\lambda$ +(马尔可夫) 中任意带有 F Σ_1^b-公式的闭定理（$\forall x(\exists y \preceq \mathsf{t})F(x,y)$），存在一个闭项 $\mathcal{POR}^\lambda \mathsf{t}$: $s \Rightarrow s$，使得 $\vdash_{\mathcal{IPOR}^\lambda}(\forall x)F(x,\mathsf{t}x)$。

从 $\mathcal{IPOR}^\lambda$ 到 $(\mathcal{IPOR}^\lambda)^*$。设给定一个主观编码 $\sharp$: $(s \Rightarrow s) \Rightarrow s$ ，将 $\mathcal{IPOR}^\lambda$ 中的一阶一元函数编码为字符串，并给定一个满足以下条件的“解码”函数 app : $s \Rightarrow s \Rightarrow s$ s:

$$\vdash_{\mathcal{IPOR}^\lambda} \mathsf{app}(\sharp\mathsf{f}, x) = \mathsf{f}x.$$

此外，令

$$x * y := \sharp(\lambda z.\mathsf{BAnd}(\mathsf{app}(x,z), \mathsf{app}(y,z)))$$

and

$$T(x) := (\exists y)(\mathsf{B}(\mathsf{app}(x,y)) = 0).$$

类型为 s 的项集合上存在一个交半格结构：当 $\vdash_{\mathcal{IPOR}^\lambda} T(\mathsf{u}) \to T(\mathsf{t})$ 时，$\mathsf{t} \sqsubseteq \mathsf{u}$；其顶元为 $\mathsf{1} := \sharp(\lambda x.1)$，交由 $x * y$ 给出。事实上，由 $T(x*1) \leftrightarrow T(\underline{x})$，可得 $x \sqsubseteq \underline{\mathbf{1}}$。此外，由 $\mathsf{B}(\mathsf{app}(x,\mathsf{u})) = 0$，我们得到 $\mathsf{B}(\mathsf{app}(x*y,\mathsf{u})) = \mathsf{BAnd}(\mathsf{app}(x,\mathsf{u}), \mathsf{app}(y,\mathsf{u})) = 0$,

由此可得 $T(x) \to T(x*y)$，即 $x*y \sqsubseteq x$。类似地，可以证明 $x*y \sqsubseteq y$。最后，由 $T(x) \to T(v)$ 和 $T(y) \to T(v)$，我们推得 $T(x*y) \to T(v)$；这是因为 $\vdash_{\mathcal{IPOR}^\lambda} T(x*y) \to T(y)$。请注意，公式 $T(x)$ 不是一个Σ_1^b公式，因为它的存在量词没有界定。

定义 3.10. 对于任意一个关于 $\mathcal{IPOR}^\lambda$ F 的公式，以及一个新变量 x，我们归纳地定义公式 $x \Vdash F$：

$$\begin{aligned} x \Vdash F &:= F \vee T(x) \quad (F \ atomic) \\ x \Vdash G \wedge H &:= x \Vdash G \wedge x \Vdash H \\ x \Vdash G \vee H &:= x \Vdash G \vee x \Vdash H \\ x \Vdash G \to H &:= (\forall y)(y \Vdash G \to x*y \Vdash H) \\ x \Vdash (\exists y)G &:= (\exists y)x \Vdash G \\ x \Vdash (\forall y)G &:= (\forall y)x \Vdash G. \end{aligned}$$

下面的引理 3.13 是通过对 $\mathcal{IPOR}^\lambda$ 中公式的结构进行归纳法证明的，与 [4] 中的情况相同。

引理 3.13. 如果 F 可在不使用 NP 归纳的情况下于 $\mathcal{IPOR}^\lambda$ 中证明，那么 $x \Vdash F$ 可在 $\mathcal{IPOR}^\lambda$ 中证明。

引理 3.14. 设 $F = (\exists x \preceq \mathsf{t})G$，其中 G 是一个 Σ_0^b-公式。那么，存在一个项 $\mathsf{u_F}: s$，满足 $FV(\mathsf{u_F}) = FV(G)$，使得：

$$\vdash_{\mathcal{IPOR}^\lambda} F \leftrightarrow T(\mathsf{u_F}).$$

证明. 由于 $G(x)$ 是一个 Σ_0^b-公式，对于所有项 $\mathsf{v}: s$，$\vdash_{\mathcal{IPOR}^\lambda} G(x) \leftrightarrow \mathsf{t}_{x \preceq \mathsf{t} \wedge G}(x) = 0$，其中 $\mathsf{t}_{x \preceq \mathsf{t} \wedge G}$ 的自由变量是 t 和 G。设 $H(x)$ 是一个 Σ_0^b- 公式，通过对其结构进行归纳法可证明，对于任意项 $\mathsf{v}: s$，$\mathsf{t}_{H(v)} = \mathsf{t}_H(\mathsf{v})$。于是，

$$\vdash_{\mathcal{IPOR}^\lambda} F \leftrightarrow (\exists x)\mathsf{t}_{x \preceq \mathsf{t} \wedge G}(x) = 0 \leftrightarrow (\exists x)T(\sharp(\lambda x.\mathsf{t}_{x \preceq \mathsf{t} \wedge G}(x))).$$

因此，我们令 $\mathsf{u_F} = \sharp(\lambda x.\mathsf{t}_{x \preceq \mathsf{t} \wedge G}(x))$. □

由此我们还可以推导出以下三个性质：

i. $\vdash_{\mathcal{IPOR}^\lambda} (x \Vdash F) \leftrightarrow (F \vee T(x))$
ii. $\vdash_{\mathcal{IPOR}^\lambda} (x \Vdash \neg F) \leftrightarrow (F \to T(x))$
iii. $\vdash_{\mathcal{IPOR}^\lambda} (x \Vdash \neg\neg F) \leftrightarrow (F \vee T(x))$,

其中 F 是一个 Σ_1^b-公式。

推论 3.6（马尔可夫原理）。如果 F 是一个 Σ_1^b-公式，那么

$$\vdash_{\mathcal{IPOR}^\lambda} x \Vdash \neg\neg F \to F.$$

为了定义 $\mathcal{IPOR}^\lambda$ 的扩展 $(\mathcal{IPOR}^\lambda)^*$，我们以形式化的方式引入 PIND。

定义 3.11（PIND）。令 PIND(F) 表示以下公式：

$$\big(F(\epsilon) \wedge \big((\forall x)(F(x) \to F(x0)) \wedge (\forall x)(F(x) \to F(x1))\big)\big) \to (\forall x)F(x).$$

注意，如果 $F(x)$ 是形如 $(\exists y \preceq \mathrm{t})\mathrm{u} = \mathrm{v}$ 的公式，那么 $z \Vdash \mathrm{PIND}(F)$ 的形式为 PIND($F(x) \vee T(z)$)，这不是 NP 归纳模式的一个实例（因为公式 $T(z) = (\exists x)\mathrm{B}(\mathrm{app}(z, x)) = 0$ 不是有界的）。

定义 3.12（理论 $(\mathcal{IPOR}^\lambda)^*$）。令 $(\mathcal{IPOR}^\lambda)^*$ 表示在 $\mathcal{IPOR}^\lambda$ 的基础上扩展得到的理论，其中包含归纳模式 PIND($F(x) \vee G$) 的所有实例；这里 $F(x)$ 的形式为 $(\exists y \preceq \mathrm{t})\mathrm{u} = \mathrm{v}$，而 G 是一个任意公式，且满足$x \notin FV(G)$。

于是我们推导出以下命题，它将 $\mathcal{IPOR}^\lambda$ 中的可导性与 $(\mathcal{IPOR}^\lambda)^*$ 中的可导性联系起来。

命题 3.15. 对任意 Σ_1^b-公式 F，若 $\vdash_{\mathcal{IPOR}^\lambda} F$，则$\vdash_{(\mathcal{IPOR}^\lambda)^*} x \Vdash F$。

最后，我们通过为 PIND($F(x) \vee G$) 构造一个实现项，将可实现性扩展到 $(\mathcal{IPOR}^\lambda)^*$。

引理 3.16. 设 $F(x) : (\exists y \preceq \mathrm{t})\mathrm{u} = 0$，且 G 是任意一个不含 x 自由出现的公式。那么，存在项 t，使得：

$$\vdash_{\mathcal{IPOR}^\lambda} \mathrm{t}\ \circledR\ PIND(F(x) \vee G).$$

因此，根据定理 3.10，对于任意 Σ_1^b-公式 F 和公式 G，若满足$x \notin FV(F)$,

$$\vdash_{\mathcal{IPOR}^\lambda} PIND(F(x) \vee G).$$

命题 3.17. 对任意 Σ_1^b-公式 F 和 G，若满足 $x \notin FV(F)$，则 $\vdash_{\mathcal{IPOR}^\lambda}$PIND($F(x) \vee G$)。

推论 3.7（∀NP 保守性：$\mathcal{IPOR}^\lambda$ +排中律相对于 $\mathcal{IPOR}^\lambda$）。设 F 是一个 Σ_1^b-公式，若$\vdash_{\mathcal{IPOR}^\lambda + \text{排中律}} (\forall x)(\exists y \preceq \mathrm{t})F(x, y)$，则 $\vdash_{\mathcal{IPOR}^\lambda} (\forall x)(\exists y \preceq \mathrm{t})F(x, y)$。

证明的结尾。我们总结证明，以确立命题 3.18。

命题 3.18. 设 $(\forall x)(\exists y \preceq \mathrm{t})F(x, y)$ 是 $\mathcal{IPOR}^\lambda$ + (马尔可夫) 的一个闭项，其中 F 是一个 Σ_1^b-公式。那么，存在一个 $\mathcal{POR}^\lambda\mathrm{t} : s \Rightarrow s$ 的闭项，使得：

$$\vdash_{\mathcal{IPOR}^\lambda} (\forall x)F(x, \mathrm{t}x).$$

证明。若$\vdash_{\mathcal{IPOR}^\lambda +}$(马尔可夫) $(\forall x)(\exists y)F(x, y)$，则由 Parikh命题 3.2，也有 $\vdash_{\mathcal{IPOR}^\lambda +}$(马尔可夫) $(\exists y \preceq \mathrm{t})F(x, y)$。此外，$\vdash_{(\mathcal{IPOR}^\lambda)_*} z \Vdash (\exists y \preceq \mathrm{t})F(x, y)$。接着，考虑 $G = (\exists y \preceq \mathrm{t})F(x, y)$。令 $\mathrm{v} = \mathrm{u}_G$，利用引理 3.14，我们推得 $\vdash_{(\mathcal{IPOR}^\lambda)_*} G$，因此由引理 3.13 和 3.16 可得，存在 t、u 使得 $\vdash_{\mathcal{IPOR}^\lambda} \mathrm{t}, \mathrm{u}\ \circledR\ G$，这意味着$\vdash_{\mathcal{IPOR}^\lambda} F(x, \mathrm{t}x)$，从而 $\vdash_{\mathcal{IPOR}^\lambda} (\forall x)(F(x), \mathrm{t}x)$。 □

因此，由命题 3.12，若 $\vdash_{\mathcal{IPOR}^\lambda + \text{排中律}} (\forall x)(\exists y \preceq \mathsf{t})F(x,y)$，且 $F\mathsf{a}$ 是 Σ_1^b-公式的闭项，则存在一个 $\mathcal{POR}\,\mathsf{t} : s \Rightarrow s$ 的闭项，使得 $\vdash_{\mathcal{IPOR}^\lambda} (\forall x)F(x, \mathsf{t}x)$。最后，按照上述论证，我们得出经典 RS_2^1 所需的推论 3.8。

推论 3.8. 设 $\mathrm{RS}_2^1 \vdash (\forall x)(\exists y \preceq t)F(x,y)$，其中 F 是一个仅以 x 和 y 为自由变量的 Σ_1^b-公式。对于任意函数 $f : \mathsf{S} \times \mathsf{O} \to \mathsf{S}$，若 $(\forall x)(\exists y \preceq t)F(x,y)$ 表示 f，使得：

1. $\mathbf{RS}_2^1 \vdash (\forall x)(\exists! y)F(x,y)$
2. $[\![F(\overline{\sigma_1}, \overline{\sigma_2})]\!] = \{\eta \mid f(\sigma_1, \eta) = \sigma_2\}$,

则 $f \in \mathcal{POR}$。

现在，将定理 3.3 和推论 3.8 结合起来，我们得出定理 3.1 成立，并且 RS_2^1 为 $\mathcal{POR}$ 中函数提供了一个算术刻画。

4 关联 $\mathcal{POR}$ 与多项式时间概率图灵机

定理 3.1 仍不足以刻画概率类，因为这些类是根据概率图灵机所计算的函数来定义的；而且，正如所观察到的，这些机器访问随机性的方式与预言机函数访问随机性的方式存在关键差异。因此，我们接下来的目标是通过精确关联这两个类来弥合这一差距。[11]

4.1 预备知识

我们首先定义（或重新定义）由多项式时间概率图灵机计算的函数类（定义在字符串上），以及由多项式时间流式机器计算的函数类，也就是带有额外预言机带的图灵机。

4.1.1 RFP 类

我们首先（重新）定义由多项式时间概率图灵机计算的函数类。[12]

定义 4.1（类 RFP）。令 $\mathsf{D(S)}$ 表示函数集合 $f : \mathsf{S} \to [0,1]$，满足 $\sum_{\sigma \in \mathbb{S}} f(\sigma) = 1$。类 RFP 由所有函数 $f : \mathsf{S}^k \to \mathsf{D(S)}$ 构成，且对于某个以多项式时间运行的 PTM $\mathscr{M}_{\mathscr{P}}$，以及每个 $\sigma_1, \ldots, \sigma_k, \tau \in \mathsf{S}$，$f(\sigma_1, \ldots, \sigma_k)(\tau)$ 都与 $\mathscr{M}_{\mathscr{P}}(\sigma_1 \sharp \ldots \sharp \sigma_k) \Downarrow \tau$ 的概率相一致。

[11] 实际上，这个证明特别复杂，因此为求简明，我们这里只给出其概要。不过，有兴趣的读者可以在 [?]，中找到更多细节，而完整证明则见于 [5]。[12] 显然，这与随机函数的标准定义 [11] 有很强的关联，例如第 ?? 节所述的定义。这里，伪分布和函数定义在字符串上，而非数字上。此外，我们现在考虑的是明确关联了（多项式时间）资源界限的机器。

因此——与 $\langle \mathscr{M}_{\mathscr{P}} \rangle$ 通过 [11, 9] 类似——该机器计算出的函数会为每个可能的输出关联一个概率，该概率对应于机器的一次运行实际产生该输出的真实概率；我们需要相应地调整 Σ_1^b-可表示性的概念。

定义 4.2. 若存在一个关于 $\mathcal{RL}$ $F(x_1, \ldots, x_k, y)$ 的 Σ_1^b-公式，使得：函数 $f : \mathrm{S}^k \to \mathrm{D(S)}$ 在 RS_2^1 中是 Σ_1^b-可表示的。

1. $\mathbf{RS}_2^1 \vdash (\forall \vec{x})(\exists! y) F(\vec{x}, y)$,
2. for all $\sigma_1, \ldots, \sigma_k, \tau \in \mathbb{S}$, $f(\sigma_1, \ldots, \sigma_k, \tau) = \mu(\llbracket F(\overline{\sigma_1}, \ldots, \overline{\sigma_k}, \tau) \rrbracket)$.

本章的核心结果可以重新表述如下：

定理 4.1. 对任意函数 $f : \mathrm{S}^k \to \mathrm{D(S)}$，当 $f \in$RFP 时，f 在 RS_2^1 中是 Σ_1^b-可表示的。

定理 4.1 的证明依赖于定理 3.1；下面的引理 4.2 将函数代数 $\mathcal{POR}$ 与类 RFP 联系起来。

引理 4.2. 对于 $\mathcal{POR}$ 中的任意函数 $f : \mathrm{S}^k \times \mathrm{O} \to \mathrm{S}$，存在一个属于 RFP 的函数 $g : \mathrm{S} \to \mathrm{D(S)}$，使得对所有 $\sigma_1, \ldots, \sigma_k, \tau \in \mathrm{S}$,

$$\mu(\{\omega \mid f(\sigma_1, \ldots, \sigma_k, \eta) = \tau\}) = g(\sigma_1, \ldots, \sigma_k, \tau)$$

反之亦然。

不过，引理 4.2 的证明较为繁复，因为它基于一系列语言模拟。

4.1.2 引入 SFP 类

联系 $\mathcal{POR}$ 与 RFP 的核心思路是引入一个称为 SFP 的中间类。该类由多项式时间流式图灵机（简称 STM）计算的函数组成，其中 STM 是一种确定性图灵机，带有一条额外的（只读）磁带，直观地说，这条磁带用于表示概率选择：开始时，从 $\mathrm{B}^{\mathbb{N}}$ 中抽取额外磁带的内容；随后，在每个计算步骤中，机器从这条磁带读取一个新比特，并始终向右移动。

定义 4.3（SFP 类）。SFP 类由函数 $f : \mathrm{S}^k \times \mathrm{B}^{\mathbb{N}} \to \mathrm{S}$ 构成，满足存在一台 STM $\mathscr{M}_{\mathcal{S}}$，使其在多项式时间内运行，并且对于任意$\sigma_1, \ldots, \sigma_k \in \mathrm{S}$ 和 $\omega \in \mathrm{B}^{\mathbb{N}}$，[13] $f(\sigma_1, \ldots, \sigma_k, \omega) = \tau$，当输入为 $\sigma_1 \sharp \ldots \sharp \sigma_k$且磁带为 ω时，机器 $\mathscr{M}_{\mathcal{S}}$输出 τ。

[13]稍微滥用一下记号，我们用 ω、ω'、ω''、.....作为 $\mathrm{B}^{\mathbb{N}}$ 中序列的元变量。事实上，正如第 ?? 节所述，集合 $\{0, 1\}$ 与 $\{\mathbb{0}, \mathbb{1}\}$ 基本上是等价的。

4.2 联系 RFP 和 SFP

STM 和概率图灵机的整体行为相似，但前者以显式方式访问随机性：机器不是在每一步都抛一次硬币，而是一次性采样一个比特流，然后在每一步读取一个新比特。因此，为了证明这两个模型等价，我们将借助以下命题 4.3。

命题 4.3（概率图灵机与 STM 的等价性）。对于任意多项式时间 STM $\mathscr{M}_{\mathcal{S}}$，存在一个多项式时间概率图灵机 $\mathscr{M}_{\mathcal{S}}{}^{*}$，使得对于所有字符串 $\sigma, \tau \in \mathsf{S}$,

$$\mu(\{\omega \mid \mathscr{M}_{\mathcal{S}}(\sigma, \omega) = \tau\}) = \Pr[\mathscr{M}_{\mathcal{S}}{}^{*}(\sigma) = \tau],$$

反之亦然。

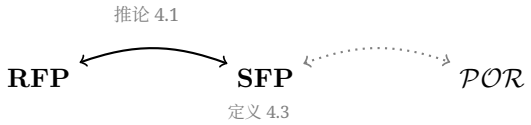
推论4.1（RFP 与 SFP 的等价性）。对于任意 $f : \mathsf{S}^k \to \mathsf{D(S)} \in \mathsf{RFP}$，存在一个 $g : \mathsf{S}^k \times \mathsf{B}^{\mathbb{N}} \to \mathsf{S} \in \mathsf{SFP}$，使得对于所有 $\sigma_1, \ldots, \sigma_k, \tau \in \mathsf{S}$,

$$f(\sigma_1, \ldots, \sigma_k, \tau) = \mu(\{\omega \mid g(\sigma_1, \ldots, \sigma_k, \omega) = \tau\}),$$

反之亦然。

4.3 联系 SFP 和 $\mathcal{POR}$

最后，我们需要证明 $\mathcal{POR}$ 与 SFP 等价：



从概率图灵机转向 STM，我们得到了一种以类似于 $\mathcal{POR}$中函数的方式访问随机性的机器模型：如前所述，在计算开始时会抽取一个预言机，然后通过查询该预言机来继续计算。不过，这两类机器处理随机性的方式仍存在重要差异。$\mathcal{POR}$ 中的函数访问的预言机是一个函数 $\eta \in \mathsf{B}^{\mathbb{S}}$，而 STM 的预言机则是一个比特流$\omega \in \mathsf{B}^{\mathbb{N}}$。换言之，$\mathcal{POR}$ 中的函数形式为 $f_{\mathcal{POR}} : \mathsf{S}^k \times \mathsf{O} \to \mathsf{S}$，而 SFP 中的函数形式为 $f_{\mathbf{SFP}} : \mathsf{S}^k \times \mathsf{B}^{\mathbb{N}} \to \mathsf{S}$。因此，我们无法直接比较二者，而是分两个主要步骤进行间接比较。

4.3.1 从 SFP 到 $\mathcal{POR}$

首先，我们证明，任何可由多项式时间 STM 计算的函数都属于 $\mathcal{POR}$。

命题 4.4（从 SFP 到 $\mathcal{POR}$）。对于任意 $f : \mathsf{S}^k \times \mathsf{B}^{\mathbb{N}} \to \mathsf{S} \in \mathsf{SFP}$，都存在函数 $f^{\star} : \mathsf{S}^k \times \mathsf{O} \to \mathsf{S} \in \mathcal{POR}$，使得对于所有 $\sigma_1, \ldots, \sigma_k, \tau \in \mathsf{S}$ 和 $\omega \in \mathsf{B}^{\mathbb{N}}$,

$$\mu(\{\omega \in \mathbb{B}^{\mathbb{N}} \mid f(\sigma_1, \ldots, \sigma_k, \omega) = \tau\}) = \mu(\{\eta \in \mathbb{O} \mid f^{\star}(\sigma_1, \ldots, \sigma_k, \eta) = \tau\}).$$

基本观察是，给定输入 $\sigma \in S$ 和额外磁带$\omega \in B^{\mathbb{N}}$，在多项式时间内运行的 STM 只能访问 ω 的有限部分，其长度可由某个多项式 $p(|\sigma|)$ 界定。利用这一事实，我们构造 $f^\star$ 如下：

1. 我们引入新的类 PTF，它由函数 $f : S^k \times S \to S$ 构成，这些函数由有限流图灵机（简称 FSTM）计算，其额外磁带是一个有限字符串。2. 我们定义函数 $h \in \mathrm{PTF}$，使得对于任意 $f : S \times B^{\mathbb{N}} \to S$，若其多项式界为 $p(x)$，

$$f(n, \omega) = h(x, \omega_{p(|x|)}).$$

3. 我们定义 $h' : S \times S \times O \to S$，使得，

$$h'(x, y, \eta) = h(x, y).$$

通过对 FSTM 进行编码，我们证明 $h' \in \mathcal{POR}$。此外，h' 可以在不使用查询函数的情况下定义，因为 h'的计算从不查看 η。

4. 最后，我们定义提取函数 $e : S \times O \to S \in \mathcal{POR}$，它模仿前缀提取器 $\omega_{p(|x|)}$，使其输出与所有可能的 ω的前缀具有相同的分布，尽管所处空间不同。[14]这是通过利用一个双射 $dyad: S \to N$ 得到的，该双射确保对于每个 $\omega \in B^{\mathbb{N}}$，都存在一个 $\eta \in B^S$，使得 ω 的任意前缀都是某个 y对应的 $e(y, \eta)$ 的输出。由于 $\mathcal{POR}$ 在复合下封闭，我们最终定义

$$f^\star(x, \eta) := h'(x, e(x, \eta), \eta).$$

4.3.2 从 $\mathcal{POR}$到 SFP

为了通过 STM 模拟 $\mathcal{POR}$ 的函数，我们注意到，这两种模型调用的预言机形态不同，而且前者操纵此类预言机的方式也更加灵活：

- STM 在生成每一步之前都会查询预言机。相比之下，$\mathcal{POR}$ 的函数可以在计算过程中自由调用查询函数 $Q(x, \eta)$。我们将这种访问策略称为按需访问。

- STM 在计算的每一步都会查询预言机的一个新比特，且无法访问先前观察到的比特。我们将这种访问策略称为线性访问。相比之下，$\mathcal{POR}$ 的函数可以根据需要多次查询相同的比特。

因此，即使对于像 $Q(x, \eta)$ 这样的基本函数，要通过 STM 直接模拟 $\mathcal{POR}$ 也颇具挑战。因此，我们再次采取间接路径：经过一系列模拟，分别处理这些差异。

[14]回想一下，$\eta \in B^{\mathbb{N}}$，而 e 的第二个参数属于 O。

1. 首先，我们将 $\mathcal{POR}$ 翻译成一种命令式语言 $\mathrm{SIFP}_{\mathrm{RA}}$ ，该语言的设计受到 Winskel 的 IMP [12], 启发，且具有与 $\mathcal{POR}$相同的访问策略。$\mathrm{SIFP}_{\mathrm{RA}}$ 包含赋值、while 结构，以及命令 Flip(e)；该命令先将 e 求值为字符串 σ ，然后将值 $\eta(\sigma)$存储到寄存器中。通过对函数代数进行归纳法，可以轻松得到 $\mathrm{SIFP}_{\mathrm{RA}}$ 中预言机函数的编码。

2. 接着，我们将 $\mathrm{SIFP}_{\mathrm{RA}}$ 转换为另一种命令式语言，称为 $\mathrm{SIFP}_{\mathrm{LA}}$，它采用线性访问策略。$\mathrm{SIFP}_{\mathrm{LA}}$ 的定义与 $\mathrm{SIFP}_{\mathrm{RA}}$相同，唯一区别是将 Flip($e$) 替换为新命令 RandBit()，该命令生成一个随机比特并将其存入寄存器。从 $\mathrm{SIFP}_{\mathrm{RA}}$ 到 $\mathrm{SIFP}_{\mathrm{LA}}$ 的弱模拟通过逐步构建一张关联表来定义，其中包含以往观测的（字符串，比特）形式的配对。每次调用 Flip(e) 时，模拟都会检查是否已观测到配对 (e, b)。若没有，则通过生成一个新配对 (e, RandBit()) 来扩充该表。这是整个模拟中复杂得多的一步。

3. 语言 $\mathrm{SIFP}_{\mathrm{LA}}$ 可以翻译为 STM。注意，$\mathrm{SIFP}_{\mathrm{LA}}$ 的访问策略仍然是按需的：执行指令前，RandBit() 可以被调用，也可以不被调用。因此，我们首先考虑将 $\mathrm{SIFP}_{\mathrm{LA}}$ 翻译为一种支持按需访问策略的 STM 变体——也就是说，在一个计算步骤中，可以访问额外磁带上的一位，也可以不访问。然后，将所得程序编码为常规 STM。注意，我们不能指望模拟按需机器 $\mathscr{M}_{\mathcal{S}}{}^{\dagger}$ 的机器 $\mathscr{M}_{\mathcal{S}}$ 产生相同的输出和预言机。相反，与许多其他情况一样，我们证明可以定义 $\mathscr{M}_{\mathcal{S}}{}^{\dagger}$，使得对于任意 $\sigma, \tau \in \mathrm{S}$，集合 $\{\omega \mid \mathscr{M}_{\mathcal{S}}{}^{\dagger}(\sigma, \omega) = \tau\}$ 和 $\{\omega \mid \mathscr{M}_{\mathcal{S}}(\sigma, \omega) = \tau\}$ 具有相同的测度。

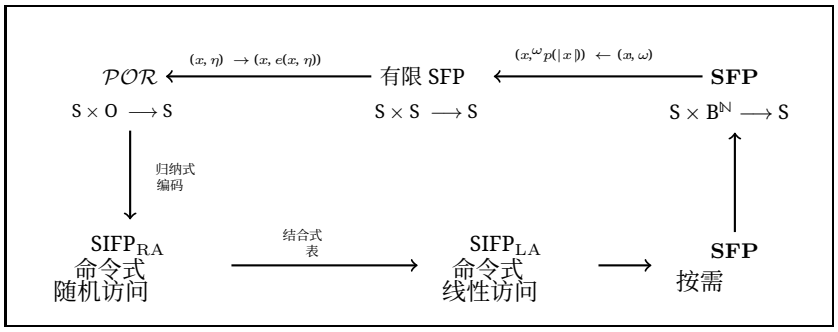


图 5： $\mathcal{POR}$ 与 SFP 4.1 之间的等价性

4.3.3 证明的收尾。

这些要素足以按照图 4.3.3 所示完成证明，并建立多项式时间随机函数与 RS_2^1 的 Σ_1^b-公式之间的联系。

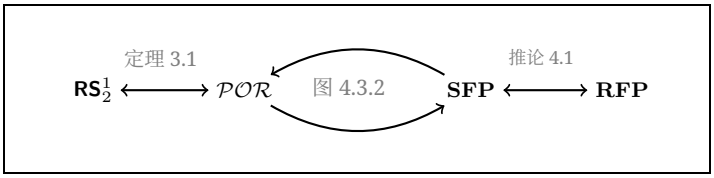


图 6：定理 4.1 的证明概要

参考文献

[1] S.R. Buss.《有界算术》。博士论文，普林斯顿大学，1986年。[2] S.R. Buss.《算术的一阶证明论》。载于 Elsavier 编《证明论手册》。Buss, S.R.，1998年。[3] S. Cook 和 A. Urquhart.《可行构造算术的函数解释》。《纯粹与应用逻辑年刊》，63:103–200，1993年。[4] T. Coquand 和 M. Hofmann.《确立经典系统相对于其直觉主义版本的保守性的新方法》。《计算机科学中的数学结构》，9(4):323–333，1999年。[5] D. Davoli.《有界算术与随机化计算》。硕士论文，http://amslaurea.unibo.it/26234/，2022年。[6] F. Ferreira.《多项式时间可计算算术及其保守扩张》。博士论文，1988年12月。[7] F. Ferreira.《多项式时间可计算算术》。载于 W. Sieg 编《逻辑与计算》，《当代数学》第106卷，第137–156页。AMS，1990年。[8] G. Ferreira 和 I. Oitavem.《对 S_2^1 在 Σ_1^b-NIA中的一种解释》。《Portugaliae Mathematica》，63:427–450，2006年。[9] J.T. Gill.《概率图灵机的计算复杂性》。《J. Comput.》，6(4):675–695，1977年。[10] R.J. Parikh.《语言生成装置》。《Quart. Prog. Rep.》，60:199–212，1961年。[11] E.S. Santos.《概率图灵机与可计算性》。《美国数学会会刊》，22(3):704–710，1969年。

[12] G. Winskel。《程序设计语言的形式语义》。麻省理工学院出版社，1993。

A 第 3 节中的证明

A.1 关于定理 3.3 的更多细节

定理 3.3 的证明。通过对 $f \in \mathcal{POR}$ 的结构进行归纳法来证明。基例。若 f 是一个基本函数，则有五种可能的子情况：

- $f = E$ 在 RS$_{12}$ 中由公式 $F_E(x,y)$：$x = x \wedge y = \epsilon$ 表示为 Σ_1^b。存在条件推导如下：

$$\dfrac{\dfrac{\dfrac{\dfrac{}{z = z \vdash (\exists y)(z = z \wedge y = \epsilon), z = z}\,Ax}{\vdash (\exists y)(z = z \wedge y = \epsilon), z = z}\,Ref \quad \dfrac{\dfrac{}{\epsilon = \epsilon \vdash (\exists y)(z = z \wedge y = \epsilon), \epsilon = \epsilon}\,Ax}{\vdash (\exists y)(z = z \wedge y = \epsilon), \epsilon = \epsilon}\,Ref}{\vdash (\exists y)(z = z \wedge y = \epsilon), z = z \wedge \epsilon = \epsilon}\,\wedge R}{(\exists y)(z = z \wedge y = \epsilon)}\,\exists R}{\vdash (\forall x)(\exists y)(x = x \wedge y = \epsilon)}\,\forall R$$

唯一性条件推导如下：

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{x_2 = x_3, x_1 = x_1, x_2 = \epsilon, x_3 = \epsilon \vdash x_2 = x_3}\,Ax}{x_1 = x_1, x_2 = \epsilon, x_1 = x_1, x_3 = \epsilon \vdash x_2 = x_3}\,Repl}{x_1 = x_1 \wedge x_2 = \epsilon, x_1 = x_1 \wedge x_2 = \epsilon \vdash x_2 = x_3}\,\wedge Ls}{(x_1 = x_1 \wedge x_2 = \epsilon) \wedge (x_1 = x_1 \wedge x_2 = \epsilon) \vdash x_2 = x_3}\,\wedge L}{\vdash (x_1 = x_1 \wedge x_2 = \epsilon) \wedge (x_1 = x_1 \wedge x_2 = \epsilon) \rightarrow x_2 = x_3}\,\rightarrow R}{\vdash (\forall x)(\forall y)(\forall z)((x = x \wedge y = \epsilon) \wedge (x = x \wedge z = \epsilon) \rightarrow y = z)}\,\forall Rs$$

通过证明对于所有 $n, m \in \mathsf{S}$ 和 $\eta^* \in \mathsf{O}$，当 $\eta \in [\![\overline{\sigma_1} = \overline{\sigma_1} \wedge \overline{\sigma_2} = \epsilon]\!]$ 时，$E(\sigma_1, \eta^*) = \sigma_2$，即可证明语义条件。

$\Rightarrow$ 假设 $\sigma_2 = \boldsymbol{\epsilon}$。因此，

$$\begin{aligned}
[\![\overline{\sigma_1} = \overline{\sigma_1} \wedge \overline{\sigma_2} = \epsilon]\!] &= [\![\overline{\sigma_1} = \overline{\sigma_1} \wedge \overline{\boldsymbol{\epsilon}} = \epsilon]\!] \\
&= [\![\overline{\sigma_1} = \overline{\sigma_1} \wedge \epsilon = \epsilon]\!] \\
&= [\![\overline{\sigma_1} = \overline{\sigma_1}]\!] \cap [\![\epsilon = \epsilon]\!] \\
&= \mathbb{O} \cap \mathbb{O} \\
&= \mathbb{O}.
\end{aligned}$$

显然，对于任意 η^*，$\eta^* \in \mathsf{O}$，即 $\eta^* \in [\![\overline{\sigma_1} = \overline{\sigma_1} \wedge \overline{m} = \epsilon]\!]$。

$\Leftarrow$ 假设（通过逆否命题）$m \neq \boldsymbol{\epsilon}$。因此，

$$\begin{aligned}
[\![\overline{\sigma_1} = \overline{\sigma_1} \wedge \overline{\sigma_2} = \epsilon]\!] &= [\![\overline{\sigma_1} = \overline{\sigma_1}]\!] \cap [\![\overline{\sigma_2} = \epsilon]\!] \\
&= \mathbb{O} \cap \emptyset \\
&= \emptyset.
\end{aligned}$$

显然，对于任意 η^*、$\eta^* \notin \emptyset$，因此 $\eta^* \notin [\![\overline{\sigma_1} = \overline{\sigma_1} \wedge \overline{\sigma_2} = \emptyset]\!]$。

• $f = P_i^n$，对于 $1 \le i \le n \in \mathbf{N}$。函数 si 在 RS12 中由公式表示为：$\bigwedge_{j\in J}($ $x_j = x_j) \wedge y = x_i$，其中 $J = \{1, \ldots, n\} \setminus i$。证明与上面的证明类似。

• $f = S_b$。该函数由公式在 RS12 中表示为 Σ_1^b: $y = x\mathbf{b}$，其中 $\mathbf{b} \in \{0, 1\}$，且当 $b = 0$ 时 $\mathbf{b} = 0$，当 $b = 1$ 时 $\mathbf{b} = 1$。存在条件推导如下:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{z\mathbf{b} = z\mathbf{b} \vdash (\exists y)(y = z\mathbf{b}), z\mathbf{b} = z\mathbf{b}}\,Ax}{\vdash (\exists y)(y = z\mathbf{b}), z\mathbf{b} = z\mathbf{b}}\,Ref}{\vdash (\exists y)(y = z\mathbf{b})}\,\exists R}{\vdash (\forall x)(\exists y)(y = x\mathbf{b})}\,\forall R$$

唯一性推导如下:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{x_2 = x_3, x_2 = x_1\mathbf{b}, x_3 = x_1\mathbf{b} \vdash x_2 = x_3}\,Ax}{x_2 = x_1\mathbf{b}, x_3 = x_1\mathbf{b} \vdash x_2 = x_3}\,Repl}{x_2 = x_1\mathbf{b} \wedge x_3 = x_1\mathbf{b} \vdash x_2 = x_3}\,\wedge L}{\vdash (x_2 = x_1\mathbf{b}) \wedge (x_3 = x_1\mathbf{b}) \to x_2 = x_3}\,\to R}{\vdash (\forall x)(\forall y)(\forall z)((y = x\mathbf{b}) \wedge (z = x\mathbf{b}) \to y = z)}\,\forall R\mathrm{s}$$

语义条件的证明如下：对于所有 σ_1、$\sigma_2 \in \mathbf{S}$ 和 $\eta^* \in \mathbf{O}$，当 $\eta^* \in [\![\overline{\sigma_2} = \overline{\sigma_1}\,\mathbf{b}]\!]$ 时，$S_b(\sigma_1, \eta^*) = \sigma_2$。

$\Rightarrow$ 假设 $b = 0$。因此，$\sigma_2 = \sigma_1\mathbb{0}$（且 $\mathbf{b} = 0$）。于是，

$$\begin{aligned}[\![\overline{\sigma_2} = \overline{\sigma_1}0]\!] &= [\![\overline{\sigma_1\mathbb{0}} = \overline{n}0]\!] \\ &= [\![\overline{n}0 = \overline{n}0]\!] \\ &= \mathbb{O}.\end{aligned}$$

对于任意 η^*、$\eta^* \in \mathbf{O}$，即 $\eta^* \in [\![\overline{\sigma_2} = \overline{\sigma_1}0]\!]$。同理，若 $b = 1$ 且 $\sigma_2 = \sigma_1\mathbb{1}$（且 $\mathbf{b} = 1$），则，

$$\begin{aligned}[\![\overline{\sigma_2} = \overline{\sigma_1}1]\!] &= [\![\overline{n\mathbb{1}} = \overline{n}1]\!] \\ &= [\![\overline{n}1 = \overline{n}1]\!] \\ &= \mathbb{O}.\end{aligned}$$

$\Leftarrow$ 假设（根据逆否命题）$b = 0$ 且 $\sigma_2 \neq \sigma_1\mathbb{0}$（且 $\mathbf{b} = 1$）。那么，显然 $[\![\overline{\sigma_2} = \overline{\sigma_1}1]\!] = \emptyset$。因此，对于任意 $\eta^* \in \mathbf{O}$，$\eta^* \notin \emptyset$。$b = 0$ 且 $m \neq n1$（且 $\mathbf{b} = 0$）的情况等价。

• $f = C$。该函数在 RS12 中可由公式 $F_C(x, v, z_0, z_1, y) : (x = \epsilon \wedge y = v) \vee (\exists x' \preceq x)($ $x = x'0 \wedge y = z_0) \vee (\exists x' \preceq x)(x = x'\mathbb{1} \wedge y = z_1)$ 表示。

• $f = Q$。该函数在 RS12 中由 F_Q 表示为 Σ_1^b: $(\mathrm{Flip}(x) \wedge y = 1) \vee (\neg\mathrm{Flip}(x)$ $\wedge y = 0)$。存在条件证明如下:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\texttt{Flip}(x)\vdash(\exists y)F_Q(z,y),\texttt{Flip}(z)}Ax}{\vdash(\exists y)F_Q(z,y),\texttt{Flip}(z),\neg\texttt{Flip}(z)}\neg R \quad \mathcal{D}_{\exists Q} \quad \vdash(\exists y)F_Q(z,y),\texttt{Flip}(z),1=0}{\vdash(\exists y)F_Q(z,y),\texttt{Flip}(z),\neg\texttt{Flip}(z)\wedge 1=0}\wedge R \quad \dfrac{\dfrac{}{1=1\vdash\ldots,1=1}Ax}{\vdash\ldots,1=1}Ref}{\vdash(\exists y)F_Q(z,y),(\texttt{Flip}(z)\wedge 1=1),(\neg\texttt{Flip}(z)\wedge 1=0)}\wedge R}{\vdash(\exists y)F_Q(z,y),(\texttt{Flip}(z)\wedge 1=1)\vee(\neg\texttt{Flip}(z)\wedge 1=0)}\vee R}{\vdash(\exists y)((\texttt{Flip}(z)\wedge y=1)\vee(\neg\texttt{Flip}(z)\wedge y=0))}\exists R}{\vdash(\forall x)(\exists y)((\texttt{Flip}(x)\wedge y=1)\vee(\neg\texttt{Flip}(x)\wedge y=0))}\forall R$$

其中

$$\mathcal{D}_{\exists Q}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\texttt{Flip}(z)\vdash\ldots.,\texttt{Flip}(z)}Ax}{\vdash\ldots\texttt{Flip}(z),\neg\texttt{Flip}(z)}\neg R \quad \dfrac{\dfrac{}{0=0\vdash\ldots,\texttt{Flip}(z),0=0}Ax}{\vdash\ldots,\texttt{Flip}(z),0=0}Ref}{\vdash\ldots,\texttt{Flip}(z),\texttt{Flip}(z)\wedge 0=1,\neg\texttt{Flip}(z)\wedge 0=0}\wedge R}{\vdash(\exists y)F_Q(z,y),1=0,\texttt{Flip}(z),F_Q(z,0)}\vee R}{\vdash(\exists y)F_Q(z,y),\texttt{Flip}(z),1=0}\exists R$$

唯一性如下所示:

$$\dfrac{\dfrac{\mathcal{D}_{\forall Q1} \qquad \mathcal{D}_{\forall Q2}}{\texttt{Flip}(x_1)\wedge x_2=1,F_Q(x_1,x_2)\vdash x_2=x_3 \qquad \neg\texttt{Flip}(x_1)\wedge=0,F_Q(x_1,x_3)\vdash x_2=x_3}\vee L}{\dfrac{\dfrac{\dfrac{F_Q(x_1,x_2),F_Q(x_1,x_3)\vdash x_2=x_3}{F_Q(x_1,x_2)\wedge F_Q(x_1,x_3)\vdash x_2=x_3}\wedge L}{\vdash F_Q(x_1,x_2)\wedge F_Q(x_1,x_3)\to x_2=x_3}\to R}{\vdash(\forall x)(\forall y)(\forall z)(F_Q(x,y)\wedge F_Q(x,z)\to y=z)}\forall Rs$$

其中

$$\mathcal{D}_{\forall Q1}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{x_2=x_3,\texttt{Flip}(x_1)\ x_2=1,x_3=1\vdash x_2=x_3}Ax}{\texttt{Flip}(x_1)\ x_2=1,\texttt{Flip}(x_1)\ x_3=1\vdash x_2=x_3}Repl}{\texttt{Flip}(x_1)\ x_2=1,\texttt{Flip}(x_1)\wedge x_3=1\vdash x_2=x_3}\wedge L \quad \dfrac{\dfrac{\dfrac{}{\texttt{Flip}(x_1)\ x_2=1,x_3=0\vdash x_2=x_3,\texttt{Flip}(x_1)}Ax}{\texttt{Flip}(x_1)\ x_2=1,\neg\texttt{Flip}(x_1)\ x_3=0\vdash x_2=x_3}\neg L}{\texttt{Flip}(x_1)\ x_2=1,\neg\texttt{Flip}(x_1)\wedge x_3=0\vdash x_2=x_3}\wedge L}{\texttt{Flip}(x_1)\ x_2=1,F_Q(x_1,x-3)\vdash x_2=x_3}\vee L}{\texttt{Flip}(x_1)\wedge x_2=1,F_Q(x_1,x3)\vdash x_2=x_3}\wedge L$$

$$\mathcal{D}_{\forall Q2}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\texttt{Flip}(x_1)\ x_3=1,y=0\vdash x_2=x_3,\texttt{Flip}(x_1)}Ax}{\neg\texttt{Flip}(x_1)\ y=0,\texttt{Flip}(x_1)\ x_3=1\vdash x_2=x_3}\neg L}{\neg\texttt{Flip}(x_1)\ y=0,\texttt{Flip}(x_1)\wedge x_3=1\vdash x_2=x_3}\wedge L \quad \dfrac{\dfrac{\dfrac{}{x_2=x_3,\neg\texttt{Flip}(x_1)\ x_2=0,x_3=0\vdash x_2=x_3}Ax}{\neg\texttt{Flip}(x_1)\ x_2=0,\neg\texttt{Flip}(x_1)\ x_3=0\vdash x_2=x_3}Repl}{\neg\texttt{Flip}(x_1)\ x_2=0,\neg\texttt{Flip}(x_1)\wedge x_3=0\vdash x_2=x_3}\wedge L}{\neg\texttt{Flip}(x_1)\ y=0,F_Q(x_1,x3)\vdash x_2=x_3}\vee L}{\neg\texttt{Flip}(x_1)\wedge y=0,F_Q(x_1,x3)\vdash x_2=x_3}\wedge L$$

语义条件的证明基于以下事实：对于所有 σ_1,σ_2 和 $\eta^*\in \mathbf{O}$,$Q(\sigma_1,\eta^*)=\sigma_2$ 当 $\eta^*\in[\![(\mathsf{Flip}(\overline{\sigma_1})\wedge\overline{\sigma_2}=1)\vee(\neg\mathsf{Flip}(\overline{\sigma_1}\wedge\overline{\sigma_2}=0)]\!]$。

$\Rightarrow$ 假设 $Q(\sigma_1, \eta^*) = \sigma_2$ 且 $\sigma_2 = \mathbb{1}$，也就是说 $\eta^*(\sigma_1) = \mathbb{1}$。因此，

$$\begin{aligned}
[\![F_Q(\overline{\sigma_1}, \overline{\sigma_2})]\!] &= [\![(\texttt{Flip}(\overline{\sigma_1}) \wedge \overline{\mathbb{1}} = \texttt{1}) \vee (\neg\texttt{Flip}(\overline{\sigma_1}) \wedge \overline{\mathbb{1}} = \mathbb{0})]\!] \\
&= [\![(\texttt{Flip}(\overline{\sigma_1}) \wedge \texttt{1} = \texttt{1}) \vee (\neg\texttt{Flip}(\overline{\sigma_1}) \wedge \texttt{1} = \texttt{0})]\!] \\
&= [\![\texttt{Flip}(\overline{\sigma_1}) \wedge \texttt{1} = \texttt{1}]\!] \cup [\![\neg\texttt{Flip}(\overline{\sigma_1}) \wedge \texttt{1} = \texttt{0}]\!] \\
&= \big([\![\texttt{Flip}(\overline{\sigma_1})]\!] \cap [\![\texttt{1} = \texttt{1}]\!]\big) \cup \big([\![\neg\texttt{Flip}(\overline{\sigma_1})]\!] \cap [\![\texttt{1} = \texttt{0}]\!]\big) \\
&= \big([\![\texttt{Flip}(\overline{\sigma_1})]\!] \cap \mathbb{0}\big) \cup \big([\![\neg\texttt{Flip}(\overline{\sigma_1})]\!] \cap \emptyset\big) \\
&= [\![\texttt{Flip}(\overline{\sigma_1})]\!] \cup \emptyset \\
&= [\![\texttt{Flip}(\overline{\sigma_1})]\!] \\
&= \{\eta \mid \eta(\sigma_1) = \mathbb{1}\}.
\end{aligned}$$

如 $\eta^*(\sigma_1) = \mathbb{1}$所示，因此 $\eta^* \in \{\eta \mid \eta(n) = \mathbb{1}\} = [\![(\text{Flip}(\overline{\sigma_1}) \wedge \overline{\mathbb{1}} = \texttt{1}) \vee (\neg\text{Flip}(\overline{\sigma_1}) \wedge \overline{\mathbb{1}} = \texttt{0})]\!]$。

假设 $Q(\sigma_1, \eta^*) = \sigma_2$ 且 $\sigma_2 = \mathbb{0}$，也就是说 $\eta^*(\sigma_1) = \mathbb{0}$。因此，

$$\begin{aligned}
[\![F_Q(\overline{\sigma_1}, \overline{\sigma_2})]\!] &= [\![(\texttt{Flip}(\overline{\sigma_1}) \wedge \overline{\mathbb{1}} = \texttt{1}) \vee (\neg\texttt{Flip}(\overline{\sigma_1}) \wedge \overline{\mathbb{1}} = \texttt{0})]\!] \\
&= [\![(\texttt{Flip}(\overline{\sigma_1}) \wedge \texttt{0} = \texttt{1}) \vee (\neg\texttt{Flip}(\overline{\sigma_1}) \wedge \texttt{0} = \texttt{0})]\!] \\
&= [\![\texttt{Flip}(\overline{\sigma_1}) \wedge \texttt{0} = \texttt{1}]\!] \cup [\![\neg\texttt{Flip}(\overline{\sigma_1}) \wedge \texttt{0} = \texttt{0}]\!] \\
&= \big([\![\texttt{Flip}(\overline{\sigma_1})]\!] \cap [\![\texttt{0} = \texttt{1}]\!]\big) \cup \big([\![\neg\texttt{Flip}(\overline{\sigma_1})]\!] \cap [\![\texttt{0} = \texttt{0}]\!]\big) \\
&= ([\![\texttt{Flip}(\overline{\sigma_1})]\!] \cap \emptyset) \cup ([\![\neg\texttt{Flip}(\overline{\sigma_1})]\!] \cap \mathbb{0}) \\
&= \emptyset \cup [\![\neg\texttt{Flip}(\overline{\sigma_1})]\!] \\
&= [\![\neg\texttt{Flip}(\overline{\sigma_1})]\!] \\
&= \mathbb{0} - [\![\texttt{Flip}(\overline{\sigma_1})]\!] \\
&= \{\eta \mid \eta(n) = \mathbb{0}\}.
\end{aligned}$$

如图所示，$\eta^*(n) = zero$，因此显然 $\eta^* \in \{\eta \mid \eta(n) = \mathbb{0}\} = [\![(\text{Flip}(\overline{\sigma_1}) \wedge \overline{\mathbb{0}} = \texttt{1}) \vee (\neg\text{Flip}(\overline{\sigma_1}) \wedge \overline{\mathbb{0}} = \texttt{0})]\!]$。

$\Leftarrow$ 假设（根据逆否命题）$\eta^*(\sigma_1) = \mathbb{1}$，因此 $Q(\sigma_1, \eta^*) = \mathbb{1}$ 且 $m = \mathbb{0}$。如上所示，在这种情况下，$[\![(\text{Flip}(\overline{\sigma_1}) \wedge \overline{\mathbb{0}} = \texttt{1}) \vee (\neg\text{Flip}(\overline{\sigma_1}) \wedge \overline{\mathbb{0}} = \texttt{0})]\!] = \{\eta \mid \eta(\sigma_1) = \mathbb{0}\}$。作为假设，$\eta^*$ 满足 $\eta^*(\sigma_1) = \mathbb{1}$，因此$\eta^* \notin \{\eta \mid \eta(\sigma_1) = \mathbb{0}\}$，也就是说 $\eta^* \notin [\![(\text{Flip}(\overline{\sigma_1} \wedge \overline{\mathbb{0}} = \texttt{1}) \vee (\neg\text{Flip}(\overline{\sigma_1}) \wedge \overline{\mathbb{0}} = \texttt{0})]\!]$。假设（根据逆否命题）$\eta^*(\sigma_1) = \mathbb{0}$，因此 $Q(\sigma_1, \eta^*) = \mathbb{0}$ 且 $m = \mathbb{1}$。如上所示，在 $[\![(\text{Flip}(\overline{\sigma_1}) \wedge \overline{\mathbb{1}} = \texttt{1}) \vee (\neg\text{Flip}(\overline{\sigma_1}) \wedge \overline{\mathbb{1}} = \texttt{0})]\!] = \{\eta \mid \eta(\sigma_1) = \mathbb{1}\}$ 的情况下，作为假设，η^* 满足 $\eta^*(\sigma_1) = \mathbb{0}$，因此$\eta^* \notin \{\eta \mid \eta(\sigma_1) = \mathbb{1}\}$，也就是说 $\eta^* \notin [\![(\text{Flip}(\overline{\sigma_1}) \wedge \overline{\mathbb{1}} = \texttt{1}) \vee (\neg\text{Flip}(\overline{\sigma_1}) \wedge \overline{\mathbb{1}} = \texttt{0})]\!]$。

归纳情形。如果 $f \in \mathcal{POR}$ 是由 Σ_1^b 可表示函数通过复合或有界递归得到的，那么 f 也是 Σ_1^b 可表示的。

□

B 第4节的证明

B.1 RFP 与 SFP 的关系

B.1.1 关于流式图灵机

我们以形式化的方式定义流式图灵机。

定义 B.1（流式图灵机）。流式图灵机是一个四元组 $\mathscr{MS} = \langle \mathrm{Q}\ q_0, \Sigma, \delta \rangle$，其中：

- Q 是一个有限状态集合，其元素记为 $q_1, q_2, \ldots$
- $q_0 \in$Q 是一个初始状态
- Σ 是一个有限字符集，由 c_1、c_2、.....表示
- δ：$\hat{}\Sigma \times \mathrm{Q} \times \hat{}\Sigma \times \mathrm{B} \to \hat{}\Sigma \times \{\mathrm{L}, \mathrm{R}\}$ 是一个转移函数，用于描述机器到达的新配置。

L 和 R 是两个固定且不同的符号（例如 1 和 0），$\hat{}\ \Sigma = \Sigma \cup \{\circledast\}$ 和$\circledast \notin \Sigma$ 是空白字符。

定义 B.2（STM 的配置）。STM 的配置是一个四元组 $\langle \sigma, q, \tau, \omega \rangle$，其中：

- $\sigma \in \{\mathbb{0}, \mathbb{1}, \circledast\}^*$ 是读写头左侧的工作带部分
- $q \in$Q 是机器的当前状态
- $\tau \in \{\mathbb{0}, \mathbb{1}, \circledast\}^*$ 是读写头右侧的工作带部分
- $\omega \in \mathrm{B}^{\mathbb{N}}$ 是尚未读取的预言机带部分。

现在可以给出 STM 的可达关系族的定义。

定义 B.3（STM 的可达函数）。给定一个具有转移函数 δ 的 STM $\mathscr{M}_{\mathcal{S}}$，我们用 $\vdash_\delta$ 表示其标准步函数，并用 $\{\triangleright^n_{\mathscr{M}_{\mathcal{S}}}\}_n$ 表示满足以下条件的最小关系族：

$$\langle \sigma, q, \tau, \omega \rangle \triangleright^0_{\mathscr{M}_{\mathcal{S}}} \langle \sigma, q, \tau, \omega \rangle$$

$$\left(\langle \sigma, q, \tau, \omega \rangle \triangleright^n_{\mathscr{M}_{\mathcal{S}}} \langle \sigma', q, \tau', \omega' \rangle\right) \wedge$$

$$\left(\langle \sigma', q', \tau', \omega' \rangle \vdash_\delta \langle \sigma'', q', \tau'', \omega'' \rangle\right) \to \left(\langle \sigma, q, \tau, \omega \rangle \triangleright^{n+1}_{\mathscr{M}_{\mathcal{S}}} \langle \sigma'', q', \tau'', \omega'' \rangle\right)$$

定义 B.4（STM 计算）。给定一个 STM $\mathscr{MS} = \langle \mathrm{Q}\ q_0、\ \Sigma、\ \delta \rangle$，预言机带 $\omega : \mathrm{N} \to \mathrm{B}$ 以及函数 $g : \mathrm{N} \to \mathrm{B}$，我们称 $\mathscr{M}_{\mathcal{S}}$ 计算 $\mathrm{g} f_{\mathscr{M}_{\mathcal{S}}} = g$，当且仅当对于每个字符串 $\sigma \in \mathrm{S}$ 和预言机带 $\omega \in \mathrm{B}^{\mathbb{N}}$，都存在$n \in \mathrm{N}$ $\tau \in \mathrm{S}$ $q' \in \mathrm{Q}$，以及函数 $\psi : \mathrm{N} \to \mathrm{B}$，使得

$$\langle \epsilon, q_0, \sigma, \omega \rangle \triangleright^n_{\mathscr{M}_{\mathcal{S}}} \langle \gamma, q', \tau, \psi \rangle,$$

并且 $\langle \gamma, q', \tau, \psi \rangle$ 是 $\mathscr{MS}$的最终构型，其中 $f_{\mathscr{M}_{\mathcal{S}}}(\sigma, \omega)$ 是 γ 中不包含 $\circledast$的最长后缀。

B.1.2 命题 4.3 的证明

我们需要将此定义扩展到 S 上的概率分布，以便处理概率图灵机。

定义 B.5. 给定一个概率图灵机 $\mathscr{M}_{\mathscr{P}}$、一个配置 $\langle \sigma, q, \tau \rangle$，我们定义以下随机变量序列：

$$X^{\langle \sigma,q,\tau\rangle}_{\mathscr{M}_{\mathscr{P}},0} := \omega \to \langle \sigma, q, \tau \rangle$$

$$X^{\langle \sigma,q,\tau\rangle}_{\mathscr{M}_{\mathscr{P}},n+1} := \omega \to \begin{cases} \delta_{\mathbb{b}}\big(X^{\langle \sigma,q,\tau\rangle}(\omega)\big) & \text{if } \omega(n) = \mathbb{b} \text{ and for some } \langle \sigma', q', \tau' \rangle, \\ & \qquad \delta_{\mathbb{b}}(X^{\langle \sigma,q,\tau\rangle}_{\mathscr{M}_{\mathscr{P}},n}(\omega)) = \langle \sigma', q', \tau' \rangle \\ X^{\langle \sigma,q,\tau\rangle}_{\mathscr{M}_{\mathscr{P}},n}(\omega) & \text{if } \omega(n) = \mathbb{b} \text{ and for no } \langle \sigma', q', \tau' \rangle, \\ & \qquad \delta_{\mathbb{b}}(X^{\langle \sigma,q,\tau\rangle}_{\mathscr{M}_{\mathscr{P}},n}(\omega)) = \langle \sigma', q', \sigma' \rangle. \end{cases}$$

对于任意 $\omega \in \mathbb{B}^{\mathbb{N}}$。

直观地说，变量 $X^{\langle \sigma}_{,q,\tau\rangle\,\mathscr{M}_{\mathscr{P}},n}$ 描述机器恰好经过 n 次转移后到达的配置。若存在一个 $m \in \mathbb{N}$，使得对于任意 $\sigma \in \mathbb{S}$，$X^{\langle \sigma}_{,q_0,\tau\rangle\,\mathscr{M}_{\mathscr{P}}}\, m$ 均为终止状态，则称概率图灵机 $\mathscr{M}_{\mathscr{P}}$ 计算 $Y_{\mathscr{M}_{\mathscr{P}},\sigma}$。在这种情况下，$Y_{\mathscr{M}_{\mathscr{P}},\sigma}$ 是 $\pi_1\Big(X^{\langle \sigma,q_0,\epsilon\rangle}_{\mathscr{P}}\,\mathscr{M}_m\Big)$ 的最长后缀，其中不包含 $\circledast$。

现在我们证明命题 4.3，该命题确立了 STM 与概率图灵机之间的等价性。

命题 4.3 的证明概要。我们证明，对于任意 $\sigma, \tau \in \mathbb{S}$，

$$\mu\big(\{\omega \in \mathbb{B}^{\mathbb{N}} \mid \mathscr{M}_{\mathcal{S}}(\sigma, \omega) = \tau\}\big) = \mu\big(\mathscr{M}_{\mathscr{P}}(\sigma)^{-1}(\tau)\big)$$
$$\mu\big(\{\omega \in \mathbb{B}^{\mathbb{N}} \mid \mathscr{M}_{\mathcal{S}}(\sigma, \omega) = \tau\}\big) = \mu\big(\{\omega \in \mathbb{B}^{\mathbb{N}} \mid Y_{\mathscr{M}_{\mathcal{S}},\sigma}(\omega) = \tau\}\big).$$

实际上，我们证明了一个更强的结果，即存在一个双射 $I : \mathrm{STM} \to \mathrm{PTM}$，使得对于任意 $n \in \mathbb{N}$

$$\{\omega \in \mathbb{B}^{\mathbb{N}} \mid \langle \sigma, q_0, \tau, \omega \rangle \rhd^n_\delta \langle \tau, q, \psi, n \rangle\} = \{\omega \in \mathbb{B}^{\mathbb{N}} \mid X^{\langle \epsilon,q_0,\sigma\rangle}_{I(\mathscr{M}_{\mathcal{S}}),n}(\omega) = \langle \tau, q, \psi \rangle\}. \tag{I.}$$

这意味着，

$$\{\omega \in \mathbb{B}^{\mathbb{N}} \mid \mathscr{M}_{\mathcal{S}}(\sigma, \omega) = \tau\} = \{\omega \in \mathbb{B}^{\mathbb{N}} \mid Y_{I(\mathscr{M}_{\mathcal{S}}),\sigma}(\omega) = \tau\}. \tag{II.}$$

双射 I 将 $\mathscr{M}_{\mathcal{S}}$ 的函数 δ 分解如下：若预言机带上对应的字符为 0，则转移由 δ_0 定义；若字符为 1，则由 δ_1 定义。我们通过对 $\mathscr{M}_{\mathcal{S}}$ 计算其输入值所需的步数进行归纳，证明 (I.)。

□

B.2 从 SFP 到 $\mathcal{POR}$

为证明命题 4.4，我们展示 STM 可计算的函数与有限流STM 可计算的函数之间的对应关系。

引理 B.1. 对于所有具有多项式时间界 p 的 $f \in$SFP，都存在一个 $h \in$PTF，使得对于任意 $\omega \in \mathrm{B}^{\mathbb{N}}$ 和 $\sigma \in \mathrm{S}$,

$$f(\sigma, \eta) = h(\sigma, \omega_{p(|\sigma|)}).$$

证明. 由于 $f \in$SFP，存在多项式时间 STM $\mathscr{M}_{\mathcal{S}} = \langle \mathrm{Q}\ q_0, \Sigma, \delta \rangle$，使得$f = f_{\mathscr{M}_{\mathcal{S}}}$。考虑 FSTM $\mathscr{M}_{\mathcal{S}}{}'$，其定义与 $\mathscr{M}_{\mathcal{S}}$ 相同，但它是有限的。于是对于任意 $k \in \mathrm{N}$ 和 $\sigma', \tau', \tau'', \tau''' \in \mathrm{S}$,

$$\langle \epsilon, q_0', \sigma, \sigma' \rangle \rhd^k_{\mathscr{M}_{\mathcal{S}}} \langle \tau, q, \tau', \tau'' \rangle \quad \text{iff} \quad \langle \epsilon, q_0', \sigma, \sigma'\eta \rangle \rhd^k_{\mathscr{M}_{\mathcal{S}}'} \langle \tau, q, \tau'', \tau'''\eta \rangle.$$

此外，$\mathscr{M}_{\mathcal{S}}{}'$ 所需的步数与 $\mathscr{M}_{\mathcal{S}}$ 所需的步数相同，因此也属于 PTF。我们通过定义 $h = f_{\mathscr{M}_{\mathcal{S}}'}$ 来完成证明。 □

接下来要证明，每个函数 $f \in$PTF 都对应一个无需借助 Q 即可定义的函数。

引理 B.2. 对于任意 $f \in$ PTF 和 $\sigma \in \mathrm{S}$，存在一个 $g \in \mathcal{POR}$，使得对于任意 $x, y \in \mathrm{S}$ 和 $\eta \in \mathrm{O}$，$f(x, y) = g(x, y, \eta)$。此外，如果 f 的定义无需借助 Q，那么 g 也不包含 Q。

证明概要。我们概述证明的主要步骤:

1. 我们为 FSTM 的配置和转移函数定义基于字符串的编码，分别称为 e_c 和 e_t。此外，还存在一个函数 $step \in \mathcal{POR}$，它满足图 7 中的模拟模式。注意，e_c、e_t 和 $step$ 对于给定的模拟是正确的。

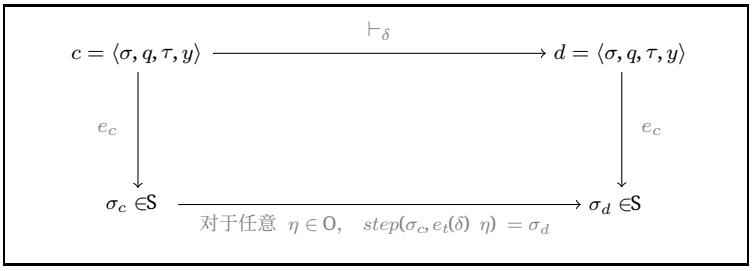


图 7: $step$的行为。

2. 对于任意 $f \in \mathcal{POR}$ 和 $\sigma, \tau \in \mathrm{S}$，如果存在一个 $\mathcal{RL}$-项 $t(x)$，它能界定任意可能输入下 $f(\sigma, \eta)$ 的大小，那么 $f_m = \lambda z, x, \eta^{|z|}(x, \eta) \in \mathcal{POR}$.[15]

[15]注意，如果定义 f 时不递归调用 Q，那么也可以不使用它来定义 f_m。

3. 给定一台机器 $\mathscr{M}_{\mathcal{S}}$，如果 $\sigma \in \mathsf{S}$ 是$\mathscr{M}_{\mathcal{S}}$某个配置的正确编码，那么对于任意 $\eta \in \mathsf{O}$ $|step(\sigma,\eta)|$ 是 $\mathcal{O}(|\sigma|)$。4. 对于任意 $\eta \in \mathsf{O}$，如果 $c = e_c(\sigma, q, \tau, y, \eta)$，那么存在一个函数 $dectape$，使得 $dectape(x, \eta)$ 是不含 $\circledast$ 的最长后缀。

□

因此，根据引理 B.2，每个函数 $f \in$ SFP 都可以通过一个函数 $g \in \mathcal{POR}$ 来模拟，并将预言机 f 的一个多项式长度前缀作为额外输入。

推论 B.1. 对任意 $f \in$SFP 和多项式 p，存在一个函数 $f \in \mathcal{POR}$，使得对于任意 $\omega \in \mathsf{B}^{\mathbb{N}}$、$\eta \in \mathsf{O}$ 和 $x \in$S,

$$f(x, \omega) = g(x, \omega_{p(|x|),\eta}).$$

证明. 假设 $f \in$ SFP 且 $y = \eta_{p(|x|)}$。根据引理 B.1，存在一个函数$h \in$PTF，使得对于任意 $\eta : \mathsf{N} \to \mathsf{B}$ 和 $x \in$S,

$$f(x, \eta) = h(x, \eta_{p(|x|)}).$$

此外，由引理 B.2，存在一个 $g \in \mathcal{POR}$，使得对于任意 x、$y \in$S $\omega \in \mathsf{O}$,

$$g(x, y, \omega) = h(x, y).$$

那么 g 就是所需的函数。 □

现在我们证明存在一个函数 $e \in \mathcal{POR}$，它生成的字符串与 $\mathsf{S}^{\mathbb{N}}$ 中各函数的前缀具有相同的分布。直观地说，该函数从 η 中提取 $|x|+1$ 位，并将它们连接起来作为输出。e 的定义通过一个数的二进制表示 $dyad$: N $\to$ S 得到。因此，函数 e 创建字符串 1_0、1_1、. . .、$\mathbb{1}^k$，并在给定的坐标上对函数 η 进行采样——即 $dy(\mathbb{1}^0)$ $dy(\mathbb{1}^1)$ . . .、$dy(\mathbb{1}^k)$——将结果连接成一个字符串。

定义 B.6（函数 $dyad$）。函数 $dyad$: N $\to$ S 将每个$n \in$ N 映射为从 $n+1$ 的二进制表示中去掉最左位后得到的字符串。

为了定义 $dy(\cdot,\cdot)$，引入了一些辅助函数，即$binsucc : \mathsf{S} \times \mathsf{O} \to \mathsf{S}$,

$$\begin{aligned} binsucc(\epsilon, \eta) &:= \mathbb{1} \\ binsucc(x\mathbb{0}, \eta) &:= x\mathbb{1}|_{x\mathbb{0}\mathbb{0}} \\ binsucc(x\mathbb{1}, \eta) &:= binsucc(x, \eta)\mathbb{0}|_{x\mathbb{0}\mathbb{0}}. \end{aligned}$$

以及 $bin : \mathsf{S} \times \mathsf{O} \to \mathsf{S}$,

$$\begin{aligned} bin(\epsilon, \eta) &:= \mathbb{0} \\ bin(x\mathbb{b}, \eta) &:= binsucc(bin(x, \eta), \eta)|_{x\mathbb{b}}. \end{aligned}$$

定义 B.7（函数 dy）。函数 $dy:\ \mathsf{S}\times\mathsf{O}\ \to\mathsf{S}$ 定义如下：

$$dy(x,\eta) := lrs(bin(x,\eta),\eta),$$

其中 lrs 是一个字符串操作器：如果字符串非空，就移除其最左位；否则返回 ϵ。[16]

容易证明，函数 $dyad(n)$ 是双射，以下命题可通过归纳法证明。

命题 B.3. 对任意 $n\in\mathsf{N}$ $\sigma\in\mathsf{S}$ 和 $\eta\in\mathsf{O}$，若 $|\sigma|=n+1$，则

$$dy(\sigma,\eta)=dyad(n).$$

我们还引入函数 e，并证明其正确性（对字符串的结构进行归纳）。

定义 B.8（函数 e）。令 $e:\mathsf{S}\times\mathsf{O}\ \to\mathsf{S}$ 定义如下：

$$\begin{aligned} e(\epsilon,\eta) &:= \epsilon \\ e(x\mathbb{b},\eta) &:= e(x,\omega)Q(dy(x,\eta),\eta)|_{x\mathbb{b}}. \end{aligned}$$

引理 B.4（e 的正确性）。对于任意 $\sigma\in\mathsf{S}$ 和 $i\in\mathsf{N}$，若 $|\sigma|=i+1$，则对每个 $j\le i\in\mathsf{N}$ 和 $\eta\in\mathsf{O}$：

i. $e(\sigma,\eta)(i)=\eta(dy(\mathbb{1}^j,\eta))$，ii. $e(\sigma,\eta)$ 的长度恰好为 $i+1$。

我们还引入了一个关系 $\sim_{dy}$，它同样是一个双射。

定义 B.9。我们将 $\sim_{dy}$ 定义为 $\mathsf{O}\times\mathsf{B}^{\mathbb{N}}$ 中满足以下条件的最小关系：

$$\eta\sim_{dy}\eta\ \text{ iff }\ \text{for any } n\in\mathbb{N},\omega(n)=\eta(dy(\mathbb{1}^{n+1},\omega)).$$

引理 B.5。若 $\omega\sim_{dy}\eta$，则存在一个 $n\in\mathsf{N}$，

$$e(\underline{n}_{\mathbb{N}},\eta).$$

证明。证明采用逆否命题。假设 $\omega_n\neq e(\underline{n}_{\mathbb{N}},\eta)$。根据引理 B.4，存在一个 $m\in\mathsf{N}$，使得 $\omega(m)\neq\eta(dy(\underline{m}_{\mathbb{N}},\eta))$，这导致矛盾。□

我们现在终于可以证明命题 4.4。

命题 4.4 的证明。根据推论 B.1，存在一个函数 $f'\in\mathcal{POR}$ 和一个多项式 p，使得对于任意 $\sigma,\tau\in\mathsf{S}$，$\omega\in\mathsf{B}^{\mathbb{N}}$ 和 $\eta\in\mathsf{O}$，

$$\sigma=\omega_{p(x)}\to f(\sigma,\omega)=f'(\sigma,\tau,\eta). \qquad (*)$$

[16]完整详情请见 [5]。

固定 $\overline{\omega} \in \{\omega \in \mathsf{B}^{\mathbb{N}} \mid f(\sigma,\omega) = y\}$，其关于 sim_{dy}的像属于 $\{\eta \in \mathsf{O} \mid f'(x, e(p'(s(x,\eta)\ \eta)\ \eta)\ \eta) = \tau\}$，其中 s是计算 $\mathbb{1}^{|x|+1}$的 $\mathcal{POR}$函数。根据引理 B.5,

$$\overline{\omega}_{p(x)} = e(p(size(x,\eta),\eta),$$

其中 $p' \in \mathcal{POR}$ 计算多项式 p，且该多项式的定义不依赖于 Q。此外，给定一个固定的 $\overline{\eta} \in \{\eta \in \mathsf{O} \mid f'(\sigma, e(p'(size(\sigma,\eta)\ \eta)\ \eta)\ \eta) = \tau\}$，它关于 $\sim_{dy} \in \{\omega \in \mathsf{B}^{\mathbb{N}} \mid f(\sigma,\omega) = \tau\}$的原像。证明与上面的证明类似。由于 $\sim_{dy}$ 是.....之间的双射

$$\mu(\{\omega \in \mathbb{B}^{\mathbb{N}} \mid f(\sigma,\omega) = \tau\}) = \mu(\{\eta \in \mathbb{O} | f'(x, e(p(size(x,\eta),\eta),\eta),\eta) = \tau\}),$$

由此得证。 □

B.3 从 $\mathcal{POR}$ 到 SFP

首先，我们定义命令式语言 $\mathsf{SIFP}_{\mathrm{RA}}$ 及其大步语义，并证明其多项式时间程序等价于 $\mathcal{POR}$。

定义 B.10（$\mathsf{SIFP}_{\mathrm{RA}}$的程序）。$\mathsf{SIFP}_{\mathrm{RA}}\mathcal{L}(\mathsf{Stm}_{\mathrm{RA}})$ 的程序语言——即由非终结符号 $\mathsf{Stm}_{\mathrm{RA}}$ 生成的字符串集合——定义如下:

$$\begin{aligned}
\mathsf{Id} &:= X_i \mid Y_i \mid S_i \mid R \mid Q \mid Z \mid T \\
\mathsf{Exp} &:= \epsilon \mid \mathsf{Exp}.0 \mid \mathsf{Exp}.1 \mid \mathsf{Id} \mid \mathsf{Exp} \sqsubseteq \mathsf{Id} \mid \mathsf{Exp} \wedge \mathsf{Id} \mid \neg\mathsf{Exp} \\
\mathsf{Stm}_{\mathrm{RA}} &:= \mathsf{Id} \leftarrow \mathsf{Exp} \mid \mathsf{Stm}_{\mathrm{RA}}; \mathsf{Stm}_{\mathrm{RA}} \mid \texttt{while}(\mathsf{Exp})\{\mathsf{Stm}\}_{\mathrm{RA}} \mid \texttt{Flip}(\mathsf{Exp}),
\end{aligned}$$

其中 $i \in \mathsf{N}$。

与 $\mathsf{SIFP}_{\mathrm{RA}}$ 程序语言相关的大步语义依赖于存储的概念。

定义 B.11（存储）。存储是一个函数 Σ: Id $\rightharpoonup$ S。空存储是指在 ϵ 上为全函数且为常值的存储。我们将此对象表示为 [ ]。我们定义将映射从 $y \in$Id 到 $\sigma \in$S 应用于存储 Σ 的更新操作如下:

$$\Sigma[y \leftarrow \sigma](x) := \begin{cases} \sigma & \text{if } x = y \\ \Sigma(x) & \text{otherwise.} \end{cases}$$

定义 B.12（$\mathsf{SIFP}_{\mathrm{RA}}$ 中表达式的语义）。表达式 $E \in \mathcal{L}$(Exp) 的语义是满足以下规则的最小关系 $\rightharpoonup$: $\mathcal{L}$(Exp) $\times$ (Id $\to$ S) $\times$O $\times$S:

$$\frac{}{\langle \epsilon, \Sigma\rangle \rightharpoonup \boldsymbol{\epsilon}} \qquad \frac{\langle e, \Sigma\rangle \rightharpoonup \sigma}{\langle e.\mathsf{b}, \Sigma\rangle \rightharpoonup \sigma \frown \mathbb{b}}$$

$$\frac{\langle e, \Sigma\rangle \rightharpoonup \sigma \qquad \Sigma(\mathsf{Id}) = \tau \qquad \sigma \subseteq \tau}{\langle e \sqsubseteq \mathsf{Id}, \Sigma\rangle \rightharpoonup \mathbb{1}} \qquad \frac{\langle e, \Sigma\rangle \rightharpoonup \sigma \qquad \Sigma(\mathsf{Id}) = \tau \qquad \sigma \not\subseteq \tau}{\langle e \sqsubseteq \mathsf{Id}, \Sigma\rangle \rightharpoonup \mathbb{0}}$$

$$\frac{\Sigma(\mathsf{Id}) = \sigma}{\langle \mathsf{Id}, \Sigma\rangle \rightharpoonup \sigma} \qquad \frac{\mathsf{Id} \notin dom(\Sigma)}{\langle \mathsf{Id}, \Sigma\rangle \rightharpoonup \boldsymbol{\epsilon}}$$

$$\frac{\langle e, \Sigma\rangle \rightharpoonup 0}{\langle \neg e, \Sigma\rangle \rightharpoonup \mathbb{1}} \qquad \frac{\langle e, \Sigma\rangle \rightharpoonup \sigma \qquad \sigma \neq \mathbb{0}}{\langle \neg e, \Sigma\rangle \rightharpoonup \mathbb{0}}$$

$$\frac{\langle e, \Sigma\rangle \rightharpoonup \mathbb{1} \qquad \Sigma(\mathsf{Id}) = \mathbb{1}}{\langle e \wedge \mathsf{Id}, \Sigma\rangle \rightharpoonup \mathbb{1}} \qquad \frac{\langle e, \Sigma\rangle \rightharpoonup \sigma \qquad \Sigma(\mathsf{Id}) = \tau \qquad \sigma \neq \mathbb{1} \wedge \tau \neq \mathbb{1}}{\langle e \wedge \mathsf{Id}, \Sigma\rangle \rightharpoonup \mathbb{0}}$$

其中 $\mathsf{b} \in \{0, 1\}$.[17]

定义 B.13（大步操作语义）。程序 $\mathsf{P} \in \mathcal{L}(\mathrm{Stm}_{\mathrm{RA}})$ 的语义是满足以下规则的最小关系 $\triangleright \subseteq \mathcal{L}(\mathrm{Stm}_{\mathrm{RA}}) \times (\mathrm{Id} \to \mathrm{S}) \times \mathrm{O} \times (\mathrm{Id} \to \mathrm{S})$：

$$\frac{\langle e, \Sigma\rangle \rightharpoonup \sigma}{\langle \mathsf{Id} \rightharpoonup e, \Sigma, \eta\rangle \triangleright \Sigma[\mathsf{Id} \leftarrow \sigma]} \qquad \frac{\langle s, \Sigma, \eta\rangle \triangleright \Sigma' \qquad \langle t, \Sigma', \eta\rangle \triangleright \Sigma''}{\langle s; t, \Sigma, \eta\rangle \triangleright \Sigma''}$$

$$\frac{\langle e, \Sigma\rangle \rightharpoonup \mathbb{1} \qquad \langle s, \Sigma, \eta\rangle \triangleright \Sigma' \qquad \langle \texttt{while}(e)\{s\}, \Sigma', \eta\rangle \triangleright \Sigma''}{\langle \texttt{while}(e)\{s\}, \Sigma, \eta\rangle \triangleright \Sigma''}$$

$$\frac{\langle e, \Sigma\rangle \rightharpoonup \sigma \qquad \sigma \neq \mathbb{1}}{\langle \texttt{while}(e)\{s\}, \Sigma, \eta\rangle \triangleright \Sigma} \qquad \frac{\langle e, \Sigma\rangle \rightharpoonup \sigma \qquad \eta(\sigma) = \mathbb{b}}{\langle \texttt{Flip}(e), \Sigma, \eta\rangle \triangleright \Sigma[R \leftarrow \mathbb{b}]}$$

该语义使我们能够将每个 $\mathrm{SIFP}_{\mathrm{RA}}$ 程序与其所求值的函数关联起来：

定义 B.14。正确的 $\mathrm{SIFP}_{\mathrm{RA}}$ 程序 P 的函数求值定义为 $[\![\cdot]\!]\!:\mathcal{L}(\mathrm{Stm}_{\mathrm{RA}}) \to (\mathrm{S}^n \times \mathrm{O} \to \mathrm{S})$，如下所示：[18]

$$[\![\mathsf{P}]\!] := \lambda x_1, \ldots, x_n, \eta \triangleright (\langle \mathsf{P}, [\,][X_1 \leftarrow x_1], \ldots, [X_n \leftarrow x_n], \eta\rangle)(R).$$

注意，在不同的寄存器中，寄存器 R 用于存放程序执行结束时计算出的值。同样，$\{X_i\}_{i\in\mathbb{N}}$ 寄存器用于存放函数的输入。现在我们建立 $\mathcal{POR}$ 与 $\mathrm{SIFP}_{\mathrm{RA}}$ 之间的对应关系。

引理 B.6。对于任意函数 $f \in \mathcal{POR}$，都存在一个多项式时间 SIFP_{RA} 程序 P，使得对于所有 $x_1, \ldots, x_n$,

$$[\![P]\!](x_1, \ldots, x_n, \omega) = f(x_1, \ldots, x_n, \omega).$$

此外，如果 $f \in \mathcal{POR}$，那么 P 不包含任何 Flip(e) 语句。

[17]我们假设，若 $\mathsf{b} = \mathbb{1}$，则 $\mathsf{b} = \mathbb{1}$；若 $\mathsf{b} = \mathbb{0}$，则 $\mathsf{b} = \mathbb{0}$。[18]我们不使用 $\triangleright$ 的中缀表示法，而采用其前缀表示法。因此，该表示法用 $\triangleright$ 表示与 P、Σ 和 ω 相关联的存储。此外，我们使用相同的函数符号 $\triangleright$ 表示两个不同的函数：$\mathrm{SIFP}_{\mathrm{RA}}$ 的大步操作语义，以及 $\mathrm{SIFP}_{\mathrm{LA}}$ 中程序的大步操作语义。

证明概要。从技术角度来看，证明相当简单，它依赖于这样一个事实：可以为任意 $\mathcal{POR}$ 函数关联一个等价的多项式时间程序；还依赖于这样一种可能性：能够组合这些程序，并以多项式开销在 $\mathrm{SIFP}_{\mathrm{RA}}$ 中实现记号上的有界递归。具体而言，对于任意函数 $f \in \mathcal{POR}$，我们定义一个程序 $\mathscr{A}$，使得$[\![\mathscr{L}_f]\!](x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$。$\mathscr{A}$ 的正确性由以下不变性质给出：

- 计算结果存储在 R 中
- 输入存储在组 X 的寄存器中
- 函数 $\mathscr{L}$不会改变它作为输入访问的值。

我们定义 $\mathscr{A}$ 如下：

$$\begin{aligned}
\mathscr{L}_E &= R \leftarrow \epsilon \\
\mathscr{L}_{S_0} &= R \leftarrow X_0.0 \\
\mathscr{L}_{S_1} &= R \leftarrow X_0.1 \\
\mathscr{L}_{P_i^n} &= R \leftarrow X_i \\
\mathscr{L}_C &= R \leftarrow X_1 \sqsubseteq X_2 \\
\mathscr{L}Q &= \mathtt{Flip}(X_1).
\end{aligned}$$

基本情形的正确性很容易证明，且唯一包含 Flip(e)（其中 $e \in \mathcal{L}$ 属于 Exp）的翻译是 Q 的翻译。复合和有界递归的编码则更加复杂。[19]

□

B.3.1 从 $\mathrm{SIFP}_{\mathbf{RA}}$ 到 $\mathrm{SIFP}_{\mathbf{LA}}$

现在我们证明，$\mathrm{SIFP}_{\mathrm{RA}}$ 中的每个程序都等价于 $\mathrm{SIFP}_{\mathrm{LA}}$ 中的一个程序。首先，我们需要定义 $\mathrm{SIFP}_{\mathrm{LA}}$ 的语言和语义。

定义 B.15（$\mathrm{SIFP}_{\mathrm{LA}}$ 的语言）。$\mathrm{SIFP}_{\mathrm{LA}}$ $\mathcal{L}$ 的语言 $\mathrm{Stm}_{\mathrm{LA}}$，即由非终结符号 $\mathrm{Stm}_{\mathrm{LA}}$ 生成的字符串集合，定义如下：

$$\mathrm{Stm}_{\mathrm{LA}} := \mathsf{Id} \leftarrow \mathsf{Exp} \;\Big|\; \mathrm{Stm}_{\mathrm{LA}}; \mathrm{Stm}_{\mathrm{LA}} \;\Big|\; \mathtt{while}(\mathsf{Exp})\{\mathsf{Stm}\}_{\mathrm{LA}} \;\Big|\; \mathtt{RandBit}().$$

定义 B.16（$\mathrm{SIFP}_{\mathrm{LA}}$ 的大步语义）。程序 $\mathsf{P} \in \mathcal{L}(\mathrm{Stm}_{\mathrm{LA}})$ 的语义是最小关系 $\triangleright \subseteq (\mathcal{L}(\mathrm{Stm}_{\mathrm{LA}}) \times (\mathsf{Id} \to \mathsf{S} \times \mathsf{B}^{\mathbb{N}}) \times ((\mathsf{Id} \to \mathsf{S} \times \mathsf{B}^{\mathbb{N}})$，它在以下规则下封闭：

$$\frac{\langle e, \Sigma\rangle \rightharpoonup \sigma}{\langle \mathsf{Id} \leftarrow e, \Sigma, \omega\rangle \triangleright \langle \Sigma[\mathsf{Id} \leftarrow \sigma], \omega\rangle} \qquad \frac{\langle s, \Sigma, \omega\rangle \triangleright \langle \Sigma', \omega'\rangle \qquad \langle t, \Sigma', \omega\rangle \triangleright \langle \Sigma'', \omega''\rangle}{\langle s; t, \Sigma, \omega\rangle \triangleright \langle \Sigma'', \omega''\rangle}$$

$$\frac{\langle e, \Sigma\rangle \rightharpoonup \mathbb{1} \qquad \langle s, \Sigma, \omega\rangle \triangleright \langle \Sigma', \omega'\rangle \qquad \langle \mathsf{while}(e)\{s\}, \Sigma', \omega\rangle \triangleright \langle \Sigma'', \omega''\rangle}{\langle \text{当}\ (e)\ \{s\},\ \Sigma,\ \omega\rangle \triangleright \langle \Sigma',\ \omega''\rangle}$$

[19]证明它们正确性需要大量底层定义和技术结果。有关详尽的介绍，请参见 [5]。

$$\frac{\langle e, \Sigma\rangle \rightharpoonup \sigma \qquad \sigma \neq \mathbb{1}}{\langle \texttt{while}(e)\{s\}, \Sigma, \omega\rangle \triangleright \langle \Sigma, \omega\rangle} \qquad \frac{}{\langle \text{RandBit() } \Sigma,\ \mathsf{b}\omega\rangle \triangleright \langle \Sigma[R \leftarrow \mathsf{b}], \omega\rangle}$$

引理 B.7. 对于每个全程序 P $\in$SIFP$_{RA}$，都存在一个 $Q \in$SIFP$_{LA}$，使得对于任意 x, $y \in$ N,

$$\mu(\{\omega \in \mathbb{O} \mid [\![P]\!](x, \eta) = y\}) = \mu(\{\omega \in \mathbb{B}^{\mathbb{N}} \mid [\![Q]\!](x, \eta) = y\}).$$

此外，如果 P 是多项式时间的 Q，也如此。

证明概要。我们证明引理 B.7：在给定两个新的小步语义关系（LA、RA）的情况下，可以在 SIFP$_{\mathrm{RA}}$ 中模拟 SIFP$_{\mathrm{LA}}$。这两个关系是通过将相应的大步语义拆分为最小转移而得到的，每条 $\cdot\,;\ \cdot$ 指令对应一个转移。这种新语义背后的直观思想，是用构建从 SIFP$_{\mathrm{RA}}$ 到 SIFP$_{\mathrm{LA}}$ 的归纳证明所需的一些信息来丰富大步操作语义。具体而言，我们使用一个列表 Ψ，其中包含若干对（x，b），用于跟踪对原语 Flip(x) 的上一次调用（针对 SIFP$_{\mathrm{RA}}$），以及对原语 RandBit() 的第 x 次调用（针对 SIFP$_{\mathrm{LA}}$）所得到的结果。

主要问题在于如何模拟对随机带的访问。随后，我们定义翻译，使其将一张记录所有 σ 在 Flip(σ) 指令中发出的查询及所选取并返回的结果 b 的关联表存储在一个特定且全新的寄存器中。加入映射 Ψ 后，便能够在程序的语义中显式地复现关联表 Ψ 的内容。这种模拟需要将 Flip(e) 翻译为一个等价的过程。

- 对于每次模拟的查询 Flip(e)，目标程序会查找关联表

- 如果它在某个二元组（e，b）中找到查询坐标 e，则返回 b。否则，(i) 它将 Flip(e) 归约为一次 RandBit() 调用，该调用输出 b $= \mathbb{0}$ 或 b $= \mathbb{1}$ 中的一个；(ii) 它将二元组 $\langle e$，b$\rangle$ 记录在关联表中，并返回 b。

这种构造十分复杂。这种模拟保持了原程序计算出的字符串的分布：

1. 我们证明 SIFP$_{\mathrm{RA}}$ 的大步语义和小步语义具有同等的表达能力。2. 我们定义了一个关系 Θ，该关系连接 SIFP$_{\mathrm{RA}}$ 和 SIFP$_{\mathrm{LA}}$ 的小步语义中的配置：

   * 首先，我们定义一个函数 α： $\mathcal{L}$(Stm$_{\mathrm{RA}}$) $\to$ $\mathcal{L}$(Stm$_{\mathrm{LA}}$)，将程序 P$_{\mathrm{RA}}$ $\in$ $\mathcal{L}$(Stm$_{\mathrm{RA}}$) 映射为相应的 P$_{\mathrm{LA}} \in$ $\mathcal{L}$(Stm$_{\mathrm{LA}}$)，并按照上述方式翻译 Flip(e)。

   * 我们定义三元组 $\langle$P$_{\mathrm{RA}}\Sigma, \Psi\rangle$ 与单个存储Γ之间的关系 β，旨在捕捉配置到存储的依赖关系



图8：SIFP$_{\mathrm{RA}}$ 与SIFP$_{\mathrm{LA}}$之间的交换模式

P$_{\mathrm{RA}}$ 使用存储 Σ 运行时的配置与计算出的结合式表 Ψ，以及模拟 P$_{\mathrm{LA}}$时的存储 Γ 之间。因此， Γ 将 Ψ 的表示存入专用寄存器。

$*$ 一个函数 γ，它将RA 收集的预言机约束转换为LA收集的信息。然后，Θ 的定义使得当以下条件成立时， Θ(⟨P Σ$_1$, Ψ⟩, ⟨Q, Σ$_2$, Θ⟩)成立：(i.) α(P) $= Q$, (ii.)β(⟨P Σ$_1$, Ψ⟩, Σ$_2$), (iii.) γ(Ψ) $=$ Φ, (iv.) μ(Ψ) $= \mu$(Φ)。

3. 我们证明， Θ 会将每个三元组 ⟨P$_{\mathrm{RA}}$, Σ, Ψ⟩ 关联到其他三元组 ⟨P$_{\mathrm{LA}}$, Γ, Φ⟩，这些三元组相对于 RA 弱模拟关系 LA。图8展示了这一点。

□

B.3.2 从 SIFP$_{\mathbf{LA}}$ 到 SFP$_{\mathbf{OD}}$

我们引入 SFP$_{\mathrm{OD}}$，这是对应于 SFP 的一个类，它定义在一种变体 STM 上；这种 STM 可以按需从预言机读取字符。我们还证明，SIFP$_{\mathrm{LA}}$ 可以归约到它。为便于阅读，我们省略繁琐的细节，着重非正式地（但详尽地）描述如何构造按需 STM。

命题 B.8. 对于每个 P $\in \mathcal{L}$(Stm$_{LA}$)，都存在一个 $\mathscr{M}_{\mathcal{S}P}\in$ SFP，使得对于任意 $x \in$ S 和 $\omega \in$B$^{\mathbb{N}}$,

$$P(x,\omega) = \mathscr{M}_{\mathcal{S}}{}^{P}(x,\omega).$$

此外，如果 P 是多项式时间的，那么 $\mathscr{M}_{\mathcal{S}P}$ 也是多项式时间的。

证明概要。该构造依赖于通过多带按需 STM 实现 SIFP$_{\mathrm{LA}}$ 中的程序：该 STM 使用一条磁带存储每个寄存器的值，另用一条磁带存储求值表达式时得到的部分结果，再用一条磁带存储 ω。我们将用于存储表达式求值结果的磁带记为 e。以下不变性质成立：

- 在每条磁带上，值都存储在读写头的正右侧，
- 最后一个求值表达式的结果存储在读写头正右侧的磁带上 e 。

SIFP 表达式的值可以使用磁带 e 计算。[20] 所有操作都可以在不消耗预言机带上任何字符的情况下实现，且所需时间与表达式值的大小呈线性关系。我们为每条语句 s_i 分配一组机器状态： $q^I_{s_1}$、 $q^1_{s_i}$、……、 $q^F_{s_i}$。特别地，RandBit() 语句的实现方式是消耗磁带上的一个字符，并将其值复制到对应于寄存器R的磁带上。

此外，若假设 P 是多项式时间的，则在模拟每条语句之后，有：

- 与寄存器对应的第一条磁带上非空白部分的长度有多项式上界，因为其内容恰好是 P 的寄存器内容；根据其多项式时间复杂度这一假设，这些内容的长度有多项式上界，
- 与寄存器对应的所有磁带的读写头都指向其中所含字符串最左侧的符号。

众所周知，将多项式时间 TM 的磁带数量减少会带来时间上的多项式开销。因此，我们得出结论：多项式时间多带按需 STM 可以归约为多项式时间规范按需 STM。证明至此结束。 □

接下来需要证明，每个按需 STM 都可以归约为一个等价的 STM。

引理 B.9. 对于每个 M S $= \langle \mathrm{Q}\ \Sigma, \delta, q_0\rangle \in \mathrm{SFP}_{OD}$，机器 M S $' = \langle \mathrm{Q}\ \Sigma, H(\delta)\ q_0\rangle \in$ SFP 满足：对于每个 $n \in \mathbb{N}$ 以及 M S$\langle \sigma, q, \tau, \eta\rangle$ 的配置，并且对于每个 $\sigma', \tau' \in \mathrm{S}$ $q \in \mathrm{Q}$， $\mu(\{\omega \in \mathrm{B}^{\mathbb{N}} \mid (\exists \omega')\langle \sigma, q, \tau, \omega\rangle \triangleright^n_\delta \langle \sigma', q', \tau', \omega'\rangle\}) = \mu(\{\xi \in \mathrm{B}^{\mathbb{N}} \mid (\exists \xi')\langle \sigma, q, \tau, \xi\rangle \triangleright^n_{H(\delta)} \langle \sigma', q', \tau', \xi'\rangle\})$。

证明概要。即使在这种情况下，证明也依赖于一种归约。具体来说，我们证明，给定一个按需 STM，可以构造一个与其等价的 STM。直观地说，从按需 STM 到普通 STM 的编码，会对该 STM 的转移函数 δ 进行处理，将每个不会导致预言机带移动的转移（即标记为 $\natural$ 的转移）替换为两个不同的转移，其中 $\natural$ 分别替换为 0 和 1。这使得生成的机器执行相同的转移，同时将预言机带上的读写头向右移动。我们还定义了从按需 STM 到规范 STM 的编码如下：

$$H := \langle \mathbf{Q}, \Sigma, \delta, q_0\rangle \to \left\langle \mathbf{Q}, \Sigma, \bigcup \Delta_H(\delta), q_0\right\rangle.$$

[20]具体来说，我们通过对表达式语法进行归纳法来证明这一点。(1) 每次访问存储在寄存器中的值时，都是将相应磁带的内容复制到 e，这是一项简单操作（由上述不变性质可知）。(2) 连接——即 $f.0$ 和 $f.1$ ——通过在 e末尾添加一个字符来实现，其中 e包含 f的值。(3) 二元表达式并非平凡操作。由于两个操作数中有一个是寄存器标识符，机器可以直接将 e与对应于该标识符的磁带进行比较，并用比较结果替换 e 的内容；在所有情况下，比较结果都是 0 或 1。更多细节请参见 [5]。

其中 Δ_H 是,

$$\begin{aligned}
\Delta_H\big(\langle p, c_r, \mathbb{0}, q, c_w, d\rangle\big) &:= \{\langle p, c_r, \mathbb{0}, q, c_w, d\rangle\} \\
\Delta_H\big(\langle p, c_r, \mathbb{1}, q, c_w, d\rangle\big) &:= \{\langle p, c_r, \mathbb{1}, q, c_w, d\rangle\} \\
\Delta_H\big(\langle p, c_r, \natural, q, c_w, d\rangle\big) &:= \{\langle p, c_r, \mathbb{0}, q, c_w, d\rangle, \langle p, c_r, \mathbb{1}, q, c_w, d\rangle\}.
\end{aligned}$$

□

B.3.3 从 $\mathcal{POR}$ 到 SFP

由此我们完成了关于 $\mathcal{POR}$ 与 SFP 的证明。

命题 B.10（从 $\mathcal{POR}$ 到 SFP）。对于任意 $f : \mathsf{S}^k \times \mathsf{O} \to \mathsf{S} \in \mathcal{POR}$，存在一个函数 $f^\star : \mathsf{S}^k \times \mathsf{B}^{\mathbb{N}} \to \mathsf{S}$，使得对于所有 $\sigma_1, \ldots, \sigma_k, \tau \in \mathsf{S}$,

$$\mu\big(\{\omega \in \mathbb{B}^{\mathbb{N}} \mid f(\sigma_1, \ldots, \sigma_k, \omega) = \tau\}\big) = \mu\big(\{\eta \in \mathbb{0} \mid f^\star(\sigma_1, \ldots, \sigma_k, \eta) = \tau\}\big).$$

证明。由引理 B.6、引理 B.7、命题 B.8 和引理 B.9 可直接得出。

□