arXiv:2305.01755v1 [cs.LO] 2 May 2023

概率守卫 KAT 模去互模拟等价：完备性与复杂度

Wojciech Różowski ！英国伦敦大学学院计算机科学系

Tobias Kappé ！荷兰海尔伦开放大学；
荷兰阿姆斯特丹大学信息、逻辑与计算研究所（ILLC）

Dexter Kozen ！˘
美国纽约州伊萨卡康奈尔大学计算机科学系

Todd Schmid ！˘
伦敦大学学院计算机科学系，英国

Alexandra Silva ！˘
康奈尔大学计算机科学系，美国纽约州伊萨卡

摘要

我们介绍了带测试的概率守卫 Kleene 代数（ProbGKAT），这是 GKAT 的扩展，允许对具有概率分支的无解释命令式程序进行推理。我们以一类特殊的概率自动机为基础给出了其操作语义。我们给出了 ProbGKAT 表达式互模拟等价的健全且完备的 Salomaa 风格公理化。最后，我们展示了可以通过一种通用的划分细化算法，在 $O(n^3 \log n)$ 时间内判定 ProbGKAT 表达式的互模拟等价性。

2012 ACM 学科分类 计算理论 → 程序推理

关键词和短语 带测试的克莱尼代数、程序等价、完备性、余代数

范畴 赛道 B：自动机、逻辑、语义与程序设计理论

资助 本研究部分得到了欧洲研究委员会资助项目 Autoprobe（编号：101002697；Różowski、Schmid 和 Silva）、欧盟地平线2020研究与创新计划下的玛丽·斯克沃多夫斯卡-居里资助项目 VERLAN（编号：101027412；Kappé），以及美国国家科学基金会资助项目 CCF-2008083（Kozen）的支持。

1 引言

随机化是高效算法、密码协议和随机模拟设计中的一项重要特性 [10]。举一个简单的随机化示例，设想模拟一个三面骰子 [70]。至少有两种方法可以实现这一点：

- 参考实现可以使用一枚公平硬币和一枚偏置硬币，后者落在 `heads`上的概率为$\frac{1}{3}$：先抛偏置硬币。如果落在 `heads`上，则返回；否则抛公平硬币，如果落在`heads` 上则返回，否则返回。另一种做法是连续抛两次公平硬币：如果结果是`heads-heads`，则返回；如果是 `heads-tails`，则返回；如果是 `tails-heads`，则返回；如果是 `tails-tails`，则重复此过程 [40]。

这些程序可以用函数 `flip`(p) 表示，该函数以概率 p 返回 `true` (`heads`)，并以概率 $1-p$ 返回 `false` (`tails`)，见图1。如果我们能够证明这些程序等价，那么就可以确定它们实现了相同的分布。

本文介绍概率 GKAT（ProbGKAT），这是一种基于带测试的守卫 Kleene 代数（GKAT）[45, 64, 59] 的语言，并增添了用于推理此类随机化程序的额外构造。GKAT 的定律允许我们对具有确定性控制流的未解释程序的等价性进行推理，其控制流以布尔

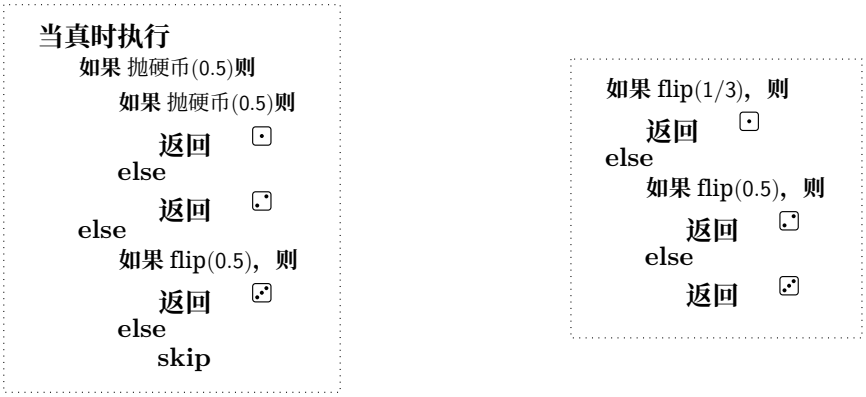


图1 左侧是 Knuth-Yao 过程，使用两次公平硬币投掷来模拟三面骰子。右侧是三面骰子的直接实现（注意，第一个 else 分支的概率为 $\frac{2}{3}$，因此 both 和 are 以 $\frac{1}{3}$ 的概率返回）。

分支（`if-then-else`）和循环（`while-do`）构造的形式表示。GKAT 配备了基于自动机理论的操作语义、近线性判定过程，以及用于推理表达式的轨迹等价 [64] 和互模拟等价 [59] 的完备公理系统；这些内容均受到 Salomaa 的克莱尼代数公理化 [58]的启发。

ProbGKAT 在 GKAT 的基础上扩展了三种新的语法构造：（1）概率选择算子，表示基于（可能带偏置的）硬币翻转进行分支；（2）概率循环算子，表示广义伯努利过程；以及（3）返回值，使得程序能够实现类似于命令式编程中 `return` 语句的有限形式的非局部控制流。

本文主要关注 ProbGKAT 表达式的互模拟等价公理化问题。我们以一个用于推理 GKAT 表达式互模拟等价的推理系统为基础 [59], ，该系统包含对 Salomaa 的 Kleene 星公理化 [58] 的推广，称为解唯一性公理（UA）；在进程代数领域中，它也被称为递归规范原则（RSP） [11]。在同时存在布尔守卫分支和概率分支的情况下，公理化变得复杂得多。除了添加描述概率选择和概率循环行为的直观规则外，我们还添加了用于刻画这两类分支与循环构造结合时相互作用的公理。此外，在 ProbGKAT 中，证明 UA 的可靠性变得极具挑战性。为此，我们利用操作模型的拓扑结构，即与互模拟等价相关联的行为伪度量。尽管难度大幅提升，我们的完备性证明仍采用了与 GKAT 模关于互模拟等价时类似的策略 [59]。

我们的主要贡献如下。

- 我们为 ProbGKAT 程序提供了操作语义，该语义依赖于一种同时具有布尔守卫转移和概率转移的自动机（第3节）。我们通过改造马尔可夫链互模拟等价的流网络刻画，对
- 这类自动机的双模拟进行了具体刻画 [36, 9]（第4节）。我们给出了 ProbGKAT 表达式双模拟等价的 Salomaa 风格公理化，并证明其可靠且完备（第5节和第6节）。我们证
- 明，当测试数量固定时，使用余代数划分细化 [20, 73] ，可以在$\mathcal{O}(n^3 \log n)$ 时间内高效判定 ProbGKAT 表达式的互模拟等价，其中 n 是待比较程序的总规模（第7节）。
-

e, f ∈ Exp ::=	p ∈ 动作集	do p
	| b ∈ BExp	断言 b
	| e +$_b$ f	如果 b则 e 否则 f
	| e ; f	
	| $e^{(b)}$	当b 执行 e
	| v ∈输出	return v
	| e ⊕$_r$ f	如果 flip(r)，则执行 e，否则执行 f
	| $e^{[r]}$	当 flip(r) 时，执行 e

图 2 ProbGKAT 的语法。

我们在第 2 节定义 ProbGKAT 的语法。第 8 节综述相关工作；结论和后续工作见第 9 节。证明见附录。

2 语法

ProbGKAT 具有双排序语法，由一个表达式集合 Exp 构成，其中包含一个BExp 布尔断言 或测试集合。对于固定的有限原始测试集合 T，测试的语法记为 BExp，并由以下文法生成

$$b, c \in \mathrm{BExp} ::= 0 \mid 1 \mid t \in \mathsf{T} \mid b + c \mid bc \mid \bar{b}$$

这里，0 和 1 分别表示假和真，$\bar{\cdot}$ 表示否定，$+$ 表示析取，并置表示合取。令 $\equiv_{\mathrm{BA}}$ 表示 BExp中的布尔等价。蕴涵是 BExp 上的一个预序，定义为 $b \leq_{\mathrm{BA}} c \iff b + c \equiv_{\mathrm{BA}} c$。BExp 关于 $\equiv_{\mathrm{BA}}$ 的商集是生成元集合 T 上的自由布尔代数，其中蕴涵——$[b]_{\equiv_{\mathrm{BA}}} \leq [c]_{\equiv_{\mathrm{BA}}} \iff b \leq_{\mathrm{BA}} c$——是一个偏序，其最小元和最大元分别为 0 和 1 的等价类。该偏序中的极小非零元素称为原子，我们将使用 At 表示原子集。对于固定的原子动作集 Act 和返回值集 Out， Exp ProbGKAT 表达式的集合由图 2 中的文法定义。

GKAT 的语法由图 2 中的前五种情况所涵盖，因此它是 ProbGKAT 的一个真子片段。这里引入了三种新的结构：返回值、概率选择和概率循环。返回值的行为类似于命令式程序中的返回语句，引入了一种非局部控制流形式。概率选择 $e \oplus_r f$ 会抛掷一枚偏置为 $r \in [0,1]$ 的偏置硬币，并根据结果，以 r 的概率执行 e，以 $1-r$ 的概率执行 f。概率循环 $e^{[r]}$ 同样以抛掷一枚偏置硬币开始，并根据结果，要么执行 e 并重新开始（概率为 r），要么终止（概率为 $1-r$）。概率循环可以被视为一种广义伯努利过程。

▶ **例 1**。 回顾引言中的两个程序（图1）：一个直接实现三面骰子，另一个用公平硬币模拟三面骰子。我们可以使用三个输出值 、 和 来表示三面骰子的可能结果。第一个程序是无限 while 循环 f $= g^{(1)}$，其中循环体为 g $= (\oplus_{\frac{1}{2}}) \oplus_{\frac{1}{2}} (\oplus_{\frac{1}{2}} 1)$。在 f 中， 表示 heads-heads，是 heads-tails，是 tails-heads，而 tails-tails 则提示重新投掷。第二个程序将 ProbGKAT 表达式 $e = \oplus_{\frac{1}{3}} (\oplus_{\frac{1}{2}})$ 编码为程序。

3 操作语义

在本节中，我们将正式介绍 ProbGKAT 自动机，即 ProbGKAT 表达式的操作模型。我们通过受 Brzozowski 导数启发的小步语义，将每个表达式与一个 ProbGKAT 自动机相关联 [14]。正如我们将看到的，最大的难点在于概率循环的语义。在给出小步语义之前，我们先介绍所需的概率分布记号和运算。

预备定义。 函数 $\nu\colon X \to [0,1]$ 称为 X 上的（概率）分布，如果它满足 $\sum_{x\in X}\nu(x) = 1$。若 $\sum_{x\in X}\nu(x) \le 1$，则称 ν 为次概率分布或次分布。本文中的每个（次）分布 ν 都是有限支撑的，这意味着集合 $\mathsf{supp}(\nu) = \{x \in X \mid \nu(x) > 0\}$ 是有限的。给定 $A \subseteq X$，我们定义 $\nu[A] = \sum_{x\in A}\nu(x)$。由于只有有限多个加数具有非零概率，因此该和是良定义的。

我们用 $\mathsf{D}_\omega(X)$ 表示集合 X 上有限支撑概率分布的集合。函数 $f\colon X \to Y$ 可以提升为分布之间的映射 $\mathsf{D}_\omega(f)\colon \mathsf{D}_\omega(X) \to \mathsf{D}_\omega(Y)$，定义为 $\mathsf{D}_\omega(f)(\nu) = \nu[f^{-1}(y)]$。给定 $x \in X$，其狄拉克 δ 分布为分布 δ_x；其中 $\delta_x(y)$ 在 $x = y$ 时等于 1，否则等于 0。给定 $f\colon X \to \mathsf{D}_\omega(Y)$，存在唯一的 $\bar{}$ 映射 $f^{\dagger}\colon \mathsf{D}_\omega(X) \to \mathsf{D}_\omega(Y)$，使得 $f = f^{\dagger} \circ \delta$，称为 f 的凸扩张，并且明确地 $\bar{}$ 定义为 $f^{\dagger}(\nu)(y) = \sum_{x\in X}\nu(x)f(x)(y)$。

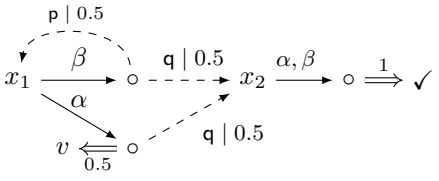
当 $\nu,\ \mu\colon X \to [0,1]$ 是概率分布且 $r \in [0,1]$ 时，我们将 $r\nu + (1-r)\mu$ 记作 ν 和 μ 的凸组合，它是由 $(r\nu + (1-r)\mu)(x) = r\nu(x) + (1-r)\mu(x)$ 给出的概率分布；该操作保持有限支撑集。

操作模型。 在操作层面，ProbGKAT 表达式表示迁移系统中的状态，该迁移系统称为 ProbGKAT 自动机。下文中，我们用 $2 = \{\checkmark\}$ 表示一个由两个符号组成的集合，分别表示拒绝和接受。

▶ **定义 2.** *A* ProbGKAT 自动机 是一个二元组 (X, β)，由状态集合 X 和一个 转移函数 $\beta\colon X \times$ 原子 $\to \mathsf{D}_\omega(2 +$ 输出 $+$ 动作集 $\times X)$ 组成。

ProbGKAT 自动机中的一个状态会将每个布尔原子 $\alpha \in \mathsf{At}$（用于捕获布尔变量的全局状态）与一个在若干可能结果上有限支撑的概率分布相关联。一种可能的结果是终止，它会结束执行，并发出成功（✓）或失败（ ），或者返回一个输出值（$v \in \mathsf{Out}$）。另一种可能的结果是推进，即执行一个动作（$\mathsf{p}^{\times} \in \mathsf{Act}$）并转换到一个状态。

▶ 示例 3。设 $X = \{x_1, x_2\}$，原子 $= \{\alpha, \beta\}$，动作集 $= \{\mathsf{p}, \mathsf{q}\}$，输出 $= \{v\}$。右侧给出了转移函数 $\tau\colon X \times$ 原子 $\to \mathsf{D}_\omega(2 +$ 输出 $+$动作集 $\times X)$ 的定义，而左侧则是 (X, τ) 的可视化表示。给定一个状态 $x \in X$ 和一个原子 $\alpha \in$ 原子，我们将其写作 $\tau(x)_\alpha$，而不是 $\tau(x)(\alpha)$。



$$\tau(x_1)_\alpha = \frac{1}{2}\delta_{(\mathsf{q},x_2)} + \frac{1}{2}\delta_v$$

$$\tau(x_1)_\beta = \frac{1}{2}\delta_{(\mathsf{p},x_1)} + \frac{1}{2}\delta_{(\mathsf{q},x_2)}$$

$$\tau(x_2)_\alpha = \tau(x_2)_\beta = \delta_\checkmark$$

我们用标注了（若干）原子的实线表示布尔守卫分支，用标注了原子动作和概率的虚线表示通往下一状态的概率标记转移，并用指向 $2 +$Out 中元素、且标注了概率的双横线箭头表示导致终止或输出的概率转移。

以下同态和双模拟的概念描述了 ProbGKAT 自动机之间的保结构映射和关系。

▶ 定义 *4. ProbGKAT* 自动机（X、β）与（Y、γ）之间的同态是一个函数 $f\colon X \to Y$，满足对所有 $x \in X$ 和 $\alpha \in$，原子 $o \in 2+$ 属于输出集，$\gamma\ (f\ (x)\ )\ _{\alpha}\ (o)\ = \beta\ (x)\ _{\alpha}\ (o)$ 。*2.* 对任意（$p\ y$）属于动作集 $\in \times Y$，$\gamma\ (f\ (x)\ )\ _{\alpha}\ (p\ y)\ = \beta\ (x)\ _{\alpha}[\{p\} \times f^{-1}\ (y)\ ]$

▶ 定义 *5.* 设（X、β）和（Y、γ）是 *ProbGKAT* 自动机，且 $R \subseteq X \times Y$ 是一个关系。R 是一个双模拟，当且仅当存在一个转移函数 $\rho\colon R \times$ 原子 $\to D_{\omega}$（$2+$ 输出集 $+$ 动作集 $\times R$），使得投影映射 $\pi_1\colon R \to X$ 和 $\pi_2\colon R \to Y$ 分别定义为 $\pi_1\ (x,\ y)\ = x$ 和 $\pi_2\ (x,\ y)\ = y$，并且它们分别是从（R、ρ）到（X、β）以及（Y、γ）的同态。

▶ 备注 6。定义 4 和 5 是对 ProbGKAT 自动机余代数理论的直接翻译（见附录 A）。余代数在我们的证明中发挥着核心作用，但为便于阐述，本文正文中并未涉及余代数。

Brzozowski 构造。 ProbGKAT 表达式可以赋予一种操作语义，其形式为 ProbGKAT 自动机 $\partial\colon \mathtt{Exp} \times \mathtt{At} \to \mathcal{D}_{\omega}(2 + \mathtt{Out} + \mathtt{Act} \times \mathtt{Exp})$。我们称之为*Brzozowski* 导数，因为它令人联想到 Brzozowski [14]针对正则表达式和确定有限自动机提出的类似构造。

给定 $\alpha \in$ 原子、e、$\mathsf{f} \in \mathtt{Exp}$、$\mathsf{b} \in \mathtt{BExp}$、$v \in \mathtt{Out}$、$r \in [0,1]$以及 $\mathsf{p} \in \mathtt{Act}$，我们定义

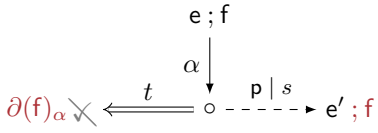
$$\partial(\mathsf{b})_\alpha = \begin{cases} \delta_{\checkmark} & \alpha \leq_{\mathtt{BA}} \mathsf{b} \\ \delta_{\text{✗}} & \alpha \leq_{\mathtt{BA}} \overline{\mathsf{b}} \end{cases} \qquad \partial(\mathsf{e} +_{\mathsf{b}} \mathsf{f})_\alpha = \begin{cases} \partial(\mathsf{e})_\alpha & \alpha \leq_{\mathtt{BA}} \mathsf{b} \\ \partial(\mathsf{f})_\alpha & \alpha \leq_{\mathtt{BA}} \overline{\mathsf{b}} \end{cases}$$

$$\partial(v)_\alpha = \delta_v \qquad \partial(\mathsf{p})_\alpha = \delta_{(\mathsf{p},1)} \qquad \partial(\mathsf{e} \oplus_r \mathsf{f})_\alpha = r\partial(\mathsf{e})_\alpha + (1-r)\partial(\mathsf{f})_\alpha$$

顺序复合和循环的导数定义如下。$\mathsf{b} \in \mathtt{BExp}$ 的出边取决于输入原子 $\alpha \in$At 是否满足 b：若满足，则以概率 1 输出 ✓ (成功)；否则以概率 1 输出 (中止)。守卫选择 $\mathsf{e} +_{\mathsf{b}} \mathsf{f}$ 的出边由 e 中标记为满足 b 的原子的出边，以及 f 中标记为满足 b 的 $\overline{\text{出边}}$组成（与 GKAT 中相同）。对于任意输入原子，输出值$v \in$Out 都以概率 1 返回值 v。原子动作 $\mathsf{p} \in$Act 对任意输入原子都发出 p，并转移到表达式 1。概率选择 $\mathsf{e} \oplus_r \mathsf{f}$ 的出边由 e 的出边（概率按 r 缩放）和 f 的出边（概率按 $1-r$ 缩放）组成。

顺序复合 $\mathsf{e}\,;\mathsf{f}$ 的行为更为复杂。我们需要考虑 e 可能以某个概率 t 接受给定的输入原子 α，在这种情况下，f 中标记为 α 的出边将计入 $\mathsf{e}\,;\mathsf{f}$ 的出边。形式上，我们写作 $\partial(\mathsf{e}\,;\mathsf{f})_\alpha = \partial(\mathsf{e})_\alpha \lhd_\alpha \mathsf{f}$，其中给定 $\alpha \in \mathsf{At}$ 和 $\mathsf{f} \in \mathtt{Exp}$，我们将 $(- \lhd_\alpha \mathsf{f}) : \mathcal{D}_{\omega}(2 + \mathtt{Out} + \mathtt{Act} \times \mathtt{Exp}) \to \mathcal{D}_{\omega}(2 + \mathtt{Out} + \mathtt{Act} \times \mathtt{Exp})$ 定义为下文左侧所示的 $c_{\alpha,\mathsf{f}}\colon 2 + \mathtt{Out} + \mathtt{Act} \times \mathtt{Exp} \to \mathcal{D}_{\omega}(2 + \mathtt{Out} + \mathtt{Act} \times \mathtt{Exp})$ 的凸扩张。

$$c_{\alpha,\mathsf{f}}(x) = \begin{cases} \delta_x & x \in \{\text{✗}\} \cup \mathtt{Out} \\ \partial(\mathsf{f})_\alpha & x = \checkmark \\ \delta_{(\mathsf{p},\mathsf{e}';\mathsf{f})} & x = (\mathsf{p}, \mathsf{e}') \end{cases}$$

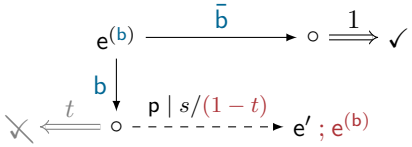


直观而言，$c_{\alpha,\ \mathsf{f}}$ 会重新引导从 e 出发的转移：接受（第二种情况）被 f 的行为取代，而转移到 e′ 的概率质量（第三种情况）

会重新分配给 $\mathsf{e}\,;\mathsf{f}$。输出$\{\,\}+\mathsf{Out}$ 中各元素的分支不受此操作影响。上方右侧给出了 $\mathsf{e}\,;\mathsf{f}$ 的导数所受影响的示意图。这里，我们假设 $\partial(\mathsf{e})_\alpha$ 可以以概率 s 执行到 e' 的 p-转移；下文对循环的导数作非正式描述时，也采用相同假设。

对于守卫循环，在定义 $\partial\left(\mathsf{e}^{(\mathsf{b})}\right)_\alpha$ 时，我们考虑三种情况。如果 $\alpha \le_{\mathsf{BA}} \bar{\mathsf{b}}$，则当前状态不满足循环守卫条件，可以跳过该循环：$\partial\left(\mathsf{e}^{(\mathsf{b})}\right)_\alpha = \delta_{\checkmark}$。如果 $\alpha \le_{\mathsf{BA}} \mathsf{b}$ 且 $\partial(\mathsf{e})_\alpha(\checkmark) = 1$，则调用循环体，但内部程序 e 不执行任何动作。我们将发散循环视为拒绝，因此在这种情况下，我们设置 $\partial\left(\mathsf{e}^{(\mathsf{b})}\right)_\alpha = \delta_{\lightning}$。如果 $\alpha \le_{\mathsf{BA}} \mathsf{b}$ 且 $\partial(\mathsf{e})_\alpha(\checkmark) < 1$，则程序执行循环体并重新开始，每次执行时都必须重新分配立即接受 $\partial(\mathsf{e})_\alpha(\checkmark)$ 的概率质量。因此，对于 $\alpha \le_{\mathsf{BA}} \mathsf{b}$ 和 $\partial(\mathsf{e})_\alpha(\checkmark) < 1$，$\partial(\mathsf{e}^{(\mathsf{b})})_\alpha$ 的定义如下所示（左侧）：当 e 拒绝或返回时，它也会拒绝或返回；当 e 转移到 e' 时，它转移到 $\mathsf{e}^{(\mathsf{b})}$；当 e 转移到 e' 时亦然。

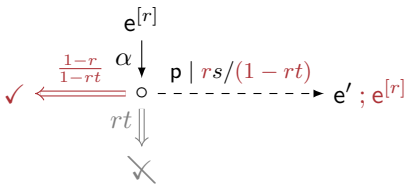
$$\partial(\mathsf{e}^{(\mathsf{b})})_\alpha(x) = \begin{cases} \frac{\partial(\mathsf{e})_\alpha(x)}{1-\partial(\mathsf{e})_\alpha(\checkmark)} & x \in \{\mathsf{x}\} \cup \mathsf{Out} \\ \frac{\partial(\mathsf{e})_\alpha(\mathsf{p},\mathsf{e}')}{1-\partial(\mathsf{e})_\alpha(\checkmark)} & x = \left(\mathsf{p}, \left(\mathsf{e}'\,;\mathsf{e}^{(\mathsf{b})}\right)\right) \\ 0 & \text{otherwise} \end{cases}$$



循环定义中所用的概率重新加权，源于将循环定义为分布上某个序关系下的最小不动点，这与 Stark 和 Smolka [68] 的做法类似。

最后，我们规定概率循环的行为。在特殊情形下，若 $\partial(\mathsf{e})_\alpha(\checkmark) = 1$ 且 $r = 1$，循环将不会终止；因此我们令 $\partial\left(\mathsf{e}^{[r]}\right)_\alpha = \delta_{\lightning}$。其他情况下，我们考察 $\partial(\mathsf{e})_\alpha$，为每个 $\alpha \in$ 原子构造 $\partial(\mathsf{e}^{[r]})_\alpha$。首先，我们确保循环可以以概率 $1-r$ 跳过。接下来，我们考虑 e 可能拒绝或返回一个值的情况，并修改产生结果的分支，将 $\mathsf{e}^{[r]}$ 加入以便下一步执行，这与守卫循环中的做法相同。剩余的概率质量为 $r\partial(e)_\alpha(\checkmark)$，即以一个可以跳过循环体的原子进入循环的概率。与守卫循环的情况一样，我们舍弃这种可能性，并将其重新分配给其余分支。$\partial(\mathsf{e}^{[r]})_\alpha$ 的最终定义如下方左侧所示。

$$\partial\left(\mathsf{e}^{[r]}\right)_\alpha(x) = \begin{cases} \frac{1-r}{1-r\partial(\mathsf{e})_\alpha(\checkmark)} & x = \checkmark \\ \frac{r\partial(\mathsf{e})_\alpha(x)}{1-r\partial(\mathsf{e})_\alpha(\checkmark)} & x \in \{\mathsf{x}\} \cup \mathsf{Out} \\ \frac{r\partial(\mathsf{e})_\alpha(\mathsf{p},\mathsf{e}')}{1-r\partial(\mathsf{e})_\alpha(\checkmark)} & x = \left(\mathsf{p}, \left(\mathsf{e}'\,;\mathsf{e}^{[r]}\right)\right) \\ 0 & \text{otherwise} \end{cases}$$



与之前一样，我们使用相同的约定，在右侧对上述概率循环语义作非正式的可视化呈现。

可达状态。对于任意 ProbGKAT 自动机 (X,β) 和任意 $x \in X$，我们用 $\mathsf{h}x\mathsf{i}_\beta$ 表示从 x 经由 β 可达的状态集合。显然，$(\mathsf{h}x\mathsf{i}_\beta,\beta)$ 是一个 ProbGKAT 自动机，并且是包含 x 的 (X,β) 的最小子自动机。典范包含映射 $(\mathsf{h}x\mathsf{i}_\beta,\beta) \to (X,\beta)$ 是一个 ProbGKAT 自动机同态。特别地，$(\mathsf{hei}_\partial,\partial)$ 是包含 e 的 $(\mathtt{Exp},\partial)$ 的最小子自动机。我们将这个子自动机称为 e 的小步语义。我们经常会滥用记号，将 $(\mathsf{hei}_\partial,\partial)$ 写作 hei_∂。

以下引理说明，每个 ProbGKAT 表达式都会生成一个有限自动机。

▶ **引理 7**。 对于所有 $\mathsf{e} \in \mathrm{Exp}$，$\mathit{hei}_\partial$ 都是有限的。事实上，状态的数量上界为 $\#(\mathsf{e})\colon\ \mathrm{Exp} \to \mathbb{N}$，其中 $\#(-)$ 递归定义如下

$$\#(\mathsf{b}) = 1 \quad \#(v) = 1 \quad \#(\mathsf{p}) = 2 \quad \#(\mathsf{e} +_\mathsf{b} \mathsf{f}) = \#(\mathsf{e}) + \#(\mathsf{f}) \quad \#(\mathsf{e} \oplus_r \mathsf{f}) = \#(\mathsf{e}) + \#(\mathsf{f})$$

$$\#(\mathsf{e}\,;\mathsf{f}) = \#(\mathsf{e}) + \#(\mathsf{f}) \quad \#\left(\mathsf{e}^{(\mathsf{b})}\right) = \#(\mathsf{e}) \quad \#\left(\mathsf{e}^{[r]}\right) = \#(\mathsf{e})$$

4 双模拟及其性质

验证给定的关系是否为双模拟（定义 5），需要在该关系上构造一个合适的转移结构。本节给出这种转移结构存在的充要条件。我们还将研究互模拟等价关系 $\sim$，即最大的双模拟 [57] 的性质。

双模拟等价的具体刻画。在 [36]，中，有一种对马尔可夫链之间双模拟的巧妙刻画，其证明运用了最大流最小割定理。将这项工作推广到 ProbGKAT 自动机，可以得到对双模拟等价关系的一种有用刻画，即同时也是等价关系的双模拟。

▶ **引理 8**。设 (X, β) 是一个ProbGKAT 自动机，且 $R \subseteq X \times X$ 是一个等价关系。 R 是双模拟，当且仅当且仅当对所有 $(x, y) \in R$ 以及 $\alpha \in$ 原子，
1. 对于所有 $o \in 2 +$ 输出、 $\beta(x)_\alpha(o) = \beta(y)_\alpha(o)$，以及 *2.* 对于所有等价类 $Q \in X/R$ 和所有 $p \in$ 动作集， $\beta(x)_\alpha[\{p\} \times Q] = \beta(y)_\alpha[\{p\} \times Q]$

该引理可以看作是 Larsen-Skou 双模拟等价 [46] 向带输出的系统的扩展。直观地说，如果对于任意原子 $\alpha \in$ 原子以及 $(x, y) \in R$，转移对任意输出赋予相同的概率，并且发出 p 后转移到任意给定等价类的概率对于 x 和 y 两者都相同，那么 R 就是一个双模拟等价。

互模拟等价及其性质。 给定一个关系 $R \subseteq X \times Y$，定义 $R^{-1} = \{(y,\ x) \mid x\ R\ y\}$，并给定 $A \subseteq X$，记作 $R(A) = \{y \in Y \mid x\ R\ y,\ x \in A\}$。$(X,\ \beta)$ 与 $(Y,\ \gamma)$ 之间的互模拟等价关系$\sim_{\beta,\ \gamma} \subseteq X \times Y$是以下算子的最大不动点 。

▶ **定义 9**。 设 (X, β) 和 (Y, γ) 为 ProbGKAT 自动机，且 $R \subseteq X \times Y$。我们定义算子 $\Phi_{\beta,\gamma}\colon 2^{X\times Y} \to 2^{X\times Y}$，使得当任意给定的 $\alpha \in$ 原子时，若 $(x, y) \in \Phi_{\beta,\gamma}(R)$，则
对于所有 $o \in 2 +$ 输出， $\beta(x)_\alpha(o) = \gamma(y)_\alpha(o)$；对于所有 $A \subseteq X$，以及所有 $p \in$ 动作集，$\beta(x)_\alpha[\{p\} \times A] \leq \gamma(y)_\alpha[\{p\} \times R(A)]$,；对于所有 $B \subseteq Y$ 和 $p \in$ 动作集， $\gamma(y)_\alpha[\{p\} \times B] \leq \beta(x)_\alpha[\{p\} \times R^{-1}(B)]$。从现在起，当上下文已明确所指的自动机时，我们将省略 Φ 的下标。

算子 $\Phi_{\beta,\gamma}$ 也可用于定义行为伪度量。设 (X, β) 为一个 ProbGKAT 自动机。关系细化链 是关系的一个带索引族 $\{\sim^{(i)}\}_{i\in\mathbb{N}}$，定义在 X 上，其定义如下： $\sim^{(0)} = X \times X$, $\sim^{(i+1)} = \Phi(\sim^{(i)})$。我们可以直观地将该链中连续的元素视为对互模拟等价的逐步逼近（另见 [32]）。

▶ **定理 10**。 设 (X, β) 是一个 ProbGKAT 自动机。对于任意 $x, y \in X$, $x \sim y$ 当且仅当对于所有 $i \in \mathbb{N}$，我们都有 $x \sim^{(i)} y$。

因此，如果 $x,\ y \in X$ 不是双模拟等价的，那么存在一个极大的 $i \in \mathbb{N}$ 使得 $x \sim^{(i)} y$。在第 6 节中，我们利用这一点为任意 ProbGKAT 自动机的状态定义一个伪度量。通俗地说，这使我们能够量化两个状态在多大程度上接近双模拟等价。

我们的主要目标是用一组等式定律为 ProbGKAT 表达式的互模拟等价建立公理化，并使用等式逻辑推理等价性。对于这样的公理化

表1 ProbGKAT 的公理化。图中，e、f、g $\in$ Exp、b、c $\in$ BExp, $v \in$ Out、p $\in$ Act 以及 $r, s \in [0,1]$。涉及概率除法的定律仅在分母不为零时适用。为简化记号，我们写作 E (e) $= 0$ 来表示对所有 $\alpha \in$ At，E (e)$_\alpha = 0$均成立。

守卫选择公理

(G1) $e +_b e \equiv e$

(G2) $e +_b f \equiv b\,;\ e +_b f$

(G3) $e +_b f \equiv f +_{\bar{b}} e$

(G4) $(e +_b f) +_c g \equiv e +_{bc} (f +_c g)$

分配公理

(D) $e \oplus_r (f +_b g) \equiv (e \oplus_r f) +_b (e \oplus_r g)$

序列公理

(S1) $1\,;\ e \equiv e$

(S2) $e\,;1 \equiv e$

(S3) $(e\,;f)\,;g \equiv e\,;(f\,;g)$

(S4) $0\,;e \equiv 0$

(S5) $(e +_b f);\ g \equiv e;\ g +_b f;\ g$

(S6) $(e \oplus_r f)\,;g \equiv e\,;g \oplus_r f\,;g$

(S7) $v\,;e \equiv v$

(S8) $b\,;c \equiv bc$

循环公理

(L1) $e^{(b)} \equiv e\,;e^{(b)} +_b 1$

(L2) $e^{[r]} \equiv e;\ e^{[r]} \oplus_r 1$

(L3) $(e +_c 1)^{(b)} \equiv$ 和$^{[1]}$

(L4) $e^{(1)}$

(L5) $$\frac{e \equiv (f \oplus_s 1) +_c g \qquad s > 0}{c;\ e^{(b)} \equiv c;\ \left(f\,;\ e^{(b)} +_b 1\right)}$$

(L6) $$\frac{e \equiv (f \oplus_s 1) +_c g}{c\,;e^{[r]} \equiv c\,;\left(f\,;e^{[r]} \oplus_{\frac{rs}{1-r(1-s)}} 1\right)}$$

概率选择公理

(P1) $e \oplus_r e \equiv e$

(P2) $e \oplus_1 f \equiv e$

(P3) $e \oplus_r f \equiv f \oplus_{1-r} e$

(P4) $(e \oplus_r f) \oplus_s g \equiv e \oplus_{rs} (f \oplus_{\frac{(1-r)s}{1-rs}} g)$

不动点规则

(F1) $$\frac{g \equiv e\,;g +_b f \qquad \mathrm{E}(e) = 0}{g \equiv e^{(b)}\,;f}$$

(F2) $$\frac{g \equiv e\,;g \oplus_r f \qquad \mathrm{E}(e) = 0}{g \equiv e^{[r]}\,;f}$$

归纳定义 E : Exp $\to$ 原子 $\to [0,1]$ 】【。

$$\mathrm{E}(p)_\alpha = \mathrm{E}(v)_\alpha = 0$$

$$\mathrm{E}(b)_\alpha = \begin{cases} 1 & \alpha \le_{\mathrm{BA}} b \\ 0 & \alpha \le_{\mathrm{BA}} \bar{b} \end{cases}$$

$$\mathrm{E}(e +_b f)_\alpha = \begin{cases} \mathrm{E}(e)_\alpha & \alpha \le_{\mathrm{BA}} b \\ \mathrm{E}(f)_\alpha & \alpha \le_{\mathrm{BA}} \bar{b} \end{cases}$$

$$\mathrm{E}(e \oplus_r f)_\alpha = r\mathrm{E}(e)_\alpha + (1-r)\mathrm{E}(f)_\alpha$$

$$\mathrm{E}(e\,;f)_\alpha = \mathrm{E}(e)_\alpha \mathrm{E}(f)_\alpha$$

$$\mathrm{E}\left(e^{(b)}\right)_\alpha = \mathrm{E}\left(\bar{b}\right)_\alpha$$

$$\mathrm{E}\left(e^{[r]}\right)_\alpha = \begin{cases} 0 & r = 1 \text{ 以及 } \mathrm{E}(e)_\alpha = 1 \\ \frac{1-r}{1-r\mathrm{E}(e)_\alpha} & \text{否则} \end{cases}$$

为了使其存在，互模拟等价需要同时满足等价关系，并且相对于 ProbGKAT 运算具有同余关系。任何 ProbGKAT 自动机上的最大双模拟都是一种等价关系 [57], ，但要证明其具有同余性，则需要采用归纳论证。

▶ **定理 11**。 (Exp, ∂) 上的最大双模拟相对于ProbGKAT 运算是一个同余关系。

5 公理化

我们将注意力转向基于模互模拟等价 GKAT [59] 的公理系统，对 ProbGKAT 表达式的互模拟等价进行公理化。首先，我们概述这些公理，并证明其可靠性。最后，我们证明这些公理足以将每个表达式分解为一种特定的语法范式，从而将表达式与其小步语义联系起来。完备性将在下一节讨论。

公理概述。表1包含这些公理，它们分为等式型（形式为 $e \equiv f$）和拟等式型（形式为 $e_1 \equiv f_1, \ldots e_n \equiv f_n \implies e \equiv f$）。表1还包含函数 $E(-)$ 的定义，该定义对于给不动点规则添加侧条件是必要的。我们将 $\equiv \subseteq \mathtt{Exp} \times \mathtt{Exp}$ 定义为满足这些公理的最小同余关系。

公理 G1–G4 继承自 GKAT，用于规定布尔保护选择的行为。P1–P4 可以视为它们在概率选择方面的对应公理。分配公理 D 表明，守卫选择对概率选择满足分配律，这反映了我们的操作模型如何处理这两类分支。

序列公理 S1–S8 大多继承自 GKAT。新增公理包括 S6，它讨论序列对概率选择的右分配性；以及 S7，它刻画了这一显然性质：在 `return` 语句之后执行的任何代码都不会执行。L1 和 L3 来自 GKAT，而 L2 是 L1 的概率循环对应形式，它通过递归展开刻画概率循环的语义。L4 将 `while(true)` 和 `while(flip(1))` 循环等同起来。F1 和 F2 受 Salomaa 公理 [58] 启发，分别在循环体无法立即终止的前提下，为 L1 和 L2 提供部分逆命题。循环体输出 ✓ 的概率为零这一性质，使用侧条件 $E(e) = 0$进行形式化书写；它可以视为 Salomaa 公理化 [58]中的空词性质 。

由此我们得到 L5 和 L6，它们描述了带守卫的循环和概率循环的行为，其中循环体的某些部分可能会被跳过。这些是拟等式型规则，但可以替换为等价的等式——参见注 49。L5 讨论的是表达式 e上的循环：在 $1 - s$ 的概率下不执行任何动作，前提是 c 成立。该规则指出，如果我们在 c 成立的条件下开始对 e 执行循环，那么要么 b 成立并执行 f，要么它不成立，循环便会被跳过。我们可以忽略 1 在 e 中的那一部分，原因是：如果选择了这条分支，那么在循环的下一次迭代中 c 仍然成立，因此程序将不得不再次在 f 和 1 之间进行概率选择。由于 $s > 0$，它最终几乎必然会选择概率分支 f 。

第二条规则 L6，是 L5 在概率选择情形下的对应规则。不过在这种情况下，选择1 也意味着要再进行一次概率实验，以确定是否需要再执行一次循环，其概率为 r。因此，如果在 c 成立的条件下开始对 e 执行循环，就会有更多概率质量转向跳过；结果是，循环终止前会执行若干次 1 。

关于互模拟等价的可靠性。 利用第4节中的刻画，我们可以证明， $\equiv$ 是 $(\mathtt{Exp}, \partial)$ 上的双模拟等价。证明见附录D。

▶ **引理 12**。 $\equiv$ 是 $(\mathtt{Exp}, \partial)$ 上的双模拟等价

我们立即得到，可证明等价包含于互模拟等价之中。

▶ **定理 13** (可靠性)。 对于所有 $e、f \in \mathtt{Exp}$，如果 $e \equiv f$，那么 $e \sim f$

等式推理示例。 由于我们的公理是可靠的，因此我们可以通过等式推理来处理 ProbGKAT 表达式，而无需手动构造双模拟。我们再次回顾图1中的算法。为了证明正确性，我们需要证明以下等价关系

例 1 中的表达式 e 和 $\mathsf{g}^{(1)}$ 如下：

$$
\begin{aligned}
\mathsf{g}^{(1)} &\equiv \left(\left(\boxdot \oplus_{\frac{1}{2}} \boxdot\right) \oplus_{\frac{1}{2}} \left(\boxdot \oplus_{\frac{1}{2}} 1\right)\right)^{(1)} && \text{(Def. of g)}\\
&\equiv \left(\left(\left(\boxdot \oplus_{\frac{1}{2}} \boxdot\right) \oplus_{\frac{2}{3}} \boxdot\right) \oplus_{\frac{1}{2}} 1\right)^{(1)} && \text{(See below)}\\
&\equiv \left(\left(\left(\left(\boxdot \oplus_{\frac{1}{2}} \boxdot\right) \oplus_{\frac{2}{3}} \boxdot\right) \oplus_{\frac{1}{2}} 1\right) +_1 0\right)^{(1)} && \text{(See below)}\\
&\equiv \left(\left(\boxdot \oplus_{\frac{1}{2}} \boxdot\right) \oplus_{\frac{2}{3}} \boxdot\right)^{(1)} && \text{(Axioms L5 and S1)}\\
&\equiv \left(\boxdot \oplus_{\frac{1}{3}} \left(\boxdot \oplus_{\frac{1}{2}} \boxdot\right)\right)^{(1)} && \text{(Axiom P4)}\\
&\equiv \left(\boxdot \oplus_{\frac{1}{3}} \left(\boxdot \oplus_{\frac{1}{2}} \boxdot\right)\right) ; \left(\boxdot \oplus_{\frac{1}{3}} \left(\boxdot \oplus_{\frac{1}{2}} \boxdot\right)\right)^{(1)} +_1 1 && \text{(Axiom L1)}\\
&\equiv \left(\boxdot \oplus_{\frac{1}{3}} \left(\boxdot \oplus_{\frac{1}{2}} \boxdot\right)\right) ; \mathsf{e}^{(1)} +_1 1 && \text{(Def. e)}\\
&\equiv \left(\boxdot \oplus_{\frac{1}{3}} \left(\boxdot \oplus_{\frac{1}{2}} \boxdot\right)\right) ; \mathsf{e}^{(1)} && \text{(See below)}\\
&\equiv \left(\boxdot ; e^{(1)} \oplus_{\frac{1}{3}} \left(\boxdot ; e^{(1)} \oplus_{\frac{1}{2}} \boxdot ; e^{(1)}\right)\right) && \text{(Axiom S6)}\\
&\equiv \left(\boxdot \oplus_{\frac{1}{3}} \left(\boxdot \oplus_{\frac{1}{2}} \boxdot\right)\right) && \text{(Axiom S7)}\\
&\equiv \mathsf{e} && \text{(Def. e)}
\end{aligned}
$$

在第二步中，我们利用了这样一个事实：对于所有 $\mathsf{e}_1, \mathsf{e}_2, \mathsf{e}_3 \in \mathtt{Exp}$ and $r, s \in [0,1]$ with $(1-r)(1-s) > 0$，都有 $\mathsf{e}_1 \oplus_r (\mathsf{e}_2 \oplus_s \mathsf{e}_3) \equiv (\mathsf{e}_1 \oplus_k \mathsf{e}_2) \oplus_l \mathsf{e}_3$,，其中 $k = \frac{r}{1-(1-r)(1-s)}$ and $l = 1-(1-r)(1-s)$。在第三步和第八步中，我们利用了这样一个事实：对于所有 e,$\mathsf{f} \in \mathtt{Exp}$，都有 $\mathsf{e} +_1 \mathsf{f} \equiv \mathsf{e}$。这两个等价关系都可由其他公理推出；详情请参见附录中的引理 50。

基本定理。 KA（以及 KAT、GKAT）语言中的每个表达式都可以根据其小步语义重构，直至 $\equiv$。这一性质通常称为（与微积分基本定理相类比，并沿用 *Rutten* 的术语）基本定理，在许多情境下都很有用，我们稍后也会用到。

▶ **定理 14**（基本定理）。 对于每个 $\mathsf{e} \in \mathtt{Exp}$，都有

$$\mathsf{e} \equiv \bigdotplus_{\alpha \in \mathsf{At}} \left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{e})_\alpha)} \partial(\mathsf{e})_\alpha(d) \cdot \mathtt{exp}(d) \right)$$

其中， $\mathtt{exp}$ 定义了一个函数 $2+$ 输出 $+$动作集 $\times \mathtt{Exp} \to \mathtt{Exp}$，其定义如下：

$$\mathtt{exp}(\times) = 0 \quad \mathtt{exp}(\checkmark) = 1 \quad \mathtt{exp}(v) = v \quad \mathtt{exp}(\mathsf{a}, \mathsf{f}) = \mathsf{a};\mathsf{f} \qquad (v \in \mathsf{Out}, \mathsf{a} \in \mathsf{Act} \ \textit{and}\ \mathsf{f} \in \mathtt{Exp})$$

证明见附录。我们使用一种广义的守卫式概率选择，适用于表达式的带索引集合，其定义见附录 D.2。

6 完备性

鉴于上一节提出的公理，一个自然的问题是：相对于双模拟等价而言，它们是否是完备的——也就是说，是否可以使用构成 $\equiv$ 的公理证明任意双模拟等价对是等价的。传统策略是在演算中发展方程组这一思想，并证明这些系统具有唯一的（最小）解

直至达到可证明等价。如果我们能够将所关注的表达式刻画为某个公共方程组的解（通常由关联它们的双模拟关系推导得出），那么解的唯一性便能保证它们等价。遗憾的是，这一过程的第一步，即证明方程组具有唯一解，并不能推广到 ProbGKAT（GKAT 也同样如此）。事实上，某些方程组甚至没有任何 解 [45, 59]；缺乏构造解的程序也使唯一性的证明更加困难。

相反，我们采用 Bergstra 和 Klop [11]，开创的方法，并将解的唯一性纳入公理化之中。实现这一点的唯一性公理（UA）是一种公理模式，也就是说，它是一个包含无限多个公理的模板，每个未知量的数量对应一个公理。对于只有一个未知量的情况，可以证明 F1 和 F2 都是 UA 的特例，而且还能给出一个候选解。

有了 UA，通往完备性的传统路线便可行。不过，在此之前，我们必须花些功夫妥善表述这一公理模式。此外，证明 UA 的可靠性也需要付出努力。这两项工作构成本节的大部分内容；最后，我们将推导出所需的完备性性质。

（Salomaa）方程组。首先，我们形式化定义 ProbGKAT 自动机的方程组这一概念。每个变量的约束将使用以下双排序语法构建，其中 X 是一个有限不定元集合。

$$e_1, e_2 \in \mathtt{Exp}(X) ::= p \mid e_1 +_{\mathsf{b}} e_2 \qquad (p \in \mathtt{PExp}(X), \mathsf{b} \in \mathtt{BExp})$$
$$p_1, p_2 \in \mathtt{PExp}(X) ::= \mathsf{f} \mid \mathsf{g}x \mid p_1 \oplus_r p_2 \qquad (\mathsf{f}, \mathsf{g} \in \mathtt{Exp}, x \in X, r \in [0,1])$$

▶ **定义 15.** *A* 个方程系统 是一个二元组$(X, \tau\colon X \to \mathtt{Exp}(X))$，由一个有限的不定元集合 X 和一个函数 $\tau\colon X \to \mathtt{Exp}(X)$组成。若对于所有 $x \in X$，在每个 $\tau(x)$中，所有形如$\mathsf{g}x$ 的子项都满足$\mathsf{E}(\mathsf{g}) = 0$，则称这样的系统为Salomaa系统。[1]

每个有限状态 ProbGKAT 自动机都会导出一个 Salomaa 方程系统。

▶ **定义 16.** 设(X, β) 是一个有限状态ProbGKAT 自动机。与(X, β) 相关联的方程系统是一个 *Salomaa* 系统 (X, τ)，其中 $\tau\colon X \to \mathtt{Exp}(X)$ 定义如下：

$$\tau(x) = \bigplus_{\alpha \in \mathsf{At}} \left(\bigoplus_{d \in \mathtt{supp}(\beta(x))_\alpha} \beta(x)_\alpha(d) \cdot \mathtt{sys}(d) \right)$$

其中 $\mathtt{sys}\colon 2 + \text{输出} + \text{动作集} \times \mathtt{Exp} \to \mathtt{PExp}(X)$ 定义如下：

$$\mathtt{sys}(\text{✗}) = 0 \quad \mathtt{sys}(\text{✓}) = 1 \quad \mathtt{sys}(v) = v \quad \mathtt{sys}(\mathsf{a}, x) = \mathsf{a}x$$

▶ **例17.** 在与示例 3 中的自动机相关联的系统里，τ 定义如下：

$$x_1 \mapsto (\mathsf{q}x_2 \oplus_{\frac{1}{2}} v) +_\alpha \Big((\mathsf{p}x_1 \oplus_{\frac{1}{2}} \mathsf{q}x_2) +_\beta 0 \Big) \qquad x_2 \mapsto 1 +_\alpha (1 +_\beta 0)$$

给定函数 $h\colon X \to \mathtt{Exp}$，它为 X 中的每个不定元赋值，我们可以如下对每个 $e \in \mathtt{Exp}(X)$ 归纳地导出一个 ProbGKAT 表达式 $h^\#(e)$：$h^\#(\mathsf{f}) = \mathsf{f}, h^\#(p_1 \oplus_r p_2) = h^\#(p_1) \oplus_r h^\#(p_2)$，$h^\#(\mathsf{g}x) = \mathsf{g}$；$h(x)$，$h^\#(e_1 +_{\mathsf{b}} e_2) = h^\#(e_1) +_{\mathsf{b}} h^\#(e_2)$。现在我们可以给出 Salomaa 系统的解这一概念。我们不要求等式两边严格相等，而是要求它们通过一个关系相关联，并将该关系留作参数，以便稍后实例化。

[1] 在进程代数中，[52], Salomaa 系统通常被称为受守卫的。为避免与（Prob）GKAT 中的布尔保护选择混淆，我们不采用后一种称呼。

12 模双模拟的概率守卫 KAT：完备性与复杂性

▶ **定义 18**。设 $R \subseteq \mathtt{Exp} \times \mathtt{Exp}$。系统$(X, \tau)$ 的一个解，在 R 意义下，指满足以下条件的映射h： $X \to \mathtt{Exp}$： 对于所有 $x \in X$，都有 $\big(h(x)\ h^{\#}(\tau(x))\big) \in R$。

▶ **例19**。 来自例 17 的系统的一个关于 $\equiv$ 的解将满足

$$h(x_1) \equiv (\mathsf{q}\,;h(x_2) \oplus_{\frac{1}{2}} v) +_\alpha \Big((\mathsf{p}\,;h(x_1) \oplus_{\frac{1}{2}} \mathsf{q}\,;h(x_2)) +_\beta 0\Big) \qquad h(x_2) \equiv 1 +_\alpha (1 +_\beta 0)$$

在这种情况下，选择 $h(x_1) = (\mathsf{p} +_\beta v)^{[\frac{1}{2}]}; \mathsf{q}$ 和 $h(x_2) = 1$ 符合这些约束。

▶ **例20**。 设 $\mathsf{r} \in [0,1]$。下方左侧的递归规范描述了一个程序 randAdd(m,r)，该程序接收一个整数 m 和一个偏置 r。只要 m 严格小于 10，该程序就会抛掷一枚偏置为 r 的硬币，以决定是将 m 加 1 后进行递归调用，还是终止。该递归规范可以被视为一个仅包含一个未知量的 Salomaa 系统；右侧的程序是其在 $\equiv$ 意义下的一个解。

```
定义 randAdd(m，r):
    如果m < 10 那么
        如果 翻转(r)则
            m++;
            randAdd(m，r)
        else
            skip
    else
        skip
```

```
当 翻转(r)时执行
    如果 m < 10 则
        m++;
        randAdd(m，r)
    else
        skip
```

截至 $\equiv$ 的解可以用定理 14 具体刻画。

▶ **定理 21.** 设 (X, β) 是一个有限状态 ProbGKAT 自动机。映射 $h: X \to \mathtt{Exp}$是与 $\equiv$ 相关的系统的一个解，当且仅当 $[-]_\equiv \circ h$ 是一个¯ ¯ProbGKAT 自动机同态，从 (X, β) 映射到 $(\mathtt{Exp}/\equiv, \partial)$。我们用 ∂表示 $\mathtt{Exp}/\equiv$ 上的唯一转移函数，它使商映射 $[-]_\equiv : \mathtt{Exp} \to \mathtt{Exp}/\equiv$ 成为一个ProbGKAT 自动机同态，从 $(\mathtt{Exp}, \partial)$ *[57, 命题 5.8]*。

解唯一性公理。 非正式地说，UA 通过规定 Salomaa 系统的解（若存在）唯一来扩展 $\equiv$ 。形式上，我们将 $\doteq \subseteq \mathtt{Exp} \times \mathtt{Exp}$ 定义为包含 $\equiv$的最小同余关系，并满足以下（拟等式型）公理:

$$\frac{(X,\tau) \text{ is a Salomaa system} \quad f, g : X \to \mathtt{Exp} \text{ are solutions of } (X,\tau) \text{ up to } \doteq}{f(x) \doteq g(x) \text{ for all } x \in X} \tag{UA}$$

F1 和 F2 是 UA 针对含一个变量的 Salomaa 系统的实例化。

行为伪度量。现在，我们将建立验证 UA 可靠性所需的理论。首先请注意，对于每个 ProbGKAT，我们都可以定义一个函数 $d_X : X \times X \to \mathbb{R}^+$:

$$d_X(x,y) = \begin{cases} 2^{-n} & n \text{ is maximal such that } x \sim^{(n)} y \\ 0 & \text{if } x \sim y \end{cases}$$

根据定理 10，上述定义良好，且是一个伪度量，具体而言:

▶ **定义 22.** 伪度量空间是一个二元组(X, d_X)，其中 $d_X\colon X \times X \to \mathbb{R}^+$ 是一个伪度量，这意味着对于所有 $x, y, z \in X$，都有

$$d_X(x,x) = 0 \qquad d_X(x,y) = d_X(y,x) \qquad d_X(x,z) \leq d_X(x,y) + d_X(y,z)$$

设 $k \in \mathbb{R}^+$。如果一个伪度量空间之间的映射 $f\colon X \to Y$，即从 (X, d_X) 到 (Y, d_Y)，则称其为 k-利普希茨 映射，如果对于所有 $x, y \in X$ $d_Y(f(x)\ f(y)) \leq k d_X(x, y)$。

行为伪度量在强意义上满足上述定义。

▶ **引理 23**。 对于每个 ProbGKAT 自动机，(X, β)，(X, d_X) 一个超伪度量空间，其意义是，对于所有 $x, y, z \in X$，我们有 $d_X(x, z) = \max\{d_X(x, y)\ d_X(y, z)\}$。

设 (X, d_X) 和 (Y, d_Y) 是伪度量空间。它们的积 是一个伪度量空间 $(X \times Y, d_{X\times Y})$，其中 $d_{X\times Y}$定义为 $d_{X\times Y}((x, y), (x', y')) = \max\{d_X(x, x')\ d_Y(y, y')\}$。容易证明，如果这两个伪度量空间都是超度量空间，那么它们的积也是超度量空间。下文中，在上下文足以明确时，我们将省略下标。

唯一性公理的可靠性。每个带有$X = \{x_1, x_2, \ldots, x_n\}$的 Salomaa 系统 $(X, \tau\colon X \to \mathsf{Exp}(X))$ 都会诱导一个映射 $\bar{\tau}\colon \mathsf{Exp}^n \to \mathsf{Exp}^n$。直观地说，该映射将一个向量 $\vec{\mathsf{e}} = (\mathsf{e}1, \ldots, \mathsf{e}_n)$ 作为输入，并生成一个新向量，其中第 i 个分量是 $\tau(x_i)$ 在将每个 x_j 替换为 e_j 后的求值。更形式化地，给定这个 $\vec{\mathsf{e}}$，我们定义 $e\colon X \to \mathsf{Exp}$，使得 $e(x_i) = \mathsf{e}_i$，并令 $\bar{\tau}(\vec{\mathsf{e}}) = \big((e^\# \circ \tau)(x_1) \ldots, (e^\# \circ \tau)(x_n)\big)$。

为了证明 UA 的可靠性，我们首先证明 $\bar{\tau}$ 在伪度量空间 (Exp^n, d) 上是 $1\ 2$-利普希茨的，其中 d 是由 (Exp, ∂) 的 n 重积所导出的度量。

▶ **引理 24**。 给定一个 *Salomaa* 系统 $(X, \tau\colon X \to \mathsf{Exp}(X))$，从伪度量空间 (Exp^n, d) 到自身的映射 $\bar{\tau}\colon \mathsf{Exp}^n \to \mathsf{Exp}^n$ 是$1\ 2$-利普希茨的。

最后，我们可以证明以下结论。

▶**引理 25.** UA 满足互模拟等价。

证明。设 (X, τ) 是一个 Salomaa 系统，其中 $X = \{x_1, \ldots, x_n\}$，并设 $f, g\colon X \to \mathsf{Exp}(X)$ 是该系统在 $\doteq$意义下的解。最后，设 $\vec{\mathsf{f}} = (f(x_1) \ldots, f(x_n))$，且 $\vec{\mathsf{g}} = (g(x_1) \ldots, g(x_n))$。假设前提由互模拟等价满足，即对所有 $1 \leq i \leq n$，$f(x_i) \sim (f^\# \circ \tau)(x_i)$，且 $g(x_i) \sim (g^\# \circ \tau)(x_i)$。换言之，我们有 $d(\bar{\tau}(\vec{\mathsf{f}})\ \vec{\mathsf{f}}) = 0$，且 $d(\bar{\tau}(\vec{\mathsf{g}})\ \vec{\mathsf{g}}) = 0$。设对于某个 $k \in \mathbb{R}^+$，有 $d(\bar{\tau}(\vec{\mathsf{f}})\ \bar{\tau}(\vec{\mathsf{g}})) = k$。那么，由于 d 是超度量，

$$d(\vec{\mathsf{f}}, \vec{\mathsf{g}}) = \max\{d(\vec{\mathsf{f}}, \bar{\tau}(\vec{\mathsf{f}})), d(\bar{\tau}(\vec{\mathsf{f}}), \vec{\mathsf{g}})\} = d(\bar{\tau}(\vec{\mathsf{f}}), \vec{\mathsf{g}}) = \max\{d(\bar{\tau}(\vec{\mathsf{f}}), \bar{\tau}(\vec{\mathsf{g}})), d(\bar{\tau}(\vec{\mathsf{g}}), \vec{\mathsf{g}})\} = k$$

根据引理 24，我们得到 $k = d(\bar{\tau}(\vec{\mathsf{f}})\ \bar{\tau}(\vec{\mathsf{g}})) \leq \frac{1}{2} d(\vec{\mathsf{f}}\ \vec{\mathsf{g}}) = \frac{1}{2} k$这意味着 $d(\vec{\mathsf{f}}\ \vec{\mathsf{g}}) = 0$。根据 (Exp, ∂) 上乘积伪度量的定义，对于所有 $1 \leq i \leq n$，我们有 $f(x_i) \sim g(x_i)$。因此，UA 的结论由互模拟等价满足。◀

由于上述引理和定理 13，$\equiv$ 的 UA 以及公理都包含于 $\sim$（Exp, ∂）上的最大双模拟中。回忆一下，$\doteq$ 是包含这些规则的最小同余关系。由于（Exp, ∂）上的 $\sim$ 是一个同余关系（定理 11），我们有 $\doteq$ 是可靠的。

▶ **定理 26 (带 UA 的可靠性）**。对于所有 $\mathsf{e}, \mathsf{f} \in \mathsf{Exp}$ 若 $\mathsf{e} \doteq \mathsf{f}$ 则 $\mathsf{e} \sim \mathsf{f}$。

完备性。 完成所有艰苦工作后，完备性的证明便可沿用证明 GKAT [64, 59] 时的同一思路。

▶ **定理 27** (完备性)。 对于所有 e,f ∈ Exp ， 若 e ∼ f ， 则 e ≙ f

证明。令 $R \subseteq \mathrm{Exp} \times \mathrm{Exp}$ 为具有转移结构 ρ 的双模拟： $R \times$At $\to$D$_\omega$(2+输出+动作集$\times R$)，它关联 ProbGKAT 自动机 $(\mathrm{hei}_\partial, \partial)$ 和 $(\mathrm{hfi}_\partial, \partial)$，且满足 $(\mathsf{e}, \mathsf{f}) \in R$。令 π_1, π_2 为从 (R, ρ) 到 $(\mathrm{hei}_\partial, \partial)$ 和 $(\mathrm{hfi}_\partial, \partial)$ 的投影同态。由于 hei_∂ 和 hfi_∂ 均为有限（由引理 7 可知），因此 R 也是有限的。

令 j, k 为 (Exp, ∂) 中 $(\mathrm{hei}_\partial, \partial)$ 和 $(\mathrm{hfi}_\partial, \partial)$ 的包含同态。我们可以构造两个同态 $[-]_\equiv \circ j \circ \pi_1$ 和 $[-]_\equiv \circ k \circ \pi_2$，它们从 (R, ρ) 映射到 $(\mathrm{Exp}/\equiv, \partial)$。根据定理 21， $j \circ \pi_1$ 和 $k \circ \pi_2$ 是与 (R, ρ) 关联的 Salomaa 系统在 $\equiv$ 意义下的解。由于 $\equiv$ 包含于 ≙，它们也立即是 ≙ 意义下的解。

由于 UA，我们有，对于所有 $(\mathsf{g}, \mathsf{h}) \in R$， $(j \circ \pi_1)(\mathsf{g}, \mathsf{h}) \equiv (k \circ \pi_2)(\mathsf{g}, \mathsf{h})$。因此，

$$\mathsf{e} \doteq j(\mathsf{e}) \equiv (j \circ \pi_1)(\mathsf{e}, \mathsf{f}) \equiv (k \circ \pi_2)(\mathsf{e}, \mathsf{f}) \equiv k(\mathsf{f}) \doteq \mathsf{f}$$ ◀

7 可判定性与复杂度

要判定 e ≙f，我们需要证明在 (Exp, ∂) 中的状态 e 和 f 之间存在双模拟。由于双模拟只需涉及可达状态，因此只需在 $\langle \mathsf{e}, \mathsf{f} \rangle_\partial$ 中寻找该双模拟；这是包含 e 和 f 的 (Exp, ∂) 的最小子自动机，同时也是$\langle \mathsf{e} \rangle_\partial$ 和 $\langle \mathsf{f} \rangle_\partial$ 的并集；根据引理 7，该自动机是有限的。因此，我们将重点放在单个有限ProbGKAT自动机内判定互模拟等价的问题上。

本节的分析得益于两项简化性断言。**1.** 为避免比较实数（无限精度）概率，我们在本节将 ProbGKAT表达式限制为有理数概率 $r \in [0, 1] \cap \mathbb{Q}$。这一限制与先前针对概率定义的算子兼容，因为这些算子都会保持有理性。**2.** 仅仅因为布尔不可满足性可以轻易地编码为测试语言中的内容，GKAT 本身的等价性就是 co-NP困难 [64], 。我们采用固定参数方法，假设 原子（即可能出现在转换上的原子集合）预先固定。

余代数划分细化。 我们采用划分细化 [37, 38, 55], ，通过从上方逐步逼近，在自动机上有效计算最大双模拟 。在划分细化的余代数 表示法中 [73], （我们将其具体化到当前场景），各种类型的自动机都编码为抽象图。更具体地说，一个自动机由两个映射 $o\colon X \to O$ 和 $\ell\colon X \to \mathcal{B}(L \times X)$ 编码，其中

- X 是一个节点 集合，用来表示自动机的（部分）状态；O 是每个节
- 点上的可观测值 集合；L 是一个集合，表示节点之间边的可能标签 ；
- $\mathcal{B}(L \times X)$ 是一个多重集，包含表示节点之间边 的有序对。

在编码满足若干相容性条件（此处省略）的前提下，余代数划分细化可得到一个$\mathcal{O}(n \log |X|)$算法，用于计算自动机上的最大双模拟，其中 $n = \sum_{x \in X} |\ell(x)|$ 表示自动机的边 数。

编码ProbGKAT 自动机。余代数划分细化为众所周知的转移类型提供了合适的编码方法，也提供了可靠地获取复合转移类型编码的方法 [73]。这些技术的细节超出了本文的讨论范围，但其基本思想相当直观：复合转移类型通过插入表示部分求值状态的合成节点来编码——这与我们的图示包含以 为标签的箭头所指向的中间节点颇为相似。

图示包含中间节点，它们是以 α 为标签的箭头的目标。更准确地说，编码后的 ProbGKAT 自动机（Q, t）的节点分为三种类型：
1. 自动机的每个状态都是一个节点；并且**2.** 每个“中间”状态（图中的小圆圈）都是一个节点；并且**3.** 每条概率边都会引出另一个节点。

第三类节点将图中的虚线箭头（同时标有概率和动作）分成两条箭头，每条箭头都标有一个值。

形式化地，我们选择 $X := Q + I + \mathsf{Act} \times Q$ 作为节点集，其中 $I := \{t(q)_\alpha : q \in Q, \alpha \in \mathsf{At}\}$。我们还令 $L := \mathsf{At} + \mathbb{Q} + \mathsf{Act}$。映射 $\ell : X \to \mathcal{B}(L \times X)$ 定义如下：[2]

$$\ell(x) := \begin{cases} \{\!|(\alpha, t(q)_\alpha) \mid \alpha \in \mathsf{At}|\!\} & x = q \in Q \\ \{\!|(d(\mathsf{p}, q), (\mathsf{p}, q)) \mid \mathsf{p} \in \mathsf{Act}, q \in Q|\!\} & x = d \in I \\ \{\!|(\mathsf{p}, q)|\!\} & x = (\mathsf{p}, q) \in \mathsf{Act} \times Q \end{cases}$$

换言之，ℓ 将第一类和第二类节点之间的边标记为原子，将第二类和第三类节点之间的边标记为概率，并将第三类和第一类节点之间的边标记为动作。

可观测量表示第二类节点为接受、拒绝或返回值所分配的概率。形式上，$O := 1 + \mathbb{Q}^{2+\mathsf{Out}}$，其中 $* \in 1$ 表示“无可观测值”，而来自 $\mathbb{Q}^{2+\mathsf{Out}}$ 的值为每个 $\xi \in 2 +$ 输出分配一个概率。然后，我们可以通过设置 $o(d)(\xi) := d(\xi)$（当 $d \in I$ 时），以及 $o(x) := *$（否则），来定义 $o : X \to O$。[3]

判定互模拟等价。 现在，我们可以利用上文给出的编码来判定互模拟等价。

▶**定理28。** 如果所有概率均为有理数且原子固定，则ProbGKAT 自动机(Q, t) 中状态的互模拟等价可在 $O(|Q|^2 |\text{动作集}| \log(|\text{动作集} \times Q|))$时间内判定。

P上界。 来自 [73] 的结果确保我们对 ProbGKAT自动机的编码可以e配备了适当的接口，使其算法能够判定等价性。

至于复杂度，我们通过计算参数，将他们的抽象复杂度结果具体化。节点数和边数很容易得到如下上界：

$$|X| = |Q| + |I| + |\mathsf{Act} \times Q| \leq |Q| + 2 \cdot |\mathsf{Act}| \cdot |Q|$$
$$n = \sum_{x \in X} |\ell(x)| \leq |Q| \cdot |\mathsf{At}| + |Q|^2 \cdot |\mathsf{Act}| + |Q| \cdot |\mathsf{Act}|$$

由于 At 是固定的，因此可得所声称的复杂度。 ◀

由此我们可以得出，ProbGKAT表达式的互模拟等价也是可判定的。

▶**推论 29.** 如果所有概率都是有理数，且原子集合固定，那么ProbGKAT 表达式e、f $\in$ Exp 的等价性可在 $O(n^3 \log n)$时间内判定，其中 $n = \#(\mathsf{e}) + \#(\mathsf{f})$。

证明。 根据引理 7，$\langle \mathsf{e}, \mathsf{f} \rangle_\partial$ 的大小至多为 n，不同动作 e 或 f 的数量也由上界 n 固定。由定理28即可得出该结论。 ◀

[2] 这里，$\{\!|- \mid -|\!\}$ 表示多重集构造，其中每个元素至多出现一次。[3] 如果严格遵循 [73] 中的余代数方法，第三类节点的可观测映射会略有不同；为便于呈现，我们在此简化了编码。

8 相关工作

我们的工作建立在 GKAT 的基础上。GKAT 是带测试的克莱尼代数（KAT）的一个严格确定性片段 [45] 。KAT 已用于多种验证任务，例如缓存控制 [17], 、编译器优化 [43], 、源到源转换 [3], 和网络属性 [2, 25, 24, 65,66, 72], ，并已推广为包含模糊逻辑 [26]。GKAT 允许对轨迹等价 [64] 和双模拟等价 [59], 进行 Salomaa 风格的 [58]公理化，而这两者都依赖于解唯一性公理；不依赖该公理的完备性仍是一个开放问题，不过最近 [39] 证明了 GKAT 的一个片段具有完备性。

模双模拟的 GKAT 和 Milner 对正则表达式的解释，都是参数化进程 框架 [61]的片段；由于对循环的处理不同，ProbGKAT 并非如此。唯一性公理最初由 Bergstra 和 Klop 提出，称为递归规范原则（RSP） [11] ，并用于进程演算的公理化中 [12]。他们完备性证明的一般思路与我们的相似，不过关键难点在于将其扩展到概率情形。

本文也建立在概率双模拟 [46,62, 21] 以及针对具有概率转移的系统的余代数方法 [19, 9, 21,67]这一广泛研究基础之上。具体而言，我们采用了双模拟等价的关系细化刻画 [69],、针对 ω-可达自函子的终余代数的自然度量 [8, 75], 、余代数完备性定理 [33, 63, 60] ，以及余代数的最小化算法 [73, 20, 74, 35]。进程代数领域对概率双模拟的公理化进行了广泛研究，其中包括 Bandini 和 Segala 提出的无递归进程代数 [7] ，以及 Stark 和 Smolka [68] 、Mislove、Ouqaknine 和 Worrell [53]提出的递归演算。Aceto、Ésik 和 Ingólfsdóttir [1] 通过为迭代理论 [13, 23] 扩充等式公理，给出了 Stark 和 Smolka 演算的另一种公理化。

概率克莱尼代数（pKA） [49] 放宽了 Kleene 代数的公理，以便对概率谓词变换器进行推理；其公理相对于 NFA [50]的模拟等价是完备的。pKA 还扩展了概率选择算子和并发原语 [51], ，但尚未研究该系统的完备性。ProbNetKAT [24, 66] 是一种基于 KAT、用于对网络中的概率效应进行推理的领域特定语言，其中包含概率选择算子；然而，对所得语言的公理化尚未进行研究。

9 结论与未来工作

我们提出了 ProbGKAT，这是一种用于对带有分支和循环的未解释程序进行推理的语言，同时支持布尔守卫和概率守卫。我们提供了一个基于自动机理论的操作模型，并刻画了这些自动机的互模拟等价。我们给出了互模拟等价的可靠且完备的公理化，该公理化依赖于解唯一性（UA）公理，并证明了互模拟等价可以在 $O(n^3 \log n)$ 时间内高效判定。

未来工作的一个自然起点，是探讨能否将 GKAT 更传统的语言语义推广到 ProbGKAT，并对其进行公理化。更广泛地说，我们希望研究比双模拟等价更宽松的 ProbGKAT 表达式等价概念，包括互模拟距离 [6] 这一概念，以及基于定量等式逻辑 [48, 4]对其进行公理化的可能性。

第二个方向涉及没有 UA 时的完备性问题，而这仍是（Prob）GKAT 中尚未解决的问题。鉴于近期关于 GKAT 无跳过片段在互模拟等价和轨迹等价下的完备性结果，我们有意研究 ProbGKAT 的无跳过

片段。 [39] 中的证明无法直接推广到 ProbGKAT，因为概率显然无法嵌入（1-自由）正则表达式中。

与 GKAT 类似，ProbGKAT 是严格确定性的，因此避免了将非确定性与概率选择相结合时已知的复杂问题 [36, 71, 27]。我们关注近期关于通过分配律 [34, 44] 结合多重集与概率的研究能否用于扩展我们的成果，使其涵盖非确定性。

ProbGKAT 只能表示未解释程序，因此无法用于推理涉及可变状态的程序。一个带状态的概率程序示例是波利亚罐模型 [47]。为 ProbGKAT 添加可变状态 [28] 的一种方法是添加假设 [16]。遗憾的是，添加假设可能导致不可判定性或不完备性 [41],，尽管某些形式的假设仍能保持完备性 [42, 22, 56]；探索这一问题是未来一项有趣的研究方向。

参考文献

1 Luca Aceto、Zoltán Ésik 和 Anna Ingólfsdóttir。概率双模拟等价的等式公理。载于 AMAST，第 239–253 页，2002年。 doi:10.1007/3-540-45719-4_17。 2 Carolyn Jane Anderson、Nate Foster、Arjun Guha、Jean-Baptiste Jeannin、Dexter Kozen、Cole Schlesinger 和 David Walker。NetKAT：网络的语义基础。载于 POPL，第 113–126 页，2014年。 doi:10.1145/2535838.2535862。 3 Allegra Angus 和 Dexter Kozen。带测试的克莱尼代数与程序图式学。技术报告 TR2001-1844，康奈尔大学，2001年 07 月。网址： https://hdl.handle.net/1813/5831。 4 Giorgio Bacci、Giovanni Bacci、Kim G. Larsen 和 Radu Mardare。马尔可夫链上互模拟距离的完备公理化。载于 CONCUR，第 21:1–21:14 页，2016年。 doi:10.4230/LIPIcs.CONCUR.2016.21。 5 Christel Baier。概率系统的算法验证方法。特许资格论文，曼海姆大学，1998年。 6 Paolo Baldan、Filippo Bonchi、Henning Kerstan 和 Barbara König。余代数行为度量。《逻辑方法与计算机科学》，14(3)，2018年。 doi:10.23638/LMCS-14(3:20)2018。 7 Emanuele Bandini 和 Roberto Segala。概率双模拟的公理化。载于 ICALP，第 370–381 页，2001年。 doi:10.1007/3-540-48224-5_31。 8 Michael Barr。良基集合论中的终余代数。《理论计算机科学》，114(2):299–315，1993年。 doi:10.1016/0304-3975(93)90076-6。 9 Falk Bartels、Ana Sokolova 和 Erik P. de Vink。概率系统类型的层次结构。载于 CMCS，第 57–75 页，2003年。 doi:10.1016/S1571-0661(04)80632-7。 10 Gilles Barthe 、 Joost-Pieter Katoen 和 Alexandra Silva （编）。《概率编程基础》。剑桥大学出版社，剑桥，2020年。 doi:10.1017/9781108770750。 11 Jan A. Bergstra 和 Jan Willem Klop。利用进程代数验证交替位协议。载于《软件系统规范与综合的数学方法》，LNCS 第 215 卷，第 9–23 页。施普林格，1985年。 doi:10.1007/3-540-16444-8_1。 12 Jan A. Bergstra 和 Jan Willem Klop。基于双模拟语义的进程理论。载于《并发逻辑与模型中的线性时间、分支时间和偏序》，LNCS 第 354 卷，第 50–122 页，1988年。 doi:10.1007/BFb0013021。 13 Stephen L. Bloom 和 Zoltán Ésik。《迭代理论——迭代过程的方程逻辑》。EATCS理论计算机科学专著。施普林格，1993年。 doi:10.1007/978-3-642-78034-9。 14 Janusz A. Brzozowski。正则表达式的导数。《《ACM杂志》》，11(4):481–494，1964年。doi:10.1145/321239.321249。 15 Stanley Burris 和 H. P. Sankappanavar。《普遍代数教程》。施普林格，1981年。网址： http://www.math.uwaterloo.ca/~snburris/htdocs/ualg.html。

16 Ernie Cohen。克莱尼代数中的假设。技术报告，Bellcore，1994年。 17 Ernie Cohen。克莱尼代数中的惰性缓存。技术报告，Bellcore，1994年。 18 G. B. Dantzig 和 D. R. Fulkerson。网络的最大流最小割定理，第 215–222 页。普林斯顿大学出版社，普林斯顿，1957年。 doi:10.1515/9781400881987-013。 19 Erik P. de Vink 和 Jan J. M. M. Rutten。概率转移系统的双模拟：一种余代数方法。《理论计算机科学》，221(1-2):271–293，1999年。 doi:10.1016/S0304-3975(99)00035-3。 20 Hans-Peter Deifel、Stefan Milius、Lutz Schröder 和 Thorsten Wißmann。通用划分细化与加权树自动机。载于 FM，第 280–297 页，2019年。 doi:10.1007/978-3-030-30942-8 18.21 Josée Desharnais。标记马尔可夫过程。博士论文，麦吉尔大学，1999年。 22 Amina Doumane、Denis Kuperberg、Damien Pous 和 Pierre Pradic。带假设的克莱尼代数。载于 FoSSaCS，第 207–223 页，2019年。 doi:10.1007/978-3-030-17127-8_12。 23 Calvin C. Elgot。单子计算与迭代代数理论。载于 H.E. Rose 和 J.C. Shepherdson（编），《逻辑讨论会 '73》，《逻辑与数学基础研究》第 80 卷，第 175–230 页。爱思唯尔，1975 年。 doi:10.1016/S0049-237X(08)71949-9。 24 Nate Foster 、Dexter Kozen、Konstantinos Mamouras、Mark Reitblatt 和 Alexandra Silva。概率 NetKAT。载于 ESOP，第 282–309 页，2016年。 doi:10.1007/978-3-662-49498-1_12。 25 Nate Foster、Dexter Kozen、Mae Milano、Alexandra Silva 和 Laure Thompson。NetKAT 的余代数判定程序。载于 POPL，第 343–355 页，2015年。 doi:10.1145/2676726.2677011。 26 Leandro Gomes、Alexandre Madeira 和 Luís Soares Barbosa。推广 KAT 以验证加权计算。《计算机科学年刊》，29(2):141–184，2019年。 doi:10.7561/SACS.2019.2.141。 27 Alexandre Goy 和 Daniela Petrisan。通过弱分配律结合概率选择与非确定性选择。载于 LICS，第 454–464 页，2020年。 doi:10.1145/3373718.3394795。 28 Niels Bjørn Bugge Grathwohl、Dexter Kozen 和 Konstantinos Mamouras。KAT + B！载于 CSL，第 44:1–44:10 页，2014年。 doi:10.1145/2603088.2603095。 29 H. Peter Gumm。余代数一般理论要素，2000年。网址：https://www.mathematik.uni-marburg.de/~gumm/Papers/Luatcs.pdf。 30 H. Peter Gumm 和 Tobias Schröder。由弱极限保持函子产生的余代数结构。载于 CMCS，第 111–131 页，2000年。 doi:10.1016/S1571-0661(05)80346-9。 31 H. Peter Gumm 和 Tobias Schröder。有界类型余代数。《数学结构与计算机科学》，12(5):565–578，2002年。 doi:10.1017/S0960129501003590。 32 Matthew Hennessy 和 Robin Milner。关于观察非确定性与并发。载于 ICALP，第 299–309 页，1980年。 doi:10.1007/3-540-10003-2_79。 33 Bart Jacobs。确定自动机、正则表达式与语言的双代数综述。载于《代数、意义与计算：献给 Joseph A. Goguen 的论文集，庆祝其 65 岁生日》，第 375–404 页，2006年。 doi:10.1007/11780274_20。 34 Bart Jacobs。从分布上的多重集到多重集上的分布。载于 LICS，第 1–13 页，2021年。 doi:10.1109/LICS52264.2021.9470678。 35 Jules Jacobs 和 Thorsten Wißmann。快速余代数互模拟等价最小化。载于 POPL，第 1514–1541 页，2023年。 doi:10.1145/3571245。 36 Claire Jones。概率非确定性。博士论文，爱丁堡大学，英国，1990年。网址： https://hdl.handle.net/1842/413。 37 Paris C. Kanellakis 和 Scott A. Smolka。CCS 表达式、有限状态进程及三个等价性问题。载于 PODC，第 228–240 页，1983年。 doi:10.1145/800221.806724。 38 Paris C. Kanellakis 和 Scott A. Smolka。CCS 表达式、有限状态进程及三个等价性问题。《信息与计算》，86(1):43–68，1990年。 doi:10.1016/0890-5401(90)90025-D。

39 Tobias Kappé、Todd Schmid 和 Alexandra Silva。带测试的无跳转守卫 Kleene 代数的完备推理系统。载于 ESOP，第 309–336 页，2023年。 doi:10.1007/978-3-031-30044-8_12。40 Donald E. Knuth 和 Andrew C. Yao。非一致随机数生成的复杂度。载于《算法与复杂性：新方向与近期成果》，1976年。41 Dexter Kozen。Kleene 代数推理的复杂度。信息与计算，179(2):152–162，2002年。 doi:10.1006/inco.2001.2960。42 Dexter Kozen 和 Konstantinos Mamouras。带方程的克莱尼代数。载于 ICALP（第二部分），第 280–292 页，2014年。 doi:10.1007/978-3-662-43951-7_24。43 Dexter Kozen 和 Maria-Christina Patron。使用带测试的克莱尼代数认证编译器优化。载于 CL，第 568–582 页，2000年。 doi:10.1007/3-540-44957-4_38。44 Dexter Kozen 和 Wei-Lung Dustin Tseng。多重集与分布，2023年。 arXiv:2301.10812。45 Dexter Kozen 和 Wei-Lung Dustin Tseng。Böhm-Jacopini定理在命题层面是错误的。载于 MPC，第 177–192 页，2008年。 doi:10.1007/978-3-540-70594-9_11。46 Kim G. Larsen 和 Arne Skou。通过概率测试进行双模拟。Information and Computation，94(1):1–28，1991年。 doi:10.1016/0890-5401(91)90030-6。47 Hosam Mahmoud。Pólya urn模型。统计科学教材。Chapman & Hall，2008年。48 Radu Mardare、Prakash Panangaden 和 Gordon D. Plotkin。定量代数推理。载于 LICS，第 700–709 页，2016年。 doi:10.1145/2933575.2934518。49 Annabelle McIver、Carlos Gonzalía、Ernie Cohen 和 Carroll C. Morgan。使用概率克莱尼代数 pKA 进行协议验证。《J. Log. Algebraic Methods Program.》，76(1):90–111，2008年。 doi:10.1016/j.jlap.2007.10.005。50 Annabelle McIver、Tahiry M. Rabehaja 和 Georg Struth。关于概率克莱尼代数、自动机与模拟。载于 RAMICS，第 264–279 页，2011年。doi:10.1007/978-3-642-21070-9_20。51 Annabelle McIver、Tahiry M. Rabehaja 和 Georg Struth。概率并发克莱尼代数。载于 QAPL，第 97–115 页，2013年。 doi:10.4204/EPTCS.117.7。52 Robin Milner。一类正规行为的完备推理系统。《J. Comput. Syst. Sci.》，28(3):439–466，1984年。 doi:10.1016/0022-0000(84)90023-0。53 Michael W. Mislove、Joël Ouaknine 和 James Worrell。概率与非确定性的公理。载于 EXPRESS，第 7–28 页，2003年。 doi:10.1016/j.entcs.2004.04.019。54 Lawrence S. Moss。余代数逻辑。《Ann. Pure Appl. Log.》，96(1-3):277–317，1999年。 doi:10.1016/S0168-0072(98)00042-6。55 Robert Paige 和 Robert Endre Tarjan。三种划分细化算法。《SIAM J. Comput.》，16(6):973–989，1987年。 doi:10.1137/0216062。56 Damien Pous、Jurriaan Rot 和 Jana Wagemaker。关于带假设的克莱尼代数完备性的工具，2022年。 arXiv:2210.13020。57 Jan J. M. M. Rutten。泛余代数：系统理论。《理论计算机科学》，249(1):3–80，2000年。 doi:10.1016/S0304-3975(00)00056-6。58 Arto Salomaa。正规事件代数的两个完备公理系统。《《ACM杂志》》，13(1):158–169，1966年。 doi:10.1145/321312.321326。59 Todd Schmid、Tobias Kappé、Dexter Kozen 和 Alexandra Silva。带测试的守卫 Kleene 代数：余方程、余归纳与完备性。载于 ICALP，第 142:1–142:14 页，2021年。 doi:10.4230/LIPIcs.ICALP.2021.142。60 Todd Schmid、Jurriaan Rot 和 Alexandra Silva。关于星表达式与余代数完备性定理。载于 MFPS，第 242–259 页，2021年。 doi:10.4204/EPTCS.351.15。61 Todd Schmid、Wojciech Różowski、Alexandra Silva 和 Jurriaan Rot。由代数理论参数化的过程。载于 ICALP，2022年。 doi:10.4230/LIPIcs.ICALP.2022.132。62 Roberto Segala 和 Nancy A. Lynch。概率过程的概率模拟。载于 CONCUR，第 481–496 页，1994年。 doi:10.1007/978-3-540-48654-1_35。63 Alexandra Silva。克莱尼余代数。博士论文，奈梅亨大学，2010年。

64 Steffen Smolka、Nate Foster、Justin Hsu、Tobias Kappé、Dexter Kozen 和 Alexandra Silva。带测试的守卫 Kleene 代数：以近线性时间验证未解释程序。载于 POPL，第 61:1–61:28 页，2020年。 doi:10.1145/3371129。65 Steffen Smolka、Praveen Kumar、Nate Foster、Dexter Kozen 和 Alexandra Silva。Cantor 遇见 Scott：概率网络的语义基础。载于 POPL，第 557–571 页，2017年。doi:10.1145/3009837.3009843。66 Steffen Smolka、Praveen Kumar、David M. Kahn、Nate Foster、Justin Hsu、Dexter Kozen 和 Alexandra Silva。可扩展的概率网络验证。载于 PLDI，第 190–203 页，2019年。doi:10.1145/3314221.3314639。67 Ana Sokolova。余代数视角下的概率系统：综述。《理论计算机科学》，412(38):5095–5110，2011年。 doi:10.1016/j.tcs.2011.05.008。68 Eugene W. Stark 和 Scott A. Smolka。有限状态概率过程的完备公理系统。载于《证明、语言与交互：向 Robin Milner 致敬的论文集》，第 571–596 页，2000年。69 Sam Staton。余代数双模拟概念之间的关系。《Log. Methods Comput. Sci.》，7(1)，2011年。 doi:10.2168/LMCS-7(1:13)2011。70 Joseph Aaron Toumanios。三面骰子，2019年。美国专利 10384119。网址： https://image-ppubs.uspto.gov/dirsearch-public/print/downloadPdf/10384119。71 Daniele Varacca 和 Glynn Winskel。将概率分布到非确定性之上。《Mathematical Structures in Computer Science》，16(1):87–113，2006年。 doi:10.1017/S0960129505005074。72 Jana Wagemaker、Nate Foster、Tobias Kappé、Dexter Kozen、Jurriaan Rot 和 Alexandra Silva。并发 NetKAT——状态化并发网络的建模与分析。载于 ESOP，第 575–602 页，2022年。 doi:10.1007/978-3-030-99336-8_21。73 Thorsten Wißmann、Ulrich Dorsch、Stefan Milius 和 Lutz Schröder。高效且模块化的余代数划分细化。《Logical Methods in Computer Science》，16:1:8:1–8:63，2020年。doi:10.23638/LMCS-16(1:8)2020。74 Thorsten Wißmann、Stefan Milius 和 Lutz Schröder。行为不等价性的通用模态见证的拟线性时间计算。《Log. Methods Comput. Sci.》，18(4)，2022年。doi:10.46298/lmcs-18(4:6)2022。75 James Worrell。有限集函子的终序列。《理论计算机科学》，338(1-3):184–199，2005年。 doi:10.1016/j.tcs.2004.12.009。

一个余代数

在论文正文中，为了避免偏离那些可以具体描述的核心概念，我们在讲述时没有使用泛余代数的语言 [57, 29]。不过，我们在论述中确实用到了余代数，正文中的具体定义都是抽象概念的实例。这有助于简化证明，因此我们将在附录中使用余代数来证明这些结果。

我们假设读者熟悉范畴论的基本概念，例如函子、拉回和自然变换。我们先回顾泛余代数的基本概念；如需更详细的介绍，请参阅 [57, 29]。

▶ **定义 30.** 设 B 是一个 Set-自函子。一个 B-余代数是一个有序对 (X, β)，其中 X 是一个集合，$\beta : X \to BX$ 是一个转移函数。两个 B-余代数 (X, β) 和 (Y, γ) 之间的同态是一个函数 $h : X \to Y$，满足 $Bh \circ \beta = \gamma \circ h$。$B$-余代数及其间的同态构成一个范畴，我们将其记作 $\mathsf{Coalg}_{\mathcal{B}}$。

回忆一下，有限支撑概率分布的集合 $\mathcal{D}_\omega(X)$ 是 Set 上的自函子。正如前文所提到的，ProbGKAT 自动机可以建模为函子 $\mathcal{G} = \mathcal{D}_\omega(2 + \text{输出} + \text{动作集} \times \mathrm{Id})^{\mathrm{At}}$ 的余代数，接下来我们将以此为基础研究它们。

▶ **定义 31.** 设 (X,β) 和 (Y,γ) 为 B-余代数，其中 $Y \subseteq X$。如果包含映射 $i\colon Y \to X$ 是一个 B- 余代数同态，则称 (Y,γ) 为子余代数，它是 (X,β) 的子余代数。

至多存在一个余代数结构映射 $\gamma : Y \to \mathcal{B}Y$，使得包含映射 $i\colon Y \to X$ 成为从 (Y,γ) 到 (X,β) 的 B-余代数同态 [57]。任意 $\mathcal{B}$-余代数 (X,β) 的子余代数构成一个完备格 [57]。给定 $x \in X$，我们将用 $\langle x\rangle_\beta$ 表示包含 x 的 (X,β) 的最小子余代数，即由其生成的子余代数 x。

▶ 定义 *32.* 设 (X,β) 和 (Y,γ) 为 G-余代数。若存在函数 $\rho : R \to BR$，使得投影 $\pi_1,\pi_2 : R \to X$ 是从 (R,ρ) 到 (X,β) 和 (Y,γ) 的 B- 余代数同态，则称关系 $R \subseteq X \times Y$ 为双模拟。若存在双模拟 R，使得 $(x,y) \in R$，则称元素 $x \in X$ 和 $y \in Y$ 双模拟等价。

注意，定义 4 是将定义 30 中余代数同态的抽象定义实例化到 $\mathcal{G}$ 上。同样，定义 5 是定义 32 的一个实例化。

<escape>▶</escape>**命题 33.** *1.* 函子 $\mathcal{G}$ 是有界的，并且保持弱拉回
2. 存在一个 G-余代数 (Z,ζ)，它是 $Coalg_{\mathcal{G}}$ 中的终对象。换言之，对于任意 G-余代数 (X,β)，存在唯一的同态 $!_\beta : X \to Z$*3*。设 (X,β) 和 (Y,γ) 为 G-余代数。元素 $x \in X$ 和 $y \in Y$ 是双模拟等价的，当且仅当 $!_\beta(x) = !_\gamma(y)$

证明。 (1) Moss 在 [54] 中证明了 $\mathcal{D}_\omega$ 保持弱拉回。Gumm 和 Schröder [30] 证明了弱拉回的保持性在函子复合、积和余积运算下是封闭的。由于 Set 自函子 $F(X) = X^A$, $G(X) = B + X$ 和 $H(X) = C$ (其中 A, B 和 C 均为任意集合）都保持弱拉回，因此 $\mathcal{G}$ 也保持弱拉回。

(2) 根据定理 4.6]，函子 $\mathcal{D}_\omega$ 是有界的。由于 Act 和 $2+$Out 都是有限的，因此它们也是 ω-有界的。有界性在函子复合、二元积和二元余积下保持不变 [31, 推论 4.9]。由于 At 是有限的，指数函子 $\mathrm{Id}^{\mathsf{At}}$ 也是有界的。综上，我们可以得出 $\mathcal{G}$ 是有界的。终余代数的存在性由有界性推出 [57, 定理 10.3]。

(3) 由 $\mathcal{G}$ 保持弱拉回这一事实可得 [57, 定理 9.3]。 ◀

B 第3节的证明

▶ **引理 7。** 对于所有 $\mathsf{e} \in \mathtt{Exp}$，$|\mathsf{e}\rangle_\partial$ 都是有限的。事实上，状态数的上界为 $\#(\mathsf{e}) : \mathtt{Exp} \to \mathbb{N}$，其中 $\#(-)$ 递归定义如下：

$$\#(\mathsf{b}) = 1 \quad \#(v) = 1 \quad \#(\mathsf{p}) = 2 \quad \#(\mathsf{e} +_\mathsf{b} \mathsf{f}) = \#(\mathsf{e}) + \#(\mathsf{f}) \quad \#(\mathsf{e} \oplus_r \mathsf{f}) = \#(\mathsf{e}) + \#(\mathsf{f})$$

$$\#(\mathsf{e}\,;\mathsf{f}) = \#(\mathsf{e}) + \#(\mathsf{f}) \quad \#\left(\mathsf{e}^{(\mathsf{b})}\right) = \#(\mathsf{e}) \quad \#\left(\mathsf{e}^{[r]}\right) = \#(\mathsf{e})$$

证明。 我们改编了 GKAT [59] 的类似证明。对于任意 $\mathsf{e} \in \mathtt{Exp}$，令 $|\langle \mathsf{e}\rangle_\partial|$ 为包含 e 的 $(\mathtt{Exp},\partial)$ 的最小子余代数的载集基数。我们通过归纳证明，对于所有 $\mathsf{e} \in \mathtt{Exp}$，均有 $|\langle \mathsf{e}\rangle_\partial| \leq \#(\mathsf{e})$。

对于基例，注意到，对于 $v \in$输出，生成的子余代数恰好只有一个状态，该状态以概率 1 输出相应的值。因此，$\#(v) = 1$。类似地，对于 $\mathsf{b} \in \mathtt{BExp}$，有 $\#(\mathsf{b}) = 1$。对于 $\mathsf{p} \in$ 动作集，有两个状态；初始状态以概率 1 在 p 上转移到另一个状态，该状态以概率 ✓ 输出 1。

对于归纳情形，假设 $|\mathsf{he}\rangle_\partial| \leq \#(e)$、$|\mathsf{hf}\rangle_\partial| \leq \#(f)$、$\mathsf{b} \in \mathtt{BExp}$ and $r \in [0,1]$。$\mathsf{e}+_\mathsf{b}\mathsf{f}$ 的每个导数要么是 e 的导数，要么是 f 的导数，因此 $|\mathsf{he}+_\mathsf{b}\mathsf{f}\rangle_\partial| \leq |\mathsf{he}\rangle_\partial| + |\mathsf{hf}\rangle_\partial| = \#(\mathsf{e}) + \#(\mathsf{f}) = \#(\mathsf{e} +_\mathsf{b} \mathsf{f})$。通过类似的推理，$|\mathsf{he} \oplus_r \mathsf{f}\rangle_\partial| \leq \#(\mathsf{e} \oplus_r \mathsf{f})$。

- 在 e ; f 的情况下，该表达式的每个导数要么是 f 的导数，要么是 e 的某个导数后接 f。因此，$|\langle \mathsf{e}\,;\mathsf{f}\rangle_\partial| = |\langle \mathsf{e}\rangle_\partial \times \{\mathsf{f}\}| + |\langle \mathsf{e}\rangle_\partial| \leq \#(\mathsf{e}) + \#(\mathsf{f}) = \#(\mathsf{e}\,;\mathsf{f})$。对于概率循环的情况，注
- 意 e 的每个导数都是 e 的某个导数后接 $\mathsf{e}^{[r]}$。可以很容易地看出，$\mathsf{e}^{[r]}$ 的导数数量与 e 的导数数量相同。因此，$|\langle \mathsf{e}^{[r]}\rangle_\partial| \leq |\langle \mathsf{e}\rangle_\partial| = \#(\mathsf{e}) = \#(\mathsf{e}^{[r]})$。我们省略守卫循环的情况，因为其推理与概率循环的情况完全相同。◀

C 第4节的证明

一个流网络 是一个由 (G, c) 组成的二元组，其中 $G = (V, E)$ 是一个有向图，边 $E \subseteq V \times V$配有容量函数 c: $E \to \mathbb{R}^+_\infty$。通过网络 (G, c) 的 (s, t)- 流，其中 $s, t \in V$，是一个满足以下条件的函数 f: $E \to \mathbb{R}^+_\infty$：

1. 对于所有 $v \in V \setminus \{s, t\}$

$$\sum_{(u,v)\in E} f(u, v) = \sum_{(v,u)\in E} f(v, u)$$

2. 对于所有 $e \in E$, $f(e) \leq c(e)$ (流的可行性)
3. 存在一个常数 $F \in \mathbb{R}^+_\infty$ 称为流值，并满足

$$F = \sum_{(s,u)\in E} f(s, u) = \sum_{(v,t)\in E} f(v, t)$$

令 $S \subseteq V$，使得 $s \in S$。(s, t)-割 是边的集合 $E(S, V \setminus S) = \{(u, v) \in E \mid u \in S, v \in V \setminus S\}$。该割的容量 定义为

$$C_S = \sum_{(u,v)\in E(S,V\setminus S)} c(u, v)$$

以下关于流与割的结果是众所周知的。

▶ **定理 34** （最大流最小割定理 [18]）。 设（G, c）是一个流网络，其中包含 $G =$（V, E），并设 $s, t \in V$为顶点。可行（s, t）-流的最大值等于任意（s, t）-割的最小容量。

有了这一点，我们便可以验证我们对双模拟的刻画。

▶ **引理 35**。 令 (X, β) 和(Y, γ) 为 ProbGKAT 自动机，并令 $R \subseteq X \times Y$为一个关系。R 是双模拟，当且仅当对于所有 $(x, y) \in R$ 和 $\alpha \in$ 原子，以下条件成立。
1. 对所有 $o \in 2 +$ 输出，$\beta(x)_\alpha(o) = \gamma(y)_\alpha(o)$ *2.* 对所有 $A \subseteq X$ 以及所有 $p \in$ 动作集，$\beta(x)_\alpha[\{p\} \times A] \leq \gamma(y)_\alpha[\{p\} \times R(A)]$*3.* 对所有 $B \subseteq Y$以及所有 $p \in$ 动作集，$\gamma(y)_\alpha[\{p\} \times B] \leq \beta(x)_\alpha[\{p\} \times R^{-1}(B)]$

证明。设 (X, β) 和 (Y, γ) 是 G-余代数，且 $R \subseteq X \times Y$ 是一个关系。定义 32 指出，R 是一个双模拟，当且仅当存在一个 G-余代数结构映射ρ: $R \to \mathsf{G}R$，使典范投影映射成为从 (R, ρ) 到 (X, β) 和 (Y, γ) 的同态。我们可以将此定义具体展开。也就是说，关系 $R \subseteq X \times Y$ 是一个双模拟，当且仅当存在 G- 余代数结构映射 ρ: $R \to \mathsf{G}R$，使得对于所有 $(x, y) \in R$ 和所有 $\alpha \in$ 原子，以下条件均成立：

1. 对于所有 $o \in 2 +$ 输出，$\beta(x)_\alpha(o) = \rho(x, y)_\alpha(o) = \gamma(y)_\alpha(o)$**2.** 对于所有 $(\mathsf{p}\ x') \in$ 动作集 $\times X$

$$\beta(x)_\alpha(\mathsf{p}, x') = \sum_{(x',y')\in R} \rho(x, y)_\alpha(\mathsf{p}, (x', y'))$$

3. 对于所有 $(\mathsf{p}\ y') \in$ 动作集 $\times Y$

$$\gamma(y)_\alpha(\mathsf{p}, y') = \sum_{(x',y')\in R} \rho(x,y)_\alpha(\mathsf{p},(x',y'))$$

上述定义中的条件 (1) 很容易证明与引理中的条件 (1) 等价

。现在我们通过构造一族流网络并应用最大流最小割定理，证明满足后述条件的余代数结构映射 $\rho : R \to \mathcal{G}R$ 的存在等价于本引理中的条件。假设 $(x, y) \in R$。对于每个 $\alpha \in$ 原子和 $p \in$ 动作集，构造一个流网络 $(G_{\alpha,\mathsf{p}}, c_{\alpha,p})$，其中 $G_{\alpha,\mathsf{p}} = (V_{\alpha,\mathsf{p}}, E_{\alpha,\mathsf{p}})$，如下所示。

$$\begin{aligned}
V_{\alpha,\mathsf{p}} &= \{s,t\} \cup \{x' \in X \mid \beta(x)_\alpha(\mathsf{p},x') > 0\} \cup \{y' \in Y \mid \gamma(y)_\alpha(\mathsf{p},y') > 0\} \\
E_{\alpha,\mathsf{p}} &= \{(s,x') \mid x' \in X \cap V_{\alpha,\mathsf{p}}\} \\
&\quad \cup \{(x',y') \mid x' \in (X \cap V_{\alpha,\mathsf{p}}), y' \in (Y \cap V_{\alpha,\mathsf{p}}), (x',y') \in R\} \\
&\quad \cup \{(y',t) \mid y' \in Y \cap V_{\alpha,\mathsf{p}}\}
\end{aligned}$$

非正式地说，$V_{\alpha,\mathsf{p}}$ 包含指定的源顶点和目标顶点 s 和 t，以及 $\beta(x)_\alpha$ 和 $\gamma(y)_\alpha$ 的支撑集，并将其限制为第一坐标为 p 的元组。

我们从 s （分别是 t）向包含在顶点集合中的 $\beta(x)_\alpha$ （分别是 $\gamma(y)_\alpha$）支撑集中的任意元素添加一条边。当两个顶点之间存在 R 关系时，它们便相连。

容量函数 $c_{\alpha,\mathsf{p}}$ 定义如下：对于所有 $x' \in X \cap V_{\alpha,p}$，我们设定 $c_{\alpha,p}(s,x') = \beta(x)_\alpha(\mathsf{p}\ x')$，并且对于所有 $y' \in Y \cap V_{\alpha,\mathsf{p}}$，我们设定 $c_{\alpha,\mathsf{p}}(y',t) = \gamma(y)_\alpha(\mathsf{p}\ y')$。否则，对于剩余的 $(x',y') \in E$，我们选择 $c_{\alpha,\mathsf{p}}(x',y') = +\infty$。

首先，假设引理的条件 (1–3) 成立。令 $S \subseteq V_{\alpha,\mathsf{p}}$ 为包含 s 的集合，使得 $C = E(S, V_{\alpha,\mathsf{p}} \setminus S)$ 是最小容量割。该集合不能包含容量为无穷大的中心边，否则相应的流将不满足可容许性。

不失一般性，$C = A \cup B$ 其中 $A = \{(s,x') \mid s \in S, x' \in V_{\alpha,\mathsf{p}} \setminus S\}$ 且 $B = \{(y',t) \mid y' \in S, t \in V_{\alpha,\mathsf{p}} \setminus S\}$。最小割的容量，以及（根据定理 34）最大可行流的值为：

$$F_{\alpha,\mathsf{p}} = \beta(x)_\alpha[\{\mathsf{p}\} \times \pi_2(A)] + \gamma(y)_\alpha[\{\mathsf{p}\} \times \pi_1(B)]$$

现在，考虑集合 $A' = \{(s,\ x') \in E \mid (s,\ x') \notin A\}$。由于 A' 中的元素未包含在割中，$\pi_2(A')$ 中的所有顶点都出现在 S 中。因此，为了避免将无限容量的中心边纳入最小割，所有通过 R 与这些元素相关联的元素也必须包含在 S 中。因此 $R(\pi_2(A')) \subseteq S$，这意味着 $R(\pi_2(A')) \subseteq \pi_1(B)$。

利用这些观察结果，我们可以从下方界定最大流的值：

$$\begin{aligned}
F_{\alpha,\mathsf{p}} &= \beta(x)_\alpha[\{\mathsf{p}\} \times \pi_2(A)] + \gamma(y)_\alpha[\{\mathsf{p}\} \times \pi_1(B)] \\
&\geq \beta(x)_\alpha[\{\mathsf{p}\} \times \pi_2(A)] + \gamma(y)_\alpha[\{\mathsf{p}\} \times R(\pi_2(A'))] \\
&\geq \beta(x)_\alpha[\{\mathsf{p}\} \times \pi_2(A)] + \beta(x)_\alpha[\{\mathsf{p}\} \times \pi_2(A')] && (2) \\
&= \beta(x)_\alpha[\{\mathsf{p}\} \times (X \cap V_{\alpha,\mathsf{p}})] && (A \text{ and } A' \text{ are disjoint})
\end{aligned}$$

由于可容许性约束，$F_{\alpha,\ \mathsf{p}}$ 也有如下上界

$$\sum_{x' \in X \cap V_{\alpha,\mathsf{p}}} c_{\alpha,\mathsf{p}}(s,x') = \beta(x)_\alpha[\{\mathsf{p}\} \times (X \cap V_{\alpha,\mathsf{p}})]$$

这意味着上述下界是紧的。通过对称推理，我们可以推导出

$$F_{\alpha,\mathsf{p}} = \gamma(y)_\alpha[\{\mathsf{p}\} \times (Y \cap V_{\alpha,\mathsf{p}})]$$

具体而言，这意味着与源点 s 相连的每条边上的流量都必须达到容量，因为 $x' \in V_{\alpha,\mathsf{p}}$ 的 $c_{\alpha,\mathsf{p}}(s,x')$ 之和已达到允许的最大值。

现在，我们按以下方式定义 ρ：$R \to GR$。1. 对于所有 $\alpha \in$ 原子和 $o \in 2+$ 输出，令 $\rho(x,y)_\alpha(o) = \beta(x)_\alpha(o) = \gamma(y)_\alpha(o)$。2. 对于所有 $\alpha \in$ 原子、$\mathsf{p} \in$ 动作集和 $(x',y') \in R$，令 $\rho(x,y)_\alpha(\mathsf{p},(x',y')) = f_{\alpha,\mathsf{p}}(x',y')$

余代数定义中的双模拟条件 (1) 立即成立。为证明 (2)，注意到对于任意 $\alpha \in$ 原子 $p \in$ 动作集 $x' \in X$，我们有 that

$$\begin{aligned}\beta(x)_\alpha(\mathsf{p},x') &= c_{\alpha,\mathsf{p}}(s,x')\\ &= f_{\alpha,\mathsf{p}}(s,x')\\ &= \sum_{(x',y')\in E_{\alpha,p}} f_{\alpha,\mathsf{p}}(x',y')\\ &= \sum_{(x',y')\in R} \rho(x,y)_\alpha(\mathsf{p},(x',y'))\end{aligned}$$

条件（3）由对称论证可得。

对于逆命题，假设余代数定义中的条件 (2) 和 (3) 成立。我们通过反证法证明 (2) 成立。因此，假设引理陈述中的条件 (2) 不成立，即存在某个 $\alpha \in$ 原子 和 $\mathsf{p} \in$ 动作集 $A \subseteq X$，使得我们有

$$\beta(x)_\alpha[\{\mathsf{p}\}\times A] > \gamma(y)_\alpha[\{\mathsf{p}\}\times R(A)]$$

与之前一样，对于每个流网络 $(G_{\alpha,\mathsf{p}},c_{\alpha,\mathsf{p}})$，最小 (s,t)-割的容量由下式给出

$$\begin{aligned}F_{\alpha,p} &= \beta(x)_\alpha[\{\mathsf{p}\}\times\pi_2(A)] + \gamma(y)_\alpha[\{\mathsf{p}\}\times\pi_1(B)]\\ &\geq \beta(x)_\alpha[\{\mathsf{p}\}\times\pi_2(A)] + \gamma(y)_\alpha[\{\mathsf{p}\}\times R(\pi_1(A'))]\\ &> \beta(x)_\alpha[\{\mathsf{p}\}\times\pi_2(A)] + \beta(x)_\alpha[\{\mathsf{p}\}\times R(\pi_1(A'))]\\ &= \beta(x)_\alpha[\{\mathsf{p}\}\times(X\cap V_{\alpha,\mathsf{p}})]\end{aligned}$$

因此，最大流小于容量。因此存在 $x' \in X$，使得在线a

$$\begin{aligned}\beta(x)_\alpha(\mathsf{p},x') &= c_{\alpha,\mathsf{p}}(s,x')\\ &> f_{\alpha,\mathsf{p}}(s,x')\\ &= \sum_{(x',y')\in E_{\alpha,\mathsf{p}}} f_{\alpha,\mathsf{p}}(x',y')\\ &= \sum_{(x',y')\in R} \rho(x,y)_\alpha(\mathsf{p},(x',y'))\end{aligned}$$

这会导致矛盾。条件（3）由对称性成立。 ◀

▶ **引理 8**。设 (X,β) 是一个ProbGKAT 自动机，且 $R \subseteq X\times X$ 是一个等价关系。R 是双模拟，当且仅当且仅当对于所有 $(x,y) \in R$ 和 $\alpha \in$ 原子，
1. 对所有 $o \in 2+$输出、$\beta(x)_\alpha(o) = \beta(y)_\alpha(o)$，以及 *2.* 对所有等价类 $Q \in X/R$ 和所有 $p \in$ 动作集，$\beta(x)_\alpha[\{p\}\times Q] = \beta(y)_\alpha[\{p\}\times Q]$

证明。假设 R 是一个双模拟。根据引理 35，条件 (1) 立即成立。为证明 (2)，取任意等价类 $Q \in X/R$。由于根据假设 R 是一个等价关系，注意到 $R(Q) = Q = R^{-1}(Q)$。假设 $(x,y) \in R$。对所有 $\alpha \in At$以及 $\mathsf{p} \in$动作集

$$\beta(x)_\alpha[\{\mathsf{p}\}\times Q] \leq \gamma(x)_\alpha[\{\mathsf{p}\}\times Q] \leq \beta(y)_\alpha[\{\mathsf{p}\}\times Q]$$

由此我们可以得出结论（2）。

对于逆向证明，注意到引理 35 的条件 (1) 显然成立。为了证明 (2)，任取一个 $A \subseteq X$。令 A/R 为 A 关于关系 R 的商集，并令 X/R 为 X 关于 R 的商集。注意到 A/R 是 A 的一个划分，而 X/R 是 X 的一个划分。

此外，对于每个等价类 $P \in A/R$，都存在一个等价类 $Q_P \in X/R$，使得 $P \subseteq Q_P = R(P)$。由于单调性，我们还得到 $\beta(x)_\alpha[\mathsf{p} \times P] \leq \beta(x)_\alpha[\{\mathsf{p}\} \times Q_P]$ 对于所有 $\alpha \in$ 原子，$\mathsf{p} \in$ 动作集。根据 σ-可加性，我们有 that

$$\begin{aligned}
\beta(x)_\alpha[\{\mathsf{p}\} \times A] &= \beta(x)_\alpha\left[\{\mathsf{p}\} \times \bigcup_{P \in A/R} P\right] \\
&= \sum_{P \in A/R} \beta(x)_\alpha[\{\mathsf{p}\} \times P] \\
&\leq \sum_{P \in A/R} \beta(y)_\alpha[\{\mathsf{p}\} \times Q_P] \\
&= \beta(y)_\alpha\left[\{\mathsf{p}\} \times \bigcup_{P \in A/R} Q_P\right] \\
&= \beta(y)_\alpha\left[\{\mathsf{p}\} \times \bigcup_{P \in A/R} R(P)\right] \\
&= \beta(y)_\alpha[\{\mathsf{p}\} \times R(A)]
\end{aligned}$$

这就证明了对于所有 $\alpha \in$ 原子，$\mathsf{p} \in$ 动作集，(2)成立。 The case for (3) proceeds symmetrically. Wait must translate all. "对于(3)的情形可对称地进行。" Need no English. Ensure punctuation maybe sentence. final. ◀

C.1 双模拟的序理论刻画

双模拟泛函 Φ （定义 9）可以证明是单调的，而双模拟可以刻画为该算子的后不动点。

▶ **引理 36.** 设 (X, β) 和 (Y, γ) 是 G-余代数。以下结论成立：
1. $\Phi_{\beta,\gamma}$ 关于包含序单调**2.** R 是 (X, β) 和 (Y, γ) 之间的双模拟，当且仅当 $R \subseteq \Phi_{\beta,\gamma}(R)$

证明。对于 (1)，设 $R \subseteq S \subseteq X \times Y$，并假设 $(x, y) \in \Phi_{\beta,\gamma}(R)$。那么对于所有$\alpha \in$ At 和 $o \in 2^{+}$Out，都有 $\beta(x)_\alpha(o) = \gamma(y)_\alpha(o)$。对于所有 $\alpha \in$ At、$\mathsf{p} \in$ Act 以及$A \subseteq X$，都有 $\beta(x)_\alpha[\{\mathsf{p}\} \times A] \leq \gamma(y)_\alpha[\{\mathsf{p}\} \times R(A)]$。由于 $R \subseteq S$，我们有$R(A) \subseteq S(A)$。根据单调性，有 $\gamma(y)_\alpha(\{\mathsf{p}\} \times R(A)) \leq \gamma(y)[\{\mathsf{p}\} \times S(A)]$，因此 $\beta(x)_\alpha[\{\mathsf{p}\} \times A] \leq \gamma(y)_\alpha[\{\mathsf{p}\} \times S(A)]$。其余情况对称。因此 $(x, y) \in \Phi_{\beta,\gamma}(S)$，这证明了 $\Phi_{\beta,\gamma}(R) \subseteq \Phi_{\beta,\gamma}(S)$。

（2）这是显然的，因为它只是对引理 35 的重新表述。 ◀

回顾一下，Knaster-Tarski 不动点定理指出，完备格 $(X, \sqsubseteq)$ 上单调自映射 $f : X \to X$ 的最大不动点由下式给出

$$\mathsf{gfp}(f) = \bigsqcup \{x \in X \mid x \sqsubseteq f(x)\}$$

下文中，用 $\sim_{\beta,\gamma}$ 表示 (X, β) 和 (Y, γ) 之间的最大双模拟。当余代数在上下文中显而易见时，可以省略下标。

26 模双模拟的概率守卫 KAT：完备性与复杂性

▶ **推论 37.** 设 (X, β) 和 (Y, γ) 为 $\mathcal{G}$-余代数。泛函 $\Phi_{\beta,\gamma}$ 的最大不动点 $\mathsf{gfp}(\Phi_{\beta,\gamma})$ 是 (X, β) 和 (Y, γ) 之间的最大双模拟。

证明。 根据 Knaster-Tarski 不动点定理，$\mathsf{gfp}(\Phi_{\beta,\gamma})$ 是一个不动点，特别是一个后不动点。因此，根据引理 36，它是一个双模拟。

令 S 为 $\mathcal{G}$-余代数 (X, β) 和 (Y, γ) 之间的任意双模拟。同样，根据引理 36，我们有 $S \subseteq \Phi_{\beta,\gamma}(S)$，因此

$$S \subseteq \Phi_{\beta,\gamma}(S) \subseteq \bigcup \{R \subseteq X \times Y \mid R \subseteq \Phi_{\beta,\gamma}(R)\} = \mathsf{gfp}(\Phi_{\beta,\gamma})$$ ◀

在处理等价关系时，我们可以简化对 Φ 的刻画（与引理 8 类似）。在记号方面，我们将用 Φ_β 表示 $\Phi_{\beta,\beta}$。

▶ **引理 38。** 设 (X, β) 为 $\mathcal{G}$-余代数，且 $R \subseteq X \times X$ 为一个等价关系。我们有 $(x, y) \in \Phi_\beta(R)$ 当且仅当对所有 $\alpha \in$ 原子，以下条件均成立。

1. 对所有 $o \in 2 + $ 输出，$\beta(x)_\alpha(o) = \beta(y)_\alpha(o)$ *2.* 对所有 $Q \in X/R$ 以及对所有 $p \in$ 动作集，我们有 $\beta(x)_\alpha[\{p\} \times Q] = \beta(y)_\alpha[\{p\} \times Q]$。此外，$\Phi_\beta(R)$ 也是一个等价关系。

证明。 第一个断言的证明与引理 8 的证明完全相同，因此我们只专注于证明 $\Phi_\beta(R)$ 也是一个等价关系。

关于后一个结论，引理的前半部分告诉我们，可以使用 Φ_β 的更简单刻画。对于所有 $x \in X$ 和所有 $\alpha \in$ At，自反性显然成立。

1. 对所有 $o \in 2 + $ 输出、$\beta(x)_\alpha(o) = \beta(x)_\alpha(o)$。2. 对所有 $\mathrm{p} \in$ 动作集、$Q \in X/R$，我们有 $\beta(x)_\alpha[\{\mathrm{p}\} \times Q] = \beta(x)_\alpha[\{\mathrm{p}\} \times Q]$。因此 $(x, x) \in \Phi_\beta(R)$。

要看出对称性，假设对于某个 $x, y \in X$，有 $(x, y) \in \Phi_\beta(R)$。那么，由于等式的对称性，我们有所有 $\alpha \in$ 原子

1. 对于所有 $o \in 2 + $ 输出，$\beta(y)_\alpha(o) = \beta(x)_\alpha(o)$。2. 对于所有 $\mathrm{p} \in$ 动作集}，$Q \in X/R$，我们有 $\beta(y)_\alpha[\{\mathrm{p}\} \times Q] = \beta(x)_\alpha[\{\mathrm{p}\} \times Q]$。因此 $(y, x) \in \Phi_\beta(R)$。

最后，为了看出传递性，假设对于某个任意的 $x, y, z \in X$，有 $(x, y), (y, z) \in \Phi_\beta(R)$。同样，由于等式的传递性，我们有对于所有 $\alpha \in$ 原子

1. 对于所有 $o \in 2 + $ 输出，$\beta(x)_\alpha(o) = \beta(y)_\alpha(o) = \beta(z)_\alpha(o)$。2. 对于所有 $\mathrm{p} \in$ 动作集}，$Q \in X/R$，我们有 $\beta(x)_\alpha[\{\mathrm{p}\} \times Q] = \beta(y)_\alpha[\{\mathrm{p}\} \times Q] = \beta(z)_\alpha[\{\mathrm{p}\} \times Q]$，因此 $(y, z) \in \Phi_\beta(R)$。
◀

由于 Φ_β 保持等价关系，它也可以视为等价关系格上的一个自映射，该格按包含关系（细化）排序。由于 $\mathcal{G}$ 保持弱拉回，最大双模拟是一个等价关系 [57, 推论 5.6]。因此，为刻画最大双模拟，我们可以将范围限制在等价关系之内。

继续之前，我们先回顾一些定义。ω-余链 是 $\{x_i\}_{i \in \omega}$ 中元素构成的序列，其中对所有的 $i \in \omega$，都有 $x_i \sqsupseteq x_{i+1}$。如果一个自映射 $f\colon X \to X$ ω-余连续，我们就称它保持 ω-余链的交，也就是说，$f(\sqcap_{i \in \omega} x_i) = \sqcap_{i \in \omega} f(x_i)$。

▶ **命题 39。** 设 (X, ν) 是一个完备格，且 $f\colon X \to X$ 是一个自映射。

1.（*Kleene* 不动点定理）若 f 是 ω-余连续的，则它具有一个最大不动点，表示为 $\mathit{gfp}(f) = \bigsqcup_{i \in \omega} f^{(i)}(\top)$，其中 $f^{(0)} = \mathsf{id}$ 且 $f^{(n+1)} = f^{(n)} \circ f$。*2.* 若 f 是单调的，则对于每个 ω-余链 $\{x_i\}_{i \in \omega}$，都有 $f(\bigsqcup_{i \in \omega} x_i) \nu \bigsqcup_{i \in \omega} f(x_i)$。

证明。我们证明第二个结论。取一个递降的 ω-链 $\{x_i\}_{i\in\omega}$。由于单调性，将 f 应用于该链中的元素会得到另一个递降的ω-链 $\{f(x_i)\}_{i\in\omega}$。由于对于所有 $i \in \omega$，都有 $\mathrm{u}_{i\in\omega} x_i \vee x_i$，根据单调性可得$f(\mathrm{u}_{i\in\omega} x_i) \vee f(x_i)$，因此 $f(\mathrm{u}_{i\in\omega} x_i)$ 是链 $\{f(x_i)\}_{i\in\omega}$ 的一个下界，故不大于该链的交。因此，有 $f(\mathrm{u}_{i\in\omega} x_i) \vee \mathrm{u}_{i\in\omega} f(x_i)$。◀

给定一个$\mathcal{G}$-余代数（X，β），我们通过重新调整 Baier [5, 引理 3.7.5] 的结果，证明 ω-余连续性在集合 X上的等价关系格中成立。

▶ **引理 40.** 设(X, β) 为 G-余代数。则 Φ_β 在 X上的等价关系格中是 ω-余连续的。

证明。 根据命题 39 和引理 36，要证明 ω-余连续性，只需证明对于任意按包含关系排序的下降 ω-等价关系余链$\{R_i\}_{i\in\omega}$，

$$\bigcap_{i\in\omega} \Phi_\beta(R_i) \subseteq \Phi_{\beta,} \left(\bigcap_{i\in\omega} R_i \right)$$

为此，首先注意到，对于任意 $Q \in X/R$ 和 $i \in \omega$，存在唯一的 $Q_i \in X/R_i$使得 $Q \subseteq Q_i$，因此 $Q \subseteq \bigcap_{i\in\omega} Q_i$。反过来，若对于所有 $i \in \omega$ 都有 $x \in Q_i$，则任取一个 $y \in Q$ （它必定存在，因为 Q 是一个等价类）。由于对于所有 i都有 $y \in Q_i$，我们可得对于所有 $i \in \omega$都有 $x\ R_i\ y$，因此 $x\ R\ y$，也就是说 $x \in Q$。这表明 $\bigcap_{i\in\omega} Q_i \subseteq Q$，从而 $Q = \bigcap_{i\in\omega} Q_i$。此外，对于 $i \in \omega$，有 $Q_{i+1} \subseteq Q_i$。

现在，固定 $x \in X$；根据概率的单调性，我们得到

$$\beta(x)_\alpha[\{\mathsf{p}\} \times Q_0] \geq \beta(x)_\alpha[\{\mathsf{p}\} \times Q_1] \geq \cdots \geq \beta(x)_\alpha[\{\mathsf{p}\} \times Q]$$

然而，由于 $\beta(x)_\alpha$ 具有有限支撑集，该序列只能取有限多个不同的值。这意味着它会在某个 $i(x, Q) \in \omega$ 处稳定下来，也就是说，对于 $k \geq i(x, Q)$，有 $\beta(x)_\alpha[\{\mathsf{p}\} \times Q_i] = \beta(x)_\alpha[\{\mathsf{p}\} \times Q_{i+1}] \geq \beta(x)_\alpha[\{\mathsf{p}\} \times Q]$。

现在假设对于所有 i，都有 $\beta(x)_\alpha[\{\mathsf{p}\} \times Q] < \beta(x)_\alpha[\{\mathsf{p}\} \times Q_i]$。那么特别地，存在某个 $x' \in X$，使得 $\beta(x)_\alpha(\mathsf{p}\ x') > 0$，且对于所有 $i \in \omega$ 都有 $x' \in Q_i$，但 $x' \notin Q$。这与 $Q = \bigcap_{i\in\omega} Q_i$ 矛盾，因此我们得出结论：对于某个 $i \in \omega$，有 $\beta(x)_\alpha[\{\mathsf{p}\} \times Q_i] = \beta(x)_\alpha[\{\mathsf{p}\} \times Q]$——尤其是，这应当对所有 $i \geq i(x, Q)$ 都成立。

现在，给定 $(x, y) \in \bigcap_{i\in\omega} \Phi_\beta(R_i)$，根据引理 38，我们有 $\beta(x)_\alpha(o) = \beta(y)_\alpha(o)$，对所有 $o \in 2 + \mathsf{Out}$ 都成立；并且对所有 $i \in \omega$ 和 $S \in X/R_i$，都有 $\beta(x)_\alpha[\{\mathsf{p}\} \times S] = \beta(y)_\alpha[\{\mathsf{p}\} \times S]$。给定 $Q \in X/R$，若我们选择 $k = \max(i(x, Q)\ i(y, Q))$，那么上述结果表明

$$\beta(x)_\alpha[\{\mathsf{p}\} \times Q] = \beta(x)_\alpha[\{\mathsf{p}\} \times Q_k] = \beta(y)_\alpha[\{\mathsf{p}\} \times Q_k] = \beta(y)_\alpha[\{\mathsf{p}\} \times Q]$$

引理 38 的两个条件现在都已满足，因此 $(x, y) \in \Phi_\beta(R) = \Phi_\beta(\bigcap_{i\in\omega} R_i)$。◀

▶ **定理 10.** 设(X, β) 是一个ProbGKAT 自动机。对于任意 $x, y \in X$, $x \sim y$，当且仅当对所有 $i \in \mathbb{N}$，都有 $x \sim^{(i)} y$。

证明。 由 ω的 -余连续性 Φ_β 以及命题 39 可得 ◀

令 $A \subseteq \mathsf{Exp}$ 和 $\mathsf{f} \in \mathsf{Exp}$。我们定义 $A/\mathsf{f} = A/\mathsf{f} = \{\mathsf{g} \in \mathsf{Exp} \mid \mathsf{g}\,;\mathsf{f} \in A\}$。

▶**引理41。** 若 $R \subseteq \mathsf{Exp} \times \mathsf{Exp}$ 是关于 ProbGKAT 算子的同余关系，且 $(\mathsf{e},\mathsf{f}) \in R$ 那么 $R(A/\mathsf{e}) \subseteq R(A)/\mathsf{f}$。

证明。若 $\mathsf{g} \in R(A/\mathsf{e})$，则存在某个 $\mathsf{h} \in A/\mathsf{e}$，使得 $(\mathsf{h}, \mathsf{g}) \in R$。由于 $\mathsf{h} \in A/\mathsf{e}$，因此 $\mathsf{h}\,;\mathsf{e} \in A$。因为 R 是同余关系，所以 $(\mathsf{h}\,;\mathsf{e}, \mathsf{g}\,;\mathsf{f}) \in R$，进而 $\mathsf{g}\,;\mathsf{f} \in R(A)$，这又意味着 $\mathsf{g} \in A/\mathsf{f}$。◀

▶ **引理 42.** 对于所有 $\alpha \in$ 原子、e、$\mathsf{f} \in \mathtt{Exp}$、$\mathsf{p} \in$ 动作集，$A \subseteq \mathtt{Exp}$ 我们有：

$$\partial(\mathsf{e}\,;\mathsf{f})_\alpha[\{\mathsf{p}\} \times A] = \partial(\mathsf{e})_\alpha[\{\mathsf{p}\} \times A/\mathsf{f}] + \partial(\mathsf{e})_\alpha(\checkmark)\partial(\mathsf{f})_\alpha[\{\mathsf{p}\} \times A]$$

证明。 我们推导如下。

$$\begin{aligned}\partial(\mathsf{e}\,;\mathsf{f})_\alpha[\{\mathsf{p}\} \times A] &= \sum_{\mathsf{a} \in A} \partial(\mathsf{e}\,;\mathsf{f})_\alpha(\mathsf{p}, \mathsf{a}) \\ &= \sum_{\mathsf{a}_0;\mathsf{f} \in A} \partial(\mathsf{e})_\alpha(\mathsf{p}, \mathsf{a}_0) + \sum_{\mathsf{a} \in A} \partial(\mathsf{e})_\alpha(\checkmark)\partial(\mathsf{f})(\mathsf{p}, \mathsf{a}) \\ &= \partial(\mathsf{e})_\alpha[\{\mathsf{p}\} \times A/\mathsf{f}] + \partial(\mathsf{e})_\alpha(\checkmark)\partial(\mathsf{f})_\alpha[\{\mathsf{p}\} \times A]\end{aligned}$$ ◀

考虑 Brzozowski余代数 $(\mathtt{Exp}, \partial)$ 时，算子 Φ_∂ 除了保持等价关系外，还具有另一项理想性质。

▶**引理 43**。设 R 是关于 ProbGKAT 算子的同余关系。那么$\Phi_\partial(R)$ 也属于同余关系。

证明。设 $R \subseteq \mathtt{Exp} \times \mathtt{Exp}$ 是一个同余关系，且 e、f、g、$\mathsf{h} \in \mathtt{Exp}$，满足 (e, g)、$(\mathsf{f}, \mathsf{h}) \in \Phi_\partial(R)$。设 $\mathsf{b} \in \mathtt{BExp}$ 且 $r \in [0, 1]$。为证明 $(\mathsf{e} \oplus_r \mathsf{f}, \mathsf{g} \oplus_r \mathsf{h}) \in \Phi_\partial(R)$，注意，对于所有 $\alpha \in$ 原子和所有 $o \in 2+$ 输出，我们有：

$$\begin{aligned}\partial(\mathsf{e} \oplus_r \mathsf{f})_\alpha(o) &= r\partial(\mathsf{e})_\alpha(o) + (1-r)\partial(\mathsf{f})_\alpha(o) \\ &= r\partial(\mathsf{g})_\alpha(o) + (1-r)\partial(\mathsf{h})_\alpha(o) \\ &= \partial(\mathsf{g} \oplus_r \mathsf{h})_\alpha(o)\end{aligned}$$

同理，对于所有 $\alpha \in$原子、$\mathsf{p} \in$动作集以及 $Q \in \mathtt{Exp}/R$，我们有

$$\begin{aligned}\partial(\mathsf{e} \oplus_r \mathsf{f})_\alpha[\{\mathsf{p}\} \times Q] &= \sum_{\mathsf{q} \in Q} \partial(\mathsf{e} \oplus_r \mathsf{f})_\alpha(\mathsf{p}, \mathsf{q}) \\ &= \sum_{\mathsf{q} \in Q} r\partial(\mathsf{e})_\alpha(\mathsf{p}, \mathsf{q}) + (1-r)\partial(\mathsf{f})_\alpha(\mathsf{p}, \mathsf{q}) \\ &= r\partial(\mathsf{e})_\alpha[\{\mathsf{p}\} \times Q] + (1-r)\partial(\mathsf{f})_\alpha[\{\mathsf{p}\} \times Q] \\ &= r\partial(\mathsf{g})_\alpha[\{\mathsf{p}\} \times Q] + (1-r)\partial(\mathsf{h})_\alpha[\{\mathsf{p}\} \times Q] \\ &= \partial(\mathsf{g} \oplus_r \mathsf{h})_\alpha[\{\mathsf{p}\} \times Q]\end{aligned}$$

因此 $(\mathsf{e} \oplus_r \mathsf{f},\ \mathsf{g} \oplus_r \mathsf{h}) \in \Phi_\partial(R)$

为了证明$(\mathsf{e} +_\mathsf{b} \mathsf{f},\ \mathsf{g} +_\mathsf{b} \mathsf{h}) \in \Phi_\partial(R)$，考虑 $\alpha \leq_{\mathsf{BA}} \mathsf{b}$的情况。对于所有 $o \in 2+$输出，我们有

$$\partial(\mathsf{e} +_\mathsf{b} \mathsf{f})_\alpha(o) = \partial(\mathsf{e})_\alpha(o) = \partial(\mathsf{g})_\alpha(o) = \partial(\mathsf{g} +_\mathsf{b} \mathsf{h})_\alpha(o)$$

同理，对于所有 $\mathsf{p} \in$ 动作集以及 $Q \in \mathtt{Exp}/R$，我们有

$$\partial(\mathsf{e} +_\mathsf{b} \mathsf{f})_\alpha[\{\mathsf{p}\} \times Q] = \partial(\mathsf{e})_\alpha[\{\mathsf{p}\} \times Q] = \partial(\mathsf{g})_\alpha[\{\mathsf{p}\} \times Q] = \partial(\mathsf{g} +_\mathsf{b} \mathsf{h})_\alpha[\{\mathsf{p}\} \times Q]$$

¯当 $\alpha \leq_{\mathsf{BA}} \mathsf{b}$ 时，证明过程类似。

现在，我们希望证明 (e;f,g;h) $\in \Phi_\partial(R)$。在处理引理 38 中的等价关系时，我们不采用 Φ 更简单的刻画，而是验证定义 9 的条件。对于所有 $\alpha \in$At，我们有

$$\partial(\mathsf{e}\,;\mathsf{f})_\alpha(\checkmark) = \partial(\mathsf{e})_\alpha(\checkmark)\partial(\mathsf{f})_\alpha(\checkmark) = \partial(\mathsf{g})_\alpha(\checkmark)\partial(\mathsf{h})_\alpha(\checkmark) = \partial(\mathsf{e}\,;\mathsf{f})_\alpha(\checkmark)$$

对于所有 $\alpha \in$ 原子 和 $\alpha \in \{\} +$ 输出，均有。

$$\begin{aligned}\partial(\mathsf{e}\,;\mathsf{f})_\alpha(o) &= \partial(\mathsf{e})_\alpha(o) + \partial(\mathsf{e})_\alpha(\checkmark)\partial(\mathsf{f})_\alpha(o)\\ &= \partial(\mathsf{g})_\alpha(o) + \partial(\mathsf{g})_\alpha(\checkmark)\partial(\mathsf{h})_\alpha(o)\\ &= \partial(\mathsf{g}\,;\mathsf{h})_\alpha(o)\end{aligned}$$

现在，我们使用引理41和引理 42 来证明，对于所有 $\alpha \in$ 动作集、$\mathsf{p} \in$ 动作集和 $A \subseteq \mathtt{Exp}$

$$\begin{aligned}\partial(\mathsf{e}\,;\mathsf{f})_\alpha[\{\mathsf{p}\} \times A] &= \partial(\mathsf{e})_\alpha[\{\mathsf{p}\} \times A/\mathsf{f}] + \partial(\mathsf{e})_\alpha(\checkmark)\partial(\mathsf{f})_\alpha[\{\mathsf{p}\} \times A]\\ &\le \partial(\mathsf{g})_\alpha[\{\mathsf{p}\} \times R(A/\mathsf{f})] + \partial(\mathsf{g})_\alpha(\checkmark)\partial(\mathsf{h})_\alpha[\{\mathsf{p}\} \times R(A)]\\ &\le \partial(\mathsf{g})_\alpha[\{\mathsf{p}\} \times R(A)/\mathsf{g}] + \partial(\mathsf{g})_\alpha(\checkmark)\partial(\mathsf{h})_\alpha[\{\mathsf{p}\} \times R(A)]\\ &= \partial(\mathsf{g}\,;\mathsf{h})_\alpha[\{\mathsf{p}\} \times R(A)]\end{aligned}$$

对任意 $B \subseteq \mathtt{Exp}$， $\partial(\mathsf{g}\,;\mathsf{h})_\alpha[\{\mathsf{p}\} \times B] \le \partial(\mathsf{g}\,;\mathsf{h})_\alpha[\{\mathsf{p}\} \times R^{-1}(B)]$ 的证明类似。

<escape></escape>现在，考虑证明 <escape>(</escape><escape>e</escape>$^{(b)}$<escape>,</escape><escape>f</escape>$^{(b)}$<escape>) </escape> $\in \Phi_\partial$<escape>(</escape><escape>)</escape><escape>。首先，假设 </escape><escape>b</escape><escape>。在这种情况下，我们有：</escape>

$$\partial(\mathsf{e}^{(b)})_\alpha(\checkmark) = 1 = \partial(\mathsf{g}^{(b)})_\alpha(\checkmark)$$

由于所有概率质量都分配给元素 $\checkmark$，因此 Φ_∂的所有其余条件都立即得到满足。现在，假设 $\alpha \le_{\mathsf{BA}} \mathsf{b}$。首先，考虑以下子情况：$\partial(\mathsf{e})_\alpha(\checkmark) = 1$。由于 (e,g) $\in \Phi_\partial(R)$，这意味着 $\partial(\mathsf{g})_\alpha(\checkmark) = 1$。因此，

$$\partial(\mathsf{e}^{(b)})_\alpha(x) = 1 = \partial(\mathsf{g}^{(b)})_\alpha(x)$$

因此，在这种子情形下，我们有 (e$^{(b)}$,g$^{(b)}$) $\in \Phi_\partial(R)$。对于本情形的其余部分，我们可以安全地假设 $\partial(\mathsf{e})_\alpha(\checkmark) < 1$ 且 $\partial(\mathsf{g})_\alpha(\checkmark) < 1$。我们有：

$$\partial(\mathsf{e}^{(b)})_\alpha(\checkmark) = 0 = \partial(\mathsf{g}^{(b)})_\alpha(\checkmark)$$

对于所有 $o \in \{x\} +$输出，都成立如下结论。

$$\partial(\mathsf{e}^{(b)})_\alpha(o) = \frac{\partial(\mathsf{e})_\alpha(o)}{1-\partial(\mathsf{e})_\alpha(\checkmark)} = \frac{\partial(\mathsf{g})_\alpha(o)}{1-\partial(\mathsf{g})_\alpha(\checkmark)} = \partial(\mathsf{g}^{(b)})_\alpha(o)$$

再次，我们使用引理41来证明，对于任意的 $\mathsf{p} \in$ 动作集 和 $A \subseteq \mathtt{Exp}$，我们有

$$\begin{aligned}
\partial(\mathsf{e}^{(\mathsf{b})})_\alpha[\{\mathsf{p}\} \times A] &= \sum_{\mathsf{a} \in A} \partial(\mathsf{e}^{(\mathsf{b})})_\alpha(\mathsf{p}, \mathsf{a}) \\
&= \sum_{\mathsf{a}_0;\mathsf{e}^{(\mathsf{b})} \in A} \frac{\partial(\mathsf{e})_\alpha(\mathsf{p}, \mathsf{a}_0)}{1 - \partial(\mathsf{e})_\alpha(\checkmark)} \\
&= \frac{1}{1 - \partial(\mathsf{g})_\alpha(\checkmark)} \partial(\mathsf{e})_\alpha[\{\mathsf{p}\} \times A/\mathsf{e}^{(\mathsf{b})}] \\
&\leq \frac{1}{1 - \partial(\mathsf{g})_\alpha(\checkmark)} \partial(\mathsf{g})_\alpha[\{\mathsf{p}\} \times R(A/\mathsf{e}^{(\mathsf{b})})] \\
&\leq \frac{1}{1 - \partial(\mathsf{e})_\alpha(\checkmark)} \partial(\mathsf{g})_\alpha[\{\mathsf{p}\} \times R(A)/\mathsf{g}^{(\mathsf{b})}] \\
&= \sum_{\mathsf{a}_0;\mathsf{g}^{(\mathsf{b})} \in R(A)} \frac{\partial(\mathsf{g})_\alpha(\mathsf{p}, \mathsf{a}_0)}{1 - \partial(\mathsf{g})_\alpha(\checkmark)} \\
&= \partial(\mathsf{g}^{(\mathsf{b})})_\alpha[\{\mathsf{p}\} \times R(A)]
\end{aligned}$$

证明 $\partial(\mathsf{g}^{(\mathsf{b})})[\{\mathsf{p}\} \times B] \leq \partial(\mathsf{e}^{(\mathsf{b})})_\alpha[\{\mathsf{p}\} \times R^{-1}(B)]$ 对任意 $B \subseteq \mathtt{Exp}$ 和 $\mathsf{p} \in$ 动作集 都是对称的。我们得出 $(\mathsf{e}^{(\mathsf{b})}, \mathsf{g}^{(\mathsf{b})}) \in \Phi_\partial(R)$。

最后，为了证明 $(\mathsf{e}^{[r]}, \mathsf{g}^{[r]}) \in \Phi_\partial(R)$，我们首先考虑 $r = 1$ and$\partial(\mathsf{e})_\alpha(\checkmark) = 1$ 的子情况。在这里，我们还可知 $\partial(\mathsf{g})_\alpha(\checkmark) = 1$。因此，我们有

$$\partial(\mathsf{e}^{[r]})_\alpha(\mathsf{x}) = 1 = \partial(\mathsf{g}^{[r]})_\alpha(\mathsf{x})$$

这足以表明，在该子情形中确实有 $(\mathsf{e}^{[r]}, \mathsf{g}^{[r]}) \in \Phi_\partial(R)$。对于其余情况，我们可以放心地假设 $r\partial(\mathsf{e})_\alpha(\checkmark) \neq 1$，因此 $\partial(\mathsf{g})_\alpha(\checkmark)$ 也成立。我们有，

$$\partial(\mathsf{e}^{[r]})_\alpha(\checkmark) = 1 - r = \partial(\mathsf{g}^{[\mathsf{r}]})_\alpha(\checkmark)$$

对于所有 $o \in \{\ \} + 输出$，我们都有

$$\partial(\mathsf{e}^{[r]})_\alpha(o) = \frac{r\partial(\mathsf{e})_\alpha(o)}{1 - r\partial(\mathsf{e})_\alpha(\checkmark)} = \frac{r\partial(\mathsf{g})_\alpha(o)}{1 - r\partial(\mathsf{g})_\alpha(\checkmark)} = \partial(\mathsf{g}^{[r]})_\alpha(o)$$

最后，我们使用引理41证明，对于任意 $\mathsf{p} \in$动作集 和 $A \subseteq \mathtt{Exp}$，我们有

$$\begin{aligned}
\partial(\mathsf{e}^{[r]})[\{\mathsf{p}\} \times A] &= \sum_{\mathsf{a} \in A} \partial(\mathsf{e}^{[r]})_\alpha(\mathsf{p}, \mathsf{a}) \\
&= \frac{r}{1 - r\partial(\mathsf{e})_\alpha(\checkmark)} \sum_{\mathsf{a}_0;\mathsf{e}^{[r]}} \partial(\mathsf{e})_\alpha(\mathsf{p}, \mathsf{a}_0) \\
&= \frac{r}{1 - r\partial(\mathsf{e})_\alpha(\checkmark)} \partial(\mathsf{e}^{[r]})_\alpha[\{\mathsf{p}\} \times A/\mathsf{e}^{[r]}] \\
&\leq \frac{r}{1 - r\partial(\mathsf{e})_\alpha(\checkmark)} \partial(\mathsf{e}^{[r]})_\alpha[\{\mathsf{p}\} \times R(A/\mathsf{e}^{[r]})] \\
&\leq \frac{r}{1 - r\partial(\mathsf{g})_\alpha(\checkmark)} \partial(\mathsf{g}^{[r]})_\alpha[\{\mathsf{p}\} \times R(A)/\mathsf{g}^{[r]}] \\
&= \partial(\mathsf{g}^{[r]})_\alpha[\mathsf{p} \times R(A)]
\end{aligned}$$

证明对于任意 $B \subseteq \mathtt{Exp}$ 和 $\mathsf{p} \in$ 动作集，$\partial(\mathsf{g}^{[r]})_\alpha[\{\mathsf{p}\} \times B] \leq \partial(\mathsf{e}^{[r]})_\alpha[\{\mathsf{p}\} \times R^{-1}(B)]$ 的情形是对称的，故略去。因此，$(\mathsf{e}^{[r]}, \mathsf{g}^{[r]}) \in \Phi_\partial(R)$。◀

▶ **定理 11.** （$\mathtt{Exp}, \partial$）上的最大双模拟是关于ProbGKAT 运算的同余关系。

证明。 注意， Exp 上的全关系是一个同余关系。由于 Φ_∂ 保持同余关系，而同余关系在求交后也保持不变 [15,定理 5。3],根据 Φ_∂的最大不动点刻画， （Exp， ∂）上的最大双模拟是一个同余关系。◀

D 第 5 节的证明

▶ **引理 44.** 令 $\mathsf{e} \in \mathtt{Exp}$ 且 $\alpha \in$ 原子。成立的是，$\mathsf{E}(\mathsf{e})_\alpha = \partial(\mathsf{e})\alpha(\checkmark)$。

证明。 对 $\mathsf{e} \in \mathtt{Exp}$的构造进行归纳。基例显然成立。首先，考虑 $\mathsf{e} = \mathsf{f} +_\mathsf{b} \mathsf{g}$ 对于某个测试 $\mathsf{b} \in \mathtt{BExp}$的情形。假设 $\alpha \leq_{\mathsf{BA}} \mathsf{b}$；那么

$$\begin{aligned}
\mathsf{E}(\mathsf{f} +_\mathsf{b} \mathsf{g})_\alpha &= \mathsf{E}(\mathsf{f}) && (\alpha \leq_{\mathsf{BA}} \mathsf{b}) \\
&= \partial(\mathsf{f})_\alpha(\checkmark) && (\text{Induction hypothesis}) \\
&= \partial(\mathsf{f} +_\mathsf{b} \mathsf{g})_\alpha(\checkmark) && (\alpha \leq_{\mathsf{BA}} \mathsf{b})
\end{aligned}$$

¯当 $\alpha \leq_{\mathsf{BA}} \mathsf{b}$ 时，情形对称。
现在，令 $\mathsf{e} = \mathsf{f} \oplus_r \mathsf{g}$，其中 $r \in [0,1]$。我们有

$$\begin{aligned}
\mathsf{E}(\mathsf{f} \oplus_r \mathsf{g})_\alpha &= r\mathsf{E}(\mathsf{f})_\alpha + (1-r)\mathsf{E}(\mathsf{g})_\alpha && (\text{Def. of } \mathsf{E}) \\
&= r\partial(\mathsf{f})_\alpha(\checkmark) + (1-r)\partial(\mathsf{g})_\alpha(\checkmark) && (\text{Induction hypothesis}) \\
&= \partial(\mathsf{f} \oplus_r \mathsf{g})_\alpha(\checkmark) && (\text{Def. of } \partial)
\end{aligned}$$

如果 $\mathsf{e} = \mathsf{f}\,;\mathsf{g}$，那么我们有

$$\begin{aligned}
\mathsf{E}(\mathsf{f}\,;\mathsf{g})_\alpha &= \mathsf{E}(\mathsf{f})_\alpha\, \mathsf{E}(\mathsf{g})_\alpha && (\text{Def. of } \mathsf{E}) \\
&= \partial(\mathsf{f})_\alpha(\checkmark)\partial(\mathsf{g})_\alpha(\checkmark) && (\text{Induction hypothesis}) \\
&= \partial(\mathsf{f}\,;\mathsf{g})_\alpha(\checkmark) && (\text{Def. of } \partial)
\end{aligned}$$

至于循环，我们先考虑 $\mathsf{e} = \mathsf{f}^{(\mathsf{b})}$ 对于某个测试 $\mathsf{b} \in \mathtt{BExp}$的情形。首先，考虑¯当 $\alpha \leq_{\mathsf{BA}} \mathsf{b}$时的情形。根据 ∂ 的定义，立即可得

$$\mathsf{E}\left(\mathsf{f}^{(\mathsf{b})}\right)_\alpha = 1 = \partial(\mathsf{e}^{(\mathsf{b})})_\alpha(\checkmark)$$

同样地，在 $\alpha \leq_{\mathsf{BA}} \mathsf{b}$的情形下，根据 ∂ 的定义可得

$$\mathsf{E}\left(\mathsf{f}^{(\mathsf{b})}\right)_\alpha = 0 = \partial(\mathsf{f}^{(\mathsf{b})})_\alpha(\checkmark)$$

最后，考虑概率循环 $\mathsf{e} = \mathsf{f}^{[r]}$，其中 $r = 1$。首先，考虑当 $\mathsf{E}(f)_\alpha = 1$ 且 $r = 1$时的情形。根据归纳假设，我们有 $\partial(\mathsf{f})\alpha(\checkmark) = 1$。在这种情况下，根据 ∂ 的定义，我们有 $\partial(\mathsf{f}^{[r]})\alpha(\checkmark) = 0$，因此

$$\mathsf{E}\left(\mathsf{f}^{[r]}\right)_\alpha = 0 = \partial(\mathsf{f}^{[r]})_\alpha(\checkmark)$$

对于剩余情形，我们有

$$\begin{aligned}
\mathsf{E}\left(\mathsf{f}^{[r]}\right)_\alpha &= \frac{1-r}{1-r\mathsf{E}(\mathsf{f})_\alpha} && (\text{Def. of } \mathsf{E}) \\
&= \frac{1-r}{1-r\partial(\mathsf{f})_\alpha(\checkmark)} && (\text{归纳假设}) \\
&= \partial(\mathsf{f}^{[r]})_\alpha(\checkmark) && (\text{Def. of } \partial)
\end{aligned}$$

◀

▶ **引理 45**。 设 $R \subseteq \mathrm{Exp} \times \mathrm{Exp}$ 是关于 ProbGKAT 算子的同余关系，使得 $(\mathsf{e},\mathsf{f}) \in R$，并设 $Q \in \mathrm{Exp}/R$ 是 R的一个等价类。则有 $Q/\mathsf{e} = Q/\mathsf{f}$

证明。 设 $\mathsf{g} \in Q$。由于 R是同余关系，且 $(\mathsf{e},\mathsf{f}) \in R$，因此有 $(\mathsf{g};\mathsf{e}, \mathsf{g};\mathsf{f}) \in R$。因此，

$$\mathsf{g} \in Q/\mathsf{e} \iff \mathsf{g};\mathsf{e} \in Q \iff \mathsf{g};\mathsf{f} \in Q \iff \mathsf{g} \in Q/\mathsf{f}$$ ◀

▶ **引理 46**。 设 $\mathsf{e},\mathsf{f} \in \mathrm{Exp}$ 且设 $Q \in \mathrm{Exp}/\equiv$。现在 $(Q/\mathsf{f})/\mathsf{e} = Q/\mathsf{e};\mathsf{f}$

证明。 设 $\mathsf{g} \in Q$；推导如下

$$\mathsf{g} \in (Q/\mathsf{f})/\mathsf{e} \iff \mathsf{g};\mathsf{e} \in Q/\mathsf{f} \iff (\mathsf{g};\mathsf{e});\mathsf{f} \in Q \iff \mathsf{g};(\mathsf{e};\mathsf{f}) \in Q \iff \mathsf{g} \in Q/\mathsf{e};\mathsf{f}$$

这里，倒数第二步由结合律得出。 ◀

▶ **引理 47**。 设 (X,β) 是任意的 G-余代数，$x, y \in X$ 且 $R \subseteq X \times X$ 是 X上的一个等价关系。若对所有 $\alpha \in$ 原子，$\beta(x)_\alpha = \beta(y)_\alpha$ 则 $(x,y) \in \Phi_\beta(R)$

证明。 注意，若对所有 $\alpha \in$原子 分布 $\beta(x)_\alpha$ 和 $\beta(y)_\alpha$ 均相等，则引理 38 的条件立即成立。 ◀

▶ **引理 48**。 设 $\mathsf{e} \in \mathrm{Exp}$ 且 $\mathsf{b} \in \mathrm{BExp}$。若 $\alpha \leq_{\mathrm{BA}} \mathsf{b}$，则 $\partial(\mathsf{b};\mathsf{e})_\alpha = \partial(\mathsf{e})_\alpha$。

证明。 回忆一下，$\partial(\mathsf{b};\mathsf{e})_\alpha = \partial(\mathsf{b})_\alpha \lhd_\alpha \mathsf{e}$. 若 $\alpha \leq_{\mathrm{BA}} \mathsf{b}$，则 $\partial(\mathsf{b})_\alpha(\checkmark) = 1$。由于 $(- \lhd_\alpha \mathsf{e})$ 是映射 $c_{\alpha,\mathsf{e}}\colon 2 + \text{输出} + \text{动作集} \times \mathrm{Exp} \to \mathcal{D}\omega(2 + \text{输出} + \text{动作集} \times \mathrm{Exp})$ 的凸扩张，并满足 $c_{\alpha,\mathsf{e}}(\checkmark) = \partial(\mathsf{e})_\alpha$，因此我们有

$$\partial(\mathsf{b})_\alpha \lhd_\alpha \mathsf{e} = 1\partial(\mathsf{f})_\alpha = \partial(\mathsf{f})_\alpha$$ ◀

▶ **引理 12**。 $\equiv$ 是 (Exp,∂) 上的双模拟等价

证明。 根据引理 36，只需证明 $\equiv \subseteq \Phi_\partial(\equiv)$。我们将交替使用 $\Phi_\partial(\equiv)$的不同刻画，包括定义 9、引理 38 和引理 47。

我们对 $\equiv$的推导长度进行归纳。等式公理是基例，而准等式公理是归纳步骤。我们无需验证 $\equiv$的同余规则，因为根据引理 43，$\Phi_\partial(\equiv)$ 也是一种同余关系。

设 e、f、$\mathsf{g} \in \mathrm{Exp}$、$\mathsf{b}$、$\mathsf{c} \in \mathrm{BExp}$，$v \in$输出 和 r，$s \in [0,1]$。可靠性 守卫选择公理、概率选择公理 和 分配公理 可利用引理 47 证明，只需证明导数给出的每个分布都相等。

(G1) 如果 $\alpha \leq_{\mathrm{BA}} \mathsf{b}$，那么 $\partial(\mathsf{e} +_\mathsf{b} \mathsf{e})_\alpha = \partial(\mathsf{e})_\alpha$。因此，对于所有 $\alpha \in$原子，$\bar{\partial}(\mathsf{e} +_\mathsf{b} \mathsf{e})_\alpha = \partial(\mathsf{e})_\alpha$。

(G2) 若 $\alpha \leq_{\mathrm{BA}} \mathsf{b}$，则 $\partial(\mathsf{e} +_\mathsf{b} \mathsf{f})_\alpha = \partial(\mathsf{e})_\alpha$。由引理 48 可得 $\partial(\mathsf{e})_\alpha = \partial(\mathsf{b};\mathsf{e})_\alpha$，因此 $\partial(\mathsf{e} +_\mathsf{b} \mathsf{f})_\alpha = \partial(\mathsf{b};\mathsf{e} +_\mathsf{b} \mathsf{f})_\alpha$。若 $\alpha \leq \mathsf{b}$，则 $\partial(\mathsf{e} +_\mathsf{b} \mathsf{f})_\alpha = \partial(\mathsf{f})_\alpha = \partial(\mathsf{b};\mathsf{e} +_\mathsf{b} \mathsf{f})_\alpha$

(G3) 如果 $\alpha \leq_{\mathrm{BA}} \mathsf{b}$，那么 $\partial(\mathsf{e} +_\mathsf{b} \mathsf{f})_\alpha = \partial(\mathsf{f})_\alpha$。类似地，如果 $\alpha \leq_{\mathrm{BA}} \bar{\mathsf{b}}$，则 $\partial(\mathsf{e} +_\mathsf{b} \mathsf{f})_\alpha = \partial(\mathsf{e})_\alpha = \partial(\mathsf{f} +_{\bar{\mathsf{b}}} \mathsf{e})_\alpha$。

(G4) 若 $\alpha \leq_{\mathrm{BA}} \mathsf{b}$ 且 $\alpha \leq_{\mathrm{BA}} \mathsf{c}$，则 $\alpha \leq_{\mathrm{BA}} \mathsf{bc}$，因此

$$\partial((\mathsf{e} +_\mathsf{b} \mathsf{f}) +_\mathsf{c} \mathsf{g})_\alpha = \partial(\mathsf{e})_\alpha = \partial(\mathsf{e} +_{\mathsf{bc}} (\mathsf{f} +_\mathsf{c} \mathsf{g}))_\alpha$$

现在，令 $\alpha \leq_{\mathrm{BA}} \mathsf{b}$ 和 $\alpha \leq_{\mathrm{BA}} \mathsf{c}$。在这种情况下，$\alpha \leq_{\mathrm{BA}} \overline{\mathsf{bc}}$ 和 $\alpha \leq_{\mathrm{BA}} \mathsf{c}$，因此

$$\partial((\mathsf{e} +_\mathsf{b} \mathsf{f}) +_\mathsf{c} \mathsf{g})_\alpha = \partial(\mathsf{f})_\alpha = \partial(\mathsf{e} +_{\mathsf{bc}} (\mathsf{f} +_\mathsf{c} \mathsf{g}))_\alpha$$

<escape>最后，当 $\alpha \leq_{\mathrm{BA}} \bar{\mathsf{c}}$ 时，我们有 $\alpha \leq \overline{\mathsf{bc}}$，因此</escape>

$$\partial((\mathsf{e} +_\mathsf{b} \mathsf{f}) +_\mathsf{c} \mathsf{g})_\alpha = \partial(\mathsf{g})_\alpha = \partial(\mathsf{e} +_{\mathsf{bc}} (\mathsf{f} +_\mathsf{c} \mathsf{g}))_\alpha$$

(P1) 对于所有 $\alpha \in$ 原子， $\partial(\mathsf{e} \oplus_r \mathsf{e})_\alpha = r\partial(\mathsf{e})_\alpha + (1-r)\partial(\mathsf{e})_\alpha = \partial$
$(\mathsf{e})_\alpha$(P2) 对于所有 $\alpha \in$ 原子， $\partial(\mathsf{e} \oplus_1 \mathsf{f})_\alpha = 1\partial(\mathsf{e})_\alpha + 0\partial(\mathsf{f})_\alpha = \partial$
$(\mathsf{e})_\alpha$(P3) 对于所有 $\alpha \in$原子，

$$\begin{aligned}\partial(\mathsf{e} \oplus_r \mathsf{f})_\alpha &= r\partial(\mathsf{e})_\alpha + (1-r)\partial(\mathsf{f})_\alpha \\ &= (1-r)\partial(\mathsf{f})_\alpha + (1-(1-r))\partial(\mathsf{e})_\alpha \\ &= \partial(\mathsf{f} \oplus_{1-r} \mathsf{e})_\alpha\end{aligned}$$

(P4) 请注意，根据假设 $rs \neq 1$。对于所有 $\alpha \in$ 原子，

$$\begin{aligned}\partial((\mathsf{e} \oplus_r \mathsf{f}) \oplus_s \mathsf{g})_\alpha &= rs\partial(\mathsf{e})_\alpha + (1-r)s\partial(\mathsf{f})_\alpha + (1-s)\partial(\mathsf{g})_\alpha \\ &= rs\partial(\mathsf{e})_\alpha + (1-rs)\left(\frac{(1-r)s}{1-rs}\partial(\mathsf{f})_\alpha + \frac{1-s}{1-rs}\partial(\mathsf{g})_\alpha\right)\end{aligned}$$

令 $t = \frac{(1-r)s}{1-rs}$。因此，前者等于

$$rs\partial(\mathsf{e})_\alpha + (1-rs)\left(t\partial(\mathsf{f})_\alpha + (1-t)\partial(\mathsf{g})_\alpha\right) = \partial(\mathsf{e} \oplus_{rs} (\mathsf{f} \oplus_t \mathsf{g}))_\alpha$$

(D) 对于 $\alpha \leq_{\mathsf{BA}} \mathsf{b}$，我们有

$$\partial(\mathsf{e} \oplus_r (\mathsf{f} +_\mathsf{b} \mathsf{g}))_\alpha = r\partial(\mathsf{e})_\alpha + (1-r)\partial(\mathsf{f})_\alpha = \partial((\mathsf{e} +_\mathsf{b} \mathsf{f}) \oplus_r (\mathsf{e} +_\mathsf{b} \mathsf{g}))_\alpha$$

类似地，当 $\alpha \leq_{\mathsf{BA}} \mathsf{b}$时，我们有

$$\partial(\mathsf{e} \oplus_r (\mathsf{f} +_\mathsf{b} \mathsf{g}))_\alpha = r\partial(\mathsf{e})_\alpha + (1-r)\partial(\mathsf{g})_\alpha = \partial((\mathsf{e} +_\mathsf{b} \mathsf{f}) \oplus_r (\mathsf{e} +_\mathsf{b} \mathsf{g}))_\alpha$$

至于序列公理，我们将根据具体情况，使用引理 38 和 Lemma47 对 $\Phi_\partial(\equiv)$ 的刻画。

(S1) 由于对所有 $\alpha \in$原子，我们有 $\alpha \leq_{\mathsf{BA}} 1$，因此可以立即使用引理 48 证明 $\partial(1\,;\,\mathsf{e})_\alpha = \partial(\mathsf{e})_\alpha$。由引理 47 可知 $(1\,;\,\mathsf{e},\ \mathsf{e}) \in \Phi_\partial(\equiv)$
(S2) 我们验证引理 38 的条件。令 $\alpha \in$原子。

1. 对于所有 $o \in \{\checkmark\} +$输出，我们有

$$\partial(\mathsf{e}\,;1)_\alpha(o) = \partial(\mathsf{e})_\alpha(o) + \partial(\mathsf{e})_\alpha(\checkmark)\partial(1)_\alpha(o) = \partial(\mathsf{e})_\alpha(o)$$

在剩余的情况下，我们有

$$\partial(\mathsf{e}\,;1)_\alpha(\checkmark) = \partial(\mathsf{e})_\alpha(\checkmark)\partial(1)_\alpha(\checkmark) = \partial(\mathsf{e})_\alpha(\checkmark)$$

2. 令 $\mathsf{p} \in$动作集 和 $Q \in \mathsf{Exp}/\equiv$ 为 $\equiv$的一个等价类。由引理 42 可知

$$\begin{aligned}\partial(\mathsf{e}\,;1)_\alpha[\{\mathsf{p}\} \times Q] &= \partial(\mathsf{e})_\alpha[\{\mathsf{p}\} \times Q/1] + \partial(\mathsf{e})_\alpha(\checkmark)\partial(1)_\alpha[\{p\} \times Q] \\ &= \partial(\mathsf{e})_\alpha[\{\mathsf{p}\} \times Q/1]\end{aligned}$$

注意，由于 Q 是关系 $\equiv$的一个等价类，我们有

$$\mathsf{h} \in Q/1 \iff \mathsf{h}\,;1 \in Q \iff \mathsf{h} \in Q$$

由于 $Q = Q/1$，我们有

$$\partial(\mathsf{e}\,;1)_\alpha[\{\mathsf{p}\} \times Q] = \partial(\mathsf{e})_\alpha[\{\mathsf{p}\} \times Q]$$

(S3) 我们验证引理 38 的条件。令 $\alpha \in$原子。

34 模双模拟的概率守卫 KAT：完备性与复杂性

1. 对于所有 $o \not\propto \{\,\} + $输出，我们有

$$\begin{aligned}\partial((\mathsf{e}\,;\mathsf{f})\,;\mathsf{g})_\alpha(o) &= \partial(\mathsf{e}\,;\mathsf{f})_\alpha(o) + \partial(\mathsf{e}\,;\mathsf{f})_\alpha(\checkmark)\partial(\mathsf{g})_\alpha(o)\\ &= \partial(\mathsf{e})_\alpha(o) + \partial(\mathsf{e})_\alpha(\checkmark)\partial(\mathsf{f})_\alpha(o) + \partial(\mathsf{e}\,;\mathsf{f})_\alpha(\checkmark)\partial(\mathsf{g})_\alpha(o)\\ &= \partial(\mathsf{e})_\alpha(o) + \partial(\mathsf{e})_\alpha(\checkmark)\partial(\mathsf{f})_\alpha(o) + \partial(\mathsf{e})_\alpha(\checkmark)\partial(\mathsf{f})_\alpha(\checkmark)\partial(\mathsf{g})_\alpha(o)\\ &= \partial(\mathsf{e}\,;(\mathsf{f}\,;\mathsf{g}))_\alpha(o)\end{aligned}$$

在剩余的情况下，我们有

$$\partial((\mathsf{e}\,;\mathsf{f})\,;\mathsf{g})_\alpha(\checkmark) = \partial(\mathsf{e})_\alpha(\checkmark)\partial(\mathsf{f})_\alpha(\checkmark)\partial(\mathsf{g})_\alpha(\checkmark) = \partial(\mathsf{e}\,;(\mathsf{f}\,;\mathsf{g}))_\alpha(\checkmark)$$

2. 令 $\mathsf{p} \in$动作集 且 $Q \in \mathrm{Exp}/\equiv$。根据引理 42 和引理 46，

$$\begin{aligned}\partial((\mathsf{e}\,;\mathsf{f})\,;\mathsf{g})_\alpha[\{\mathsf{p}\}\times Q] &= \partial(\mathsf{e}\,;\mathsf{f})_\alpha[\{\mathsf{p}\}\times Q/\mathsf{g}] + \partial(\mathsf{e}\,;\mathsf{f})_\alpha(\checkmark)\partial(\mathsf{g})_\alpha[\{\mathsf{p}\}\times Q]\\ &= \partial(\mathsf{e})_\alpha[\{\mathsf{p}\}\times (Q/\mathsf{f})/\mathsf{g}] + \partial(\mathsf{e})_\alpha(\checkmark)\partial(\mathsf{f})_\alpha[\{\mathsf{p}\}\times Q/\mathsf{g}]\\ &\quad + \partial(\mathsf{e})_\alpha(\checkmark)\partial(\mathsf{f})_\alpha(\checkmark)\partial(\mathsf{g})_\alpha[\{p\}\times Q]\\ &= \partial(\mathsf{e})_\alpha[\{\mathsf{p}\}\times Q/\mathsf{f}\,;\mathsf{g}] + \partial(\mathsf{e})_\alpha(\checkmark)\partial(\mathsf{f}\,;\mathsf{g})_\alpha[\{\mathsf{p}\}\times Q]\\ &= \partial(\mathsf{e}\,;(\mathsf{f}\,;\mathsf{g}))_\alpha[\{\mathsf{p}\}\times Q]\end{aligned}$$

(S4) 对于所有 $\alpha \in$原子，我们有

$$\partial(0\,;\mathsf{e})_\alpha(\checkmark) = \partial(0)_\alpha(\checkmark) + \partial(0)_\alpha(\checkmark)\partial(\mathsf{e})_\alpha(\checkmark) = \partial(0)_\alpha(\checkmark) = 1$$

其余所有元素 $2 +$ 输出 $+$ 动作集 $\times\,\mathrm{Exp}$ 均未被这些分布赋予概率质量。因此，对于所有 $\alpha \in$ 原子，$\partial(1\,;\mathsf{e})_\alpha = \partial(0)_\alpha$。因此，我们可以使用引理 47 得到所需结果。

(S5) 我们使用引理 38。设 $\alpha \leq_{\mathsf{BA}} \mathsf{b}$。

1. 设 $o \in \{\,\} +$输出。我们有

$$\begin{aligned}\partial((\mathsf{e} +_{\mathsf{b}} \mathsf{f})\,;\mathsf{g})_\alpha(o) &= \partial(\mathsf{e} +_{\mathsf{b}} \mathsf{f})_\alpha(o) + \partial(\mathsf{e} +_{\mathsf{b}} \mathsf{f})_\alpha(\checkmark)\partial(\mathsf{g})_\alpha(o)\\ &= \partial(\mathsf{e})_\alpha(o) + \partial(\mathsf{e})_\alpha(\checkmark)\partial(\mathsf{g})_\alpha(o)\\ &= \partial(\mathsf{e}\,;\mathsf{g} +_{\mathsf{b}} \mathsf{f}\,;\mathsf{g})_\alpha(o)\end{aligned}$$

对于剩余的情形，我们有

$$\begin{aligned}\partial((\mathsf{e} +_{\mathsf{b}} \mathsf{f})\,;\mathsf{g})_\alpha(\checkmark) &= \partial(\mathsf{e} +_{\mathsf{b}} \mathsf{f})_\alpha(\checkmark)\partial(\mathsf{g})_\alpha(\checkmark)\\ &= \partial(\mathsf{e})_\alpha(\checkmark)\partial(\mathsf{g})_\alpha(\checkmark)\\ &= \partial(\mathsf{e}\,;\mathsf{g} +_{\mathsf{b}} \mathsf{f}\,;\mathsf{g})_\alpha(\checkmark)\end{aligned}$$

2. 设 $\mathsf{p} \in$动作集 $Q \in \mathrm{Exp}/\equiv$且 。根据引理 42，我们有

$$\begin{aligned}\partial((\mathsf{e} +_{\mathsf{b}} \mathsf{f})\,;\mathsf{g})_\alpha[\{\mathsf{p}\}\times Q] &= \partial(\mathsf{e} +_{\mathsf{b}} \mathsf{f})_\alpha[\{\mathsf{p}\}\times Q/\mathsf{g}] + \partial(\mathsf{e} +_{\mathsf{b}} \mathsf{f})_\alpha(\checkmark)\partial(g)_\alpha[\{\mathsf{p}\}\times Q]\\ &= \partial(\mathsf{e})_\alpha[\{\mathsf{p}\}\times Q/\mathsf{g}] + \partial(\mathsf{e})_\alpha(\checkmark)\partial(g)_\alpha[\{\mathsf{p}\}\times Q]\\ &= \partial(\mathsf{e}\,;\mathsf{g})_\alpha[\{\mathsf{p}\}\times Q]\\ &= \partial(\mathsf{e}\,;\mathsf{g} +_{\mathsf{b}} \mathsf{f}\,;\mathsf{g})_\alpha[\{\mathsf{p}\}\times Q]\end{aligned}$$

¯当 $\alpha \leq_{\mathsf{BA}} \mathsf{b}$ 时，我们省略对称情形 .

(S6) 设 $\alpha \in$原子。与（S5）的情况一样，我们依赖引理 38 和引理 42。

1. 对于所有 $o \not\propto \{\,\} + $输出，我们有

$$\begin{aligned}\partial((\mathsf{e} \oplus_r \mathsf{f})\,;\mathsf{g})_\alpha(o) &= \partial(\mathsf{e} \oplus_r \mathsf{f})_\alpha(o) + \partial(\mathsf{e} \oplus_r \mathsf{f})(\checkmark)\partial(\mathsf{g})(o)\\ &= r\partial(\mathsf{e})_\alpha(o) + (1-r)\partial(\mathsf{f})_\alpha(o)\\ &\quad + (r\partial(\mathsf{e})_\alpha(\checkmark) + (1-r)\partial(\mathsf{f})_\alpha(\checkmark))\,\partial(\mathsf{g})_\alpha(o)\\ &= r\partial(\mathsf{e}\,;g)_\alpha(o) + (1-r)\partial(\mathsf{f}\,;\mathsf{g})_\alpha(o)\\ &= \partial(\mathsf{e}\,;\mathsf{g} \oplus_r \mathsf{f}\,;\mathsf{g})_\alpha(o)\end{aligned}$$

对于剩余的情形，我们有这里只精品

$$\begin{aligned}\partial((\mathsf{e} \oplus_r \mathsf{f})\,;\mathsf{g})_\alpha(o) &= \partial(\mathsf{e} \oplus_r \mathsf{f})_\alpha(\checkmark)\partial(\mathsf{g})_\alpha(\checkmark)\\ &= r\partial(\mathsf{e})_\alpha(\checkmark)\partial(\mathsf{g})_\alpha(\checkmark) + (1-r)\partial(\mathsf{f})_\alpha(\checkmark)\partial(\mathsf{g})_\alpha(\checkmark)\\ &= \partial(\mathsf{e}\,;\mathsf{g} \oplus_r \mathsf{f}\,;\mathsf{g})_\alpha(\checkmark)\end{aligned}$$

2. 令 $\mathsf{p} \in$ 动作集 和 $Q \in \mathbf{Exp}/\equiv_\circ$ 我们有

$$\begin{aligned}&\partial((\mathsf{e} \oplus_r \mathsf{f})\,;\mathsf{g})_\alpha[\{\mathsf{p}\} \times Q] = \partial(\mathsf{e} \oplus_r \mathsf{f})_\alpha[\{\mathsf{p}\} \times Q/\mathsf{g}] + \partial(\mathsf{e} \oplus_r \mathsf{f})_\alpha(\checkmark)\partial(\mathsf{g})_\alpha[\{\mathsf{p}\} \times Q]\\ &= r\left(\partial(\mathsf{e})_\alpha[\{\mathsf{p}\} \times Q/\mathsf{g}] + \partial(\mathsf{e})_\alpha(\checkmark)\partial(\mathsf{g})_\alpha[\{\mathsf{p}\} \times Q]\right)\\ &\quad + (1-r)\left(\partial(\mathsf{f})_\alpha[\{\mathsf{p}\} \times Q/\mathsf{g}] + \partial(\mathsf{f})_\alpha(\checkmark)\partial(\mathsf{g})_\alpha[\{\mathsf{p}\} \times Q]\right)\\ &= r\partial(\mathsf{e}\,;\mathsf{g})_\alpha[\{\mathsf{p}\} \times Q] + (1-r)\partial(\mathsf{f}\,;\mathsf{g})_\alpha[\{\mathsf{p}\} \times Q]\\ &= \partial(\mathsf{e}\,;\mathsf{g} \oplus_r \mathsf{f}\,;\mathsf{g})_\alpha[\{\mathsf{p}\} \times Q]\end{aligned}$$

(S7) 与 (S4) 的推理过程相同

(S8) 我们使用引理 47，并证明对所有 $\alpha \in$原子，分布相等。首先，考虑 $\alpha \leq_{\mathsf{BA}} \mathsf{b}$ 和 $\alpha \leq_{\mathsf{BA}} \mathsf{c}$ 的情形。注意，这等价于 $\alpha \leq_{\mathsf{BA}} \mathsf{bc}$。在这种情况下，我们有：

$$\partial(\mathsf{b}\,;\mathsf{c})_\alpha(\checkmark) = \partial(\mathsf{b})_\alpha(\checkmark)\partial(\mathsf{c})_\alpha(\checkmark) = 1 = \partial(\mathsf{bc})_\alpha(\checkmark)$$

由于两个分布都将全部概率质量赋给同一个元素，因此它们相等。现在，考虑 $\alpha \leq_{\mathsf{BA}} \mathsf{b}$ 的情况。在这种情况下，这意味着 $\alpha \leq_{\mathsf{BA}} \mathsf{bc}$。我们有

$$\partial(\mathsf{b}\,;\mathsf{c})_\alpha(x) = \partial(\mathsf{b})_\alpha(x) + \partial(\mathsf{b})_\alpha(\checkmark)\partial(\mathsf{c})_\alpha(x) = 1 = \partial(\mathsf{bc})_\alpha(x)$$

这足以证明两个分布相等。最后，考虑以下情况当 $\alpha \leq_{\mathsf{BA}} \mathsf{b}$ 和 $\alpha \leq_{\mathsf{BA}} \mathsf{c}$时，这也意味着 $\alpha \leq_{\mathsf{BA}} \mathsf{bc}$。我们再次有

$$\partial(\mathsf{b}\,;\mathsf{c})_\alpha(x) = \partial(\mathsf{b})_\alpha(x) + \partial(\mathsf{b})_\alpha(\checkmark)\partial(\mathsf{c})_\alpha(x) = 1 = \partial(\mathsf{bc})_\alpha(x)$$

这证明两个分布相等。

现在，让我们考虑循环公理。所有情况都将依赖于引理 38。

(L1) 首先，考虑 $\alpha \leq_{\mathsf{BA}} \mathsf{b}$ 的情况。然后，

$$\partial\left(\mathsf{e}^{(\mathsf{b})}\right)_\alpha(\checkmark) = 1 = \partial(1)_\alpha(\checkmark) = \partial\left(\mathsf{e}\,;\mathsf{e}^{(\mathsf{b})} +_{\mathsf{b}} 1\right)_\alpha(\checkmark)$$

由于这两个分布都将全部概率质量赋予 ✓，因此引理 38 的所有条件立即得到满足。对于其余情况，我们假设 $\alpha \leq_{\mathsf{BA}} \mathsf{b}$。首先考虑以下子情况： $\partial(\mathsf{e})_\alpha(\checkmark) = 1$。于是，

$$\partial\left(\mathsf{e}\,;\mathsf{e}^{(\mathsf{b})} +_{\mathsf{b}} 1\right)_\alpha(x) = \partial\left(\mathsf{e}\,;\mathsf{e}^{(\mathsf{b})}\right)_\alpha(x)$$

$$
\begin{aligned}
&= \partial(\mathsf{e})_\alpha(\checkmark)\partial\left(\mathsf{e}^{(\mathsf{b})}\right)(\checkmark) \\
&= \partial(\mathsf{e})_\alpha(\checkmark)\partial\left(\mathsf{e}^{(\mathsf{b})}\right)(\checkmark) \\
&= 1 \\
&= \partial\left(\mathsf{e}^{(\mathsf{b})}\right)_\alpha(\checkmark)
\end{aligned}
$$

由于这两个分布同样都将全部概率质量赋予 ，引理 38 的所有条件均得到满足。对于最后一种情况，我们现在可以假设 $\partial(\mathsf{e})_\alpha(\checkmark) \neq 1$。我们验证引理 38 的所有条件。

1. 对于 $o \in \{\}$ +输出，我们有

$$
\begin{aligned}
\partial\left(\mathsf{e}\,;\mathsf{e}^{(\mathsf{b})} +_{\mathsf{b}} 1\right)_\alpha(o) &= \partial\left(\mathsf{e}\,;\mathsf{e}^{(\mathsf{b})}\right)_\alpha(o) \\
&= \partial(\mathsf{e})_\alpha(o) + \partial(\mathsf{e})_\alpha(\checkmark)\partial\left(\mathsf{e}^{(\mathsf{b})}\right)_\alpha(o) \\
&= \partial(\mathsf{e})_\alpha(o) + \partial(\mathsf{e})_\alpha(\checkmark)\frac{\partial(\mathsf{e})_\alpha(o)}{1-\partial(\mathsf{e})_\alpha(\checkmark)} \\
&= \frac{\partial(\mathsf{e})_\alpha(o)(1-\partial(\mathsf{e})_\alpha(\checkmark)) + \partial(\mathsf{e})_\alpha(\checkmark)\partial(\mathsf{e})_\alpha(o)}{1-\partial(\mathsf{e})_\alpha(\checkmark)} \\
&= \frac{\partial(\mathsf{e})_\alpha(o)}{1-\partial(\mathsf{e})_\alpha(\checkmark)} \\
&= \partial\left(\mathsf{e}^{(\mathsf{b})}\right)_\alpha(o)
\end{aligned}
$$

对于接受的剩余情况，我们有

$$
\begin{aligned}
\partial\left(\mathsf{e}\,;\mathsf{e}^{(\mathsf{b})} +_{\mathsf{b}} 1\right)_\alpha(\checkmark) &= \partial\left(\mathsf{e}\,;\mathsf{e}^{(\mathsf{b})}\right)_\alpha(\checkmark) \\
&= \partial(\mathsf{e})_\alpha(\checkmark)\partial\left(\mathsf{e}^{(\mathsf{b})}\right)_\alpha(\checkmark) \\
&= 0 \\
&= \partial\left(\mathsf{e}^{(\mathsf{b})}\right)_\alpha(\checkmark)
\end{aligned}
$$

2. 令 $\mathsf{p} \in$ 动作集 和 $Q \in \mathtt{Exp}/\equiv$ 为 $\equiv$的一个等价类。我们有

$$
\begin{aligned}
\partial\left(\mathsf{e}\,;\mathsf{e}^{(\mathsf{b})} +_{\mathsf{b}} 1\right)_\alpha[\{\mathsf{p}\} \times Q] &= \partial\left(\mathsf{e}\,;\mathsf{e}^{(\mathsf{b})}\right)_\alpha[\{\mathsf{p}\} \times Q] \\
&= \partial(\mathsf{e})_\alpha[\{\mathsf{p}\} \times Q/\mathsf{e}^{(\mathsf{b})}] + \partial(\mathsf{e})_\alpha(\checkmark)\partial\left(\mathsf{e}^{(\mathsf{b})}\right)_\alpha[\{\mathsf{p}\} \times Q] \\
&= \partial(\mathsf{e})_\alpha[\{\mathsf{p}\} \times Q/\mathsf{e}^{(\mathsf{b})}] + \partial(\mathsf{e})_\alpha(\checkmark)\frac{\partial(\mathsf{e})_\alpha[\{\mathsf{p}\} \times Q/\mathsf{e}^{(\mathsf{b})}]}{1-\partial(\mathsf{e})_\alpha(\checkmark)} \\
&= \frac{\partial(\mathsf{e})_\alpha[\{\mathsf{p}\} \times Q/\mathsf{e}^{(\mathsf{b})}]}{1-\partial(\mathsf{e})_\alpha(\checkmark)} \\
&= \partial\left(\mathsf{e}^{(\mathsf{b})}\right)_\alpha[\{\mathsf{p}\} \times Q]
\end{aligned}
$$

(L2) 首先，考虑 ∂（e）$_\alpha$（✓） $= 1$ 且 $r = 1$的情形。于是，对于所有 $\alpha \in$原子

$$
\begin{aligned}
\partial\left(\mathsf{e}\,;\mathsf{e}^{[r]} \oplus_r 1\right)_\alpha(\checkmark) &= \partial\left(\mathsf{e}\,;\mathsf{e}^{[r]}\right)_\alpha(\checkmark) \\
&= \partial(\mathsf{e})_\alpha(\checkmark) + \partial(\mathsf{e})_\alpha(\checkmark)\partial\left(\mathsf{e}^{[r]}\right)_\alpha(\checkmark)
\end{aligned}
$$

$$= \partial\left(\mathsf{e}^{[r]}\right)_\alpha(\checkmark)$$
$$= 1$$

由于两个分布都将全部概率质量分配给 ✓，引理 38 的所有条件立即得到满足。从现在起，我们可以放心地假设 $r\partial(\mathsf{e})_\alpha(\checkmark) \neq 1$。现在，我们针对所有 $\alpha \in$原子验证引理 38 的所有条件。

1. 令 $o \in \{ \}$✗+ 输出。那么，

$$\begin{aligned}\partial\left(\mathsf{e}\,;\mathsf{e}^{[r]} \oplus_r 1\right)_\alpha(o) &= r\partial\left(\mathsf{e}\,;\mathsf{e}^{[r]}\right)_\alpha(o) + (1-r)\partial(1)_\alpha(o)\\ &= r\partial(\mathsf{e})_\alpha(o) + r\partial(\mathsf{e})_\alpha(\checkmark)\frac{r\partial(\mathsf{e})_\alpha(o)}{1-r\partial(\mathsf{e})_\alpha(\checkmark)}\\ &= \frac{r\partial(\mathsf{e})_\alpha(o)}{1-r\partial(\mathsf{e})_\alpha(\checkmark)}\\ &= \partial\left(\mathsf{e}^{[r]}\right)_\alpha(o)\end{aligned}$$

现在，考虑成功终止的剩余情形。

$$\begin{aligned}\partial\left(\mathsf{e}\,;\mathsf{e}^{[r]} \oplus_r 1\right)_\alpha(\checkmark) &= r\partial\left(\mathsf{e}\,;\mathsf{e}^{[r]}\right) + (1-r)\\ &= r\partial(\mathsf{e})_\alpha(\checkmark)\frac{1-r}{1-r\partial(\mathsf{e})_\alpha(\checkmark)} + (1-r)\\ &= \frac{1-r}{1-r\partial(\mathsf{e})_\alpha(\checkmark)}\\ &= \partial\left(\mathsf{e}^{[r]}\right)_\alpha(\checkmark)\end{aligned}$$

2. 令 $\mathsf{p} \in$ 动作集 并令 $Q \in \mathsf{Exp}/\equiv$ 为 ≡的一个等价类。

$$\begin{aligned}\partial\left(\mathsf{e}\,;\mathsf{e}^{[r]} \oplus_r 1\right)_\alpha[\{\mathsf{p}\}\times Q] &= r\partial\left(\mathsf{e}\,;\mathsf{e}^{[r]}\right)_\alpha[\{\mathsf{p}\}\times Q] + (1-r)\partial(1)_\alpha[\{\mathsf{p}\}\times Q]\\ &= r\partial(\mathsf{e})_\alpha[\{\mathsf{p}\}\times Q/\mathsf{e}^{[r]}] + r\frac{r\partial(\mathsf{e})_\alpha[\{\mathsf{p}\}\times Q/\mathsf{e}^{[r]}]}{1-r\partial(\mathsf{e})_\alpha(\checkmark)}\\ &= \frac{r\partial(\mathsf{e})_\alpha[\{\mathsf{p}\}\times Q/\mathsf{e}^{[r]}]}{1-r\partial(\mathsf{e})_\alpha(\checkmark)}\\ &= \partial\left(\mathsf{e}^{[r]}\right)_\alpha[\{\mathsf{p}\}\times Q]\end{aligned}$$

¯**(L3)** 首先，考虑 $\alpha \leq_{\mathsf{BA}} \mathsf{b}$的情形。那么，

$$\partial\left((\mathsf{e} +_\mathsf{c} 1)^{(\mathsf{b})}\right)_\alpha(\checkmark) = 1 = \partial\left((\mathsf{c}\,;\mathsf{e})^{(\mathsf{b})}\right)_\alpha(\checkmark)$$

由于两个分布都将全部概率质量赋给 ✓，引理 38 的所有条件都立即得到满足。现在，考虑 $\alpha \leq_{\mathsf{BA}} \mathsf{b}$ 且 $\alpha \leq_{\mathsf{BA}}$ ¯c的情形。现在

$$\partial(\mathsf{e} +_\mathsf{c} 1)_\alpha(\checkmark) = \partial(1)_\alpha(\checkmark) = 1$$

因此

$$\begin{aligned}\partial\left((\mathsf{c}\,;\mathsf{e})^{(\mathsf{b})}\right)_\alpha(\mathsf{x}) &= \frac{\partial(\mathsf{c}\,;\mathsf{e})_\alpha(\mathsf{x})}{1-\partial(\mathsf{c}\,;\mathsf{e})_\alpha(\checkmark)}\\ &= \frac{\partial(\mathsf{c})_\alpha(\mathsf{x}) + \partial(\mathsf{c})_\alpha(\checkmark)\partial(\mathsf{e})_\alpha(\mathsf{x})}{1-\partial(\mathsf{c})_\alpha(\checkmark)\partial(\mathsf{e})_\alpha(\checkmark)}\end{aligned}$$

$$
\begin{aligned}
&= 1 \\
&= \partial\left((\mathsf{e} +_{\mathsf{c}} 1)^{(\mathsf{b})}\right)_{\alpha}(\checkmark)
\end{aligned}
$$

与前面的情况类似，两个分布都将全部概率质量分配给 ，因此引理 38 的所有条件都立即得到满足。现在，考虑以下情况：$\alpha \leq_{\mathsf{BA}} \mathsf{b}$ 和 $\alpha \leq_{\mathsf{BA}} \mathsf{c}$。首先，考虑也满足以下条件的子情况： $\partial(\mathsf{e})_{\alpha}(\checkmark) = 1$。注意，在这种情况下，两个 $\partial(\mathsf{e} +_{\mathsf{c}} 1)_{\alpha}(\checkmark) = 1$ 和 $\partial(\mathsf{c}\,;\mathsf{e})_{\alpha}(\checkmark) = 1$，因此我们有：

$$
\partial\left((\mathsf{e} +_{\mathsf{c}} 1)^{(\mathsf{b})}\right)_{\alpha}(\checkmark) = 1 = \partial\left((\mathsf{c}\,;\mathsf{e})^{(\mathsf{b})}\right)_{\alpha}(\checkmark)
$$

两个分布都将全部概率质量赋给同一个元素，因此立即满足引理 38 的要求。对于其余情况，我们现在可以放心地假设 $\partial(\mathsf{e})_{\alpha}(\checkmark) \neq 1$。这一次，我们必须验证引理 38 的所有条件。

1. 对于 $o \in \{\checkmark\}$ +输出，我们有

$$
\begin{aligned}
\partial\left((\mathsf{e} +_{\mathsf{c}} 1)^{(\mathsf{b})}\right)_{\alpha}(o) &= \frac{\partial(\mathsf{e} +_{\mathsf{c}} 1)_{\alpha}(o)}{1 - \partial(\mathsf{e} +_{\mathsf{c}} 1)_{\alpha}(\checkmark)} \\
&= \frac{\partial(\mathsf{e})_{\alpha}(o)}{1 - \partial(\mathsf{e})_{\alpha}(\checkmark)} \\
&= \frac{\partial(\mathsf{c}\,;\mathsf{e})_{\alpha}(o)}{1 - \partial(\mathsf{c}\,;\mathsf{e})_{\alpha}(\checkmark)} && \text{(Lemma 48)} \\
&= \partial\left((\mathsf{c}\,;\mathsf{e})^{(\mathsf{b})}\right)_{\alpha}(\checkmark)
\end{aligned}
$$

在立即接受的剩余情形中，我们有

$$
\partial\left((\mathsf{e} +_{\mathsf{c}} 1)^{(\mathsf{b})}\right)_{\alpha}(\checkmark) = 0 = \partial\left((\mathsf{c}\,;\mathsf{e})^{\mathsf{b}}\right)_{\alpha}(\checkmark)
$$

2. 令 $\mathsf{p} \in$ 动作集且 $Q \in \mathtt{Exp}/\equiv$。对于所有 $\alpha \in$ 原子，我们有

$$
\begin{aligned}
\partial\left((\mathsf{e} +_{\mathsf{c}} 1)^{(\mathsf{b})}\right)_{\alpha}[\{\mathsf{p}\} \times Q] &= \frac{\partial(\mathsf{e} +_{\mathsf{c}} 1)_{\alpha}[\{\mathsf{p}\} \times Q/(\mathsf{e} +_{\mathsf{c}} 1)^{(\mathsf{b})}]}{1 - \partial(\mathsf{e} +_{\mathsf{c}} 1)_{\alpha}(\checkmark)} \\
&= \frac{\partial(\mathsf{e})_{\alpha}[\{\mathsf{p}\} \times Q/(\mathsf{e} +_{\mathsf{c}} 1)^{(\mathsf{b})}]}{1 - \partial(\mathsf{e})_{\alpha}(\checkmark)} \\
&= \frac{\partial(\mathsf{c}\,;\mathsf{e})_{\alpha}[\{\mathsf{p}\} \times Q/(\mathsf{e} +_{\mathsf{c}} 1)^{(\mathsf{b})}]}{1 - \partial(\mathsf{c}\,;\mathsf{e})_{\alpha}(\checkmark)} && \text{(Lemma 48)} \\
&= \frac{\partial(\mathsf{c}\,;\mathsf{e})_{\alpha}[\{\mathsf{p}\} \times Q/(\mathsf{c}\,;\mathsf{e})^{(\mathsf{b})}]}{1 - \partial(\mathsf{c}\,;\mathsf{e})_{\alpha}(\checkmark)} && \text{(Lemma 45)} \\
&= \partial\left((\mathsf{c}\,;\mathsf{e})^{(\mathsf{b})}\right)_{\alpha}[\{\mathsf{p}\} \times Q]
\end{aligned}
$$

(L4) 令 $\alpha \in$ 原子为任意一个原子。首先考虑子情况 $\partial(\mathsf{e})_{\alpha}(\checkmark) = 1$。对于所有 $\alpha \in$原子，我们有

$$
\partial\left(\mathsf{e}^{(1)}\right)_{\alpha}(\checkmark) = 1 = \partial\left(\mathsf{e}^{[1]}\right)_{\alpha}(\checkmark)
$$

这足以验证引理 38 的条件。在本情形的其余部分，我们可以放心地假设 $\partial(\mathsf{e})_{\alpha}(\checkmark) \neq 1$。在这种情况下，我们需要针对任意 $\alpha \in$原子验证引理 38 的两个条件。

1. 令 $o \in \{\}\times+$ 输出。我们有

$$\partial\left(\mathsf{e}^{(1)}\right)_\alpha(o) = \frac{\partial(\mathsf{e})_\alpha(o)}{1-\partial(\mathsf{e})_\alpha(\checkmark)} = \frac{1\partial(\mathsf{e})_\alpha(o)}{1-1\partial(\mathsf{e})_\alpha(\checkmark)} = \partial\left(\mathsf{e}^{[1]}\right)_\alpha(o)$$

对于立即接受的情况，我们有

$$\partial\left(\mathsf{e}^{(1)}\right) = 0 = \frac{0}{1-1\partial(\mathsf{e})_\alpha(\checkmark)} = \partial\left(\mathsf{e}^{[1]}\right)_\alpha(\checkmark)$$

2. 令 $\mathsf{p} \in$ 动作集 和 $Q \in \mathtt{Exp}/\equiv_\circ$ 我们有

$$\begin{aligned}\partial\left(\mathsf{e}^{(1)}\right)_\alpha[\{\mathsf{p}\}\times Q] &= \frac{\partial(\mathsf{e})_\alpha[\{\mathsf{p}\}\times Q/\mathsf{e}^{(1)}]}{1-\partial(\mathsf{e})_\alpha(\checkmark)} \\ &= \frac{\partial(\mathsf{e})_\alpha[\{\mathsf{p}\}\times Q/\mathsf{e}^{[1]}]}{1-\partial(\mathsf{e})_\alpha(\checkmark)} && \text{(Lemma 45)} \\ &= \partial\left(\mathsf{e}^{[1]}\right)_\alpha[\{\mathsf{p}\}\times Q]\end{aligned}$$

(F1) 假设规则的前提成立。我们有 $(\mathsf{g}, \mathsf{e}\,;\mathsf{g}\ +_\mathsf{b}\mathsf{f}) \in \Phi_\partial(\equiv)$，并且对于所有$\alpha \in$ 原子，都有 $\mathrm{E}(\mathsf{g})_\alpha = 0$。根据引理 44，我们有 $\partial(\mathsf{g})_\alpha(\checkmark) = 0$ 对于所有 $\alpha \in$ 原子。首先，考虑 $\alpha \leq_{\mathsf{BA}} \mathsf{b}$ 的情况。我们验证引理 38 的条件。

1. 令 $o \in \{\}\times+$ 输出。考虑以下内容

$$\begin{aligned}\partial(\mathsf{g})_\alpha(o) &= \partial(\mathsf{e}\,;\mathsf{g}+_\mathsf{b}\mathsf{f})_\alpha(o) && \text{(归纳假设)} \\ &= \partial(\mathsf{f})_\alpha(o) \\ &= \partial\left(\mathsf{e}^{(\mathsf{b})}\right)_\alpha(o) + \partial\left(\mathsf{e}^{(\mathsf{b})}\right)_\alpha(\checkmark)\partial(\mathsf{f})_\alpha(o) \\ &= \partial\left(\mathsf{e}^{(\mathsf{b})}\,;\mathsf{f}\right)_\alpha(o)\end{aligned}$$

对于立即终止的情况，考虑

$$\begin{aligned}\partial(\mathsf{g})_\alpha(\checkmark) &= \partial(\mathsf{e}\,;\mathsf{g}+_\mathsf{b}\mathsf{f})_\alpha(\checkmark) && \text{（归纳假设）} \\ &= \partial(\mathsf{f})_\alpha(\checkmark) \\ &= \partial\left(\mathsf{e}^{(\mathsf{b})}\right)_\alpha(\checkmark)\partial(\mathsf{f})_\alpha(\checkmark) \\ &= \partial\left(\mathsf{e}^{(\mathsf{b})}\,;\mathsf{f}\right)_\alpha(\checkmark)\end{aligned}$$

2. 令 $\mathsf{p} \in$ 动作集 和 $Q \in \mathtt{Exp}/\equiv_\circ$ 我们有

$$\begin{aligned}\partial(\mathsf{g})_\alpha[\{\mathsf{p}\}\times Q] &= \partial(\mathsf{e}\,;\mathsf{g}+_\mathsf{b}\mathsf{f})_\alpha[\{\mathsf{p}\}\times Q] && \text{(Induction hypothesis)} \\ &= \partial(\mathsf{f})_\alpha[\{\mathsf{p}\}\times Q] \\ &= \partial\left(\mathsf{e}^{(\mathsf{b})}\right)[\{\mathsf{p}\}\times Q/\mathsf{f}] + \partial\left(\mathsf{e}^{(\mathsf{b})}\right)(\checkmark)\partial(\mathsf{f})_\alpha[\{\mathsf{p}\}\times Q] \\ &= \partial\left(\mathsf{e}^{(\mathsf{b})}\,;\mathsf{f}\right)_\alpha[\{\mathsf{p}\}\times Q] && \text{(Lemma 42)}\end{aligned}$$

现在，我们考虑 $\alpha \leq_{\mathsf{BA}} \mathsf{b}$.

1. 对于 $o \in \{\times\}$ $+$输出，我们有

$$\begin{aligned}\partial(\mathsf{g})_\alpha(o) &= \partial(\mathsf{e}\,;\mathsf{g}+_\mathsf{b}\mathsf{f})_\alpha(o) && \text{（归纳假设）} \\ &= \partial(\mathsf{e}\,;\mathsf{g})_\alpha(o)\end{aligned}$$

$$
\begin{aligned}
&= \partial(\mathsf{e})_\alpha(o) + \partial(\mathsf{e})_\alpha(\checkmark)\partial(\mathsf{g})_\alpha(o) \\
&= \partial(\mathsf{e})_\alpha(o) \\
&= \frac{\partial(\mathsf{e})_\alpha(o)}{1-\partial(\mathsf{e})_\alpha(\checkmark)} \\
&= \partial\left(\mathsf{e}^{(\mathsf{b})}\right)_\alpha(o) \\
&= \partial\left(\mathsf{e}^{(\mathsf{b})}\right)_\alpha(o) + \partial\left(\mathsf{e}^{(\mathsf{b})}\right)_\alpha(\checkmark)\partial(\mathsf{f})_\alpha(o) \\
&= \partial\left(\mathsf{e}^{(\mathsf{b})};\mathsf{f}\right)_\alpha(o)
\end{aligned}
$$

对于输出 ✓的剩余情况，请考虑以下内容

$$
\begin{aligned}
\partial(\mathsf{g})_\alpha(\checkmark) &= \partial(\mathsf{e};\mathsf{g}+_{\mathsf{b}}\mathsf{f})_\alpha(\checkmark) && \text{（归纳假设）} \\
&= \partial(\mathsf{e};\mathsf{g})_\alpha(\checkmark) \\
&= \partial(\mathsf{e})_\alpha(\checkmark)\partial(\mathsf{g})_\alpha(\checkmark) \\
&= 0 \\
&= \partial\left(\mathsf{e}^{(\mathsf{b})}\right)_\alpha(\checkmark) \\
&= \partial\left(\mathsf{e}^{(\mathsf{b})}\right)_\alpha(\checkmark)\partial(\mathsf{f})_\alpha(\checkmark) \\
&= \partial\left(\mathsf{e}^{(\mathsf{b})};\mathsf{f}\right)_\alpha(\checkmark)
\end{aligned}
$$

2. 对于p ∈动作集和 $Q \in \mathtt{Exp}/\equiv$，我们有

$$
\begin{aligned}
\partial(\mathsf{g})_\alpha[\{\mathsf{p}\}\times Q] &= \partial(\mathsf{e};\mathsf{g}+_{\mathsf{b}}\mathsf{f})_\alpha[\{\mathsf{p}\}\times Q] && \text{(Induction hypothesis)} \\
&= \partial(\mathsf{e};\mathsf{g})_\alpha[\{\mathsf{p}\}\times Q] \\
&= \partial(\mathsf{e})_\alpha[\{\mathsf{p}\}\times Q/\mathsf{g}] + \partial(\mathsf{e})_\alpha(\checkmark)\partial(\mathsf{g})_\alpha[\{\mathsf{p}\}\times Q] \\
&= \partial(\mathsf{e})_\alpha[\{\mathsf{p}\}\times Q/\mathsf{g}] \\
&= \partial(\mathsf{e})_\alpha[\{\mathsf{p}\}\times Q/\mathsf{e}^{(\mathsf{b})};\mathsf{f}] && \text{(Lemma 45)} \\
&= \partial(\mathsf{e})_\alpha[\{\mathsf{p}\}\times (Q/\mathsf{f})/\mathsf{e}^{(\mathsf{b})}] && \text{(Lemma 46)} \\
&= \frac{\partial(\mathsf{e})_\alpha[\{\mathsf{p}\}\times (Q/\mathsf{f})/\mathsf{e}^{(\mathsf{b})}]}{1-\partial(\mathsf{e})_\alpha(\checkmark)} \\
&= \partial\left(\mathsf{e}^{(\mathsf{b})}\right)_\alpha[\{\mathsf{p}\}\times Q/\mathsf{f}] \\
&= \partial\left(\mathsf{e}^{(\mathsf{b})}\right)_\alpha[\{\mathsf{p}\}\times Q/\mathsf{f}] + \partial\left(\mathsf{e}^{(\mathsf{b})}\right)_\alpha(\checkmark)\partial(\mathsf{f})_\alpha[\{\mathsf{p}\}\times Q] \\
&= \partial\left(\mathsf{e}^{(\mathsf{b})};\mathsf{f}\right)_\alpha[\{\mathsf{p}\}\times Q]
\end{aligned}
$$

(F2) 假设该规则的前提成立。我们有$(\mathsf{g},\ \mathsf{e};\mathsf{g}\oplus_r\mathsf{f}) \in \Phi_\partial(\equiv)$ 并且对于所有$\alpha \in$ 原子，我们有$\mathsf{E}(\mathsf{g})_\alpha = 0$。根据引理 44，我们有 $\partial(\mathsf{g})_\alpha(\checkmark) = 0$ 对所有 $\alpha \in$ 原子均成立。我们验证引理 38 的条件。

1. 对于 $o \in \{\chi\}$ +输出，成立

$$
\begin{aligned}
\partial(\mathsf{g})_\alpha(o) &= \partial(\mathsf{e};\mathsf{g}\oplus_r\mathsf{g})_\alpha(o) && \text{(In归纳假设)} \\
&= r\partial(\mathsf{e};\mathsf{g})_\alpha(o) + (1-r)\partial(\mathsf{f})_\alpha(o) \\
&= r\partial(\mathsf{e})_\alpha(o) + r\partial(\mathsf{e})_\alpha(\checkmark)\partial(\mathsf{g})_\alpha(o) + (1-r)\partial(\mathsf{f})_\alpha(o) \\
&= \frac{r\partial(\mathsf{e})_\alpha(o)}{1-r\partial(\mathsf{e})_\alpha(\checkmark)} + \frac{1-r}{1-r\partial(\mathsf{e})_\alpha(\checkmark)}\partial(\mathsf{f})_\alpha(o)
\end{aligned}
$$

$$
\begin{aligned}
&= \partial\left(\mathsf{e}^{[r]}\right)_\alpha(o) + \partial\left(\mathsf{e}^{[r]}\right)_\alpha(\checkmark)\partial(\mathsf{f})_\alpha(o) \\
&= \partial\left(\mathsf{e}^{[r]}\,;\mathsf{f}\right)_\alpha(o)
\end{aligned}
$$

现在，考虑输出 $\checkmark$ 的情形。我们有：

$$
\begin{aligned}
\partial(\mathsf{g})_\alpha(\checkmark) &= \partial(\mathsf{e}\,;\mathsf{g}\oplus_r \mathsf{f})_\alpha(\checkmark) && \text{（归纳假设）} \\
&= r\partial(\mathsf{e}\,;\mathsf{g})_\alpha(\checkmark) + (1-r)\partial(\mathsf{f})_\alpha(\checkmark) \\
&= r\partial(\mathsf{e})_\alpha(\checkmark)\partial(\mathsf{g})_\alpha(\checkmark) + (1-r)\partial(\mathsf{f})_\alpha(\checkmark) \\
&= (1-r)\partial(\mathsf{f})_\alpha(\checkmark) \\
&= \frac{1-r}{1-r\partial(\mathsf{e})_\alpha(\checkmark)}\partial(\mathsf{f})_\alpha(\checkmark) \\
&= \partial\left(\mathsf{e}^{[r]}\right)_\alpha(\checkmark)\partial(\mathsf{f})_\alpha(\checkmark) \\
&= \partial\left(\mathsf{e}^{[r]}\,;\mathsf{f}\right)_\alpha(\checkmark)
\end{aligned}
$$

2. 设 $\mathsf{p}\in$ 动作集 并设 $Q\in \mathtt{Exp}/\equiv_\circ$ 考虑以下

$$
\begin{aligned}
\partial(\mathsf{g})_\alpha[\{\mathsf{p}\}] &= \partial(\mathsf{e}\,;\mathsf{g}\oplus_r \mathsf{f})_\alpha[\{\mathsf{p}\}\times Q] && \text{(Induction hypothesis)} \\
&= r\partial(\mathsf{e}\,;\mathsf{g})_\alpha[\{\mathsf{p}\}\times Q] + (1-r)\partial(\mathsf{f})_\alpha[\{\mathsf{p}\}\times Q] \\
&= r\partial(\mathsf{e})_\alpha[\{\mathsf{p}\}\times Q/\mathsf{g}] + r\partial(\mathsf{e})_\alpha(\checkmark)\partial(\mathsf{g})_\alpha[\{\mathsf{p}\}\times Q] \\
&\quad + (1-r)\partial(\mathsf{f})_\alpha[\{\mathsf{p}\}\times Q] \\
&= r\partial(\mathsf{e})_\alpha[\{\mathsf{p}\}\times Q/\mathsf{g}] + (1-r)\partial(\mathsf{f})_\alpha[\{\mathsf{p}\}\times Q] \\
&= r\partial(\mathsf{e})_\alpha[\{\mathsf{p}\}\times Q/\mathsf{e}^{[r]}\,;\mathsf{f}] + (1-r)\partial(\mathsf{f})_\alpha[\{\mathsf{p}\}\times Q] && \text{(Lemma 45)} \\
&= r\partial(\mathsf{e})_\alpha[\{\mathsf{p}\}\times (Q/\mathsf{f})/\mathsf{e}^{[r]}] + (1-r)\partial(\mathsf{f})_\alpha[\{\mathsf{p}\}\times Q] && \text{(Lemma 46)} \\
&= \frac{r\partial(\mathsf{e})_\alpha[\{\mathsf{p}\}\times (Q/\mathsf{f})/\mathsf{e}^{[r]}]}{1-r\partial(\mathsf{e})_\alpha(\checkmark)} + \frac{(1-r)}{1-r\partial(\mathsf{e})_\alpha(\checkmark)}\partial(\mathsf{f})_\alpha[\{\mathsf{p}\}\times Q] \\
&= \partial\left(\mathsf{e}^{[r]}\right)_\alpha[\{\mathsf{p}\}\times Q/\mathsf{f}] + \partial\left(\mathsf{e}^{[r]}\right)_\alpha(\checkmark)\partial(\mathsf{f})_\alpha[\{\mathsf{p}\}\times Q] \\
&= \partial\left(\mathsf{e}^{[r]}\,;\mathsf{f}\right)_\alpha[\{\mathsf{p}\}\times Q]
\end{aligned}
$$

<escape>**(L5)** 假设前提成立且满足互模拟等价。特别地，我们有$(\mathsf{e},(\mathsf{f}\ \oplus_r 1)\ +_\mathsf{c}\mathsf{g})\ \in \Phi_\partial(\equiv)$。根据假设 $r>0$。首先，考虑 $\alpha\leq_{\mathsf{BA}}\bar{\mathsf{c}}$ 的情况。我们有</escape>

$$
\begin{aligned}
\partial\left(\mathsf{c}\,;\mathsf{e}^{(\mathsf{b})}\right)_\alpha(x) &= \partial(\mathsf{c})_\alpha(x) + \partial(\mathsf{c})_\alpha(\checkmark)\partial\left(\mathsf{e}^{(\mathsf{b})}\right)_\alpha(x) \\
&= 1 \\
&= \partial\left(\mathsf{c}\,;(\mathsf{f}\,;\mathsf{e}^{(\mathsf{b})}+_\mathsf{b} 1)\right)_\alpha(x)
\end{aligned}
$$

这足以验证引理 38 的所有条件，因为两个分布都将全部概率质量赋给同一个元素。现在，考虑 $\alpha\leq_{\mathsf{BA}}\bar{\mathsf{c}}$ 和 $\alpha\leq_{\mathsf{BA}}\mathsf{b}$ 的情况。我们有

$$
\begin{aligned}
\partial\left(\mathsf{c}\,;\mathsf{e}^{(\mathsf{b})}\right)_\alpha(\checkmark) &= \partial\left(\mathsf{e}^{(\mathsf{b})}\right)_\alpha(\checkmark) && \text{(Lemma 48)} \\
&= 1 \\
&= \partial\left(\mathsf{f}\,;\mathsf{e}^{(\mathsf{b})}+_\mathsf{b} 1\right)_\alpha(\checkmark)
\end{aligned}
$$

$$= \partial\left(\mathsf{c}\,;(\mathsf{f}\,;\mathsf{e}^{(\mathsf{b})} +_{\mathsf{b}} 1)\right)_{\alpha}(\checkmark) \qquad \text{(Lemma 48)}$$

这同样足以验证引理 38 的条件。对于其余情况，假设 $\alpha \leq_{\mathsf{BA}} \mathsf{c}$ 和 $\alpha \leq_{\mathsf{BA}} \mathsf{b}$。首先，我们考虑子情况 $\partial(\mathsf{f})_{\alpha}(\checkmark) = 1$。根据归纳假设，这意味着 $\partial(\mathsf{e})_{\alpha}(\checkmark) = 1$，因此我们有

$$\begin{aligned}
\partial\left(\mathsf{c}\,;\mathsf{e}^{(\mathsf{b})}\right)_{\alpha}(x) &= \partial\left(\mathsf{e}^{(\mathsf{b})}\right)_{\alpha}(x) \\
&= 1 \\
&= \partial(\mathsf{f})_{\alpha}(x) + \partial(\mathsf{f})_{\alpha}(\checkmark)\partial\left(\mathsf{e}^{(\mathsf{b})}\right)_{\alpha}(x) \\
&= \partial\left(\mathsf{f}\,;\mathsf{e}^{(\mathsf{b})}\right)_{\alpha}(x) \\
&= \partial\left(\mathsf{f}\,;\mathsf{e}^{(\mathsf{b})} +_{\mathsf{b}} 1\right)_{\alpha}(x) \\
&= \partial\left(\mathsf{c}\,;(\mathsf{f}\,;\mathsf{e}^{(\mathsf{b})} +_{\mathsf{b}} 1)\right)_{\alpha}(x)
\end{aligned}$$

这足以满足引理 38 的条件。最后，在本情况的剩余部分中，我们将假设 $\partial(\mathsf{f})_{\alpha}(\checkmark) \neq 1$。在这种情况下，我们需要验证引理 38 的所有条件。

1. 令 $o \in \{\}x+$ 输出。注意到

$$\begin{aligned}
\partial\left(\mathsf{c}\,;\mathsf{e}^{(\mathsf{b})}\right)_{\alpha}(o) &= \partial\left(\mathsf{e}^{(\mathsf{b})}\right)_{\alpha}(o) && \text{(Lemma 48)} \\
&= \frac{\partial(\mathsf{e})_{\alpha}(o)}{1-\partial(\mathsf{e})_{\alpha}(\checkmark)} \\
&= \frac{\partial((\mathsf{f} \oplus_r 1) +_{\mathsf{c}} \mathsf{g})_{\alpha}(o)}{1-\partial((\mathsf{f} \oplus_r 1) +_{\mathsf{c}} \mathsf{g})_{\alpha}(\checkmark)} && \text{(Induction hypothesis)} \\
&= \frac{\partial(\mathsf{f} \oplus_r 1)_{\alpha}(o)}{1-\partial(\mathsf{f} \oplus_r 1)_{\alpha}(\checkmark)} \\
&= \frac{r\partial(\mathsf{f})_{\alpha}(o)}{1-r\partial(\mathsf{f})_{\alpha}(\checkmark)-(1-r)} \\
&= \frac{\partial(\mathsf{f})_{\alpha}(o)}{1-\partial(\mathsf{f})_{\alpha}(\checkmark)} \\
&= \partial(\mathsf{f})_{\alpha}(o)\left(\frac{1-\partial(\mathsf{f})_{\alpha}(\checkmark)+\partial(\mathsf{f})_{\alpha}(\checkmark)}{1-\partial(\mathsf{f})_{\alpha}(\checkmark)}\right) \\
&= \partial(\mathsf{f})_{\alpha}(o)\left(1+\frac{\partial(\mathsf{f})_{\alpha}(\checkmark)}{1-\partial(\mathsf{f})_{\alpha}(\checkmark)}\right) \\
&= \partial(\mathsf{f})_{\alpha}(o) + \partial(\mathsf{f})_{\alpha}(\checkmark)\frac{\partial(\mathsf{f})_{\alpha}(o)}{1-\partial(\mathsf{f})_{\alpha}(o)} \\
&= \partial(\mathsf{f})_{\alpha}(o) + \partial(\mathsf{f})_{\alpha}(\checkmark)\frac{r\partial(\mathsf{f})_{\alpha}(o)}{1-r\partial(\mathsf{f})_{\alpha}(\checkmark)-(1-r)} \\
&= \partial(\mathsf{f})_{\alpha}(o) + \partial(\mathsf{f})_{\alpha}(\checkmark)\frac{\partial(\mathsf{f} \oplus_r 1)_{\alpha}(o)}{1-\partial(\mathsf{f} \oplus_r 1)_{\alpha}(\checkmark)} \\
&= \partial(\mathsf{f})_{\alpha}(o) + \partial(\mathsf{f})_{\alpha}(\checkmark)\frac{\partial((\mathsf{f} \oplus_r 1) +_{\mathsf{c}} \mathsf{g})_{\alpha}(o)}{1-\partial((\mathsf{f} \oplus_r 1) +_{\mathsf{c}} \mathsf{g})_{\alpha}(\checkmark)} \\
&= \partial(\mathsf{f})_{\alpha}(o) + \partial(\mathsf{f})_{\alpha}(\checkmark)\frac{\partial(\mathsf{e})_{\alpha}(o)}{1-\partial(\mathsf{e})_{\alpha}(\checkmark)} && \text{(Induction hypothesis)} \\
&= \partial(\mathsf{f})_{\alpha}(o) + \partial(\mathsf{f})_{\alpha}(\checkmark)\partial\left(\mathsf{e}^{(\mathsf{b})}\right)_{\alpha}(o)
\end{aligned}$$

$$
\begin{aligned}
&= \partial\left(\mathsf{f}\,;\mathsf{e}^{(\mathsf{b})}\right)_\alpha(o)\\
&= \partial\left(\mathsf{f}\,;\mathsf{e}^{(\mathsf{b})} +_{\mathsf{b}} 1\right)_\alpha(o)\\
&= \partial\left(\mathsf{c}\,;(\mathsf{f}\,;\mathsf{e}^{(\mathsf{b})} +_{\mathsf{b}} 1)\right)_\alpha(o) && \text{(Lemma 48)}
\end{aligned}
$$

现在，我们考虑输出 ✓的情况。我们有

$$
\begin{aligned}
\partial\left(\mathsf{c}\,;\mathsf{e}^{(\mathsf{b})}\right)_\alpha(o) &= \partial\left(\mathsf{e}^{(\mathsf{b})}\right)_\alpha(\checkmark) && \text{(Lemma 48)}\\
&= 0\\
&= \partial(\mathsf{f})_\alpha(\checkmark)\partial\left(\mathsf{e}^{(\mathsf{b})}\right)_\alpha(\checkmark)\\
&= \partial\left(\mathsf{f}\,;\mathsf{e}^{(\mathsf{b})}\right)_\alpha(\checkmark)\\
&= \partial\left(\mathsf{f}\,;\mathsf{e}^{(\mathsf{b})}\right)_\alpha(\checkmark)\\
&= \partial\left(\mathsf{f}\,;\mathsf{e}^{(\mathsf{b})} +_{\mathsf{b}} 1\right)_\alpha(\checkmark)\\
&= \partial\left(\mathsf{c}\,;(\mathsf{f}\,;\mathsf{e}^{(\mathsf{b})} +_{\mathsf{b}} 1)\right)_\alpha(\checkmark) && \text{(Lemma 48)}
\end{aligned}
$$

2. 设 $\mathsf{p} \in$ 动作集 和 $Q \in \mathtt{Exp}/\equiv_\circ$ 我们有

$$
\begin{aligned}
\partial\left(\mathsf{c}\,;\mathsf{e}^{(\mathsf{b})}\right)_\alpha[\{\mathsf{p}\}\times Q] &= \partial\left(\mathsf{e}^{(\mathsf{b})}\right)_\alpha[\{\mathsf{p}\}\times Q] && \text{(Lemma 48)}\\
&= \frac{\partial(\mathsf{e})_\alpha[\{\mathsf{p}\}\times Q/\mathsf{e}^{(\mathsf{b})}]}{1-\partial(\mathsf{e})_\alpha(\checkmark)}\\
&= \frac{r\partial(\mathsf{f})_\alpha[\{\mathsf{p}\}\times Q/\mathsf{e}^{(\mathsf{b})}]}{1-r\partial(\mathsf{f})_\alpha(\checkmark)-(1-r)} && \text{(Induction hypothesis)}\\
&= \frac{\partial(\mathsf{f})_\alpha[\{\mathsf{p}\}\times Q/\mathsf{e}^{(\mathsf{b})}]}{1-\partial(\mathsf{f})_\alpha(\checkmark)}\\
&= \partial(\mathsf{f})_\alpha[\{\mathsf{p}\}\times Q]\left(\frac{1-\partial(\mathsf{f})_\alpha(\checkmark)+\partial(\mathsf{f})_\alpha(\checkmark)}{1-\partial(\mathsf{f})_\alpha(\checkmark)}\right)\\
&= \partial(\mathsf{f})_\alpha[\{\mathsf{p}\}\times Q]\left(1+\frac{\partial(\mathsf{f})_\alpha(\checkmark)}{1-\partial(\mathsf{f})_\alpha(\checkmark)}\right)\\
&= \partial(\mathsf{f})_\alpha[\{\mathsf{p}\}\times Q/\mathsf{e}^{(\mathsf{b})}]+\partial(\mathsf{f})_\alpha(\checkmark)\frac{\partial(\mathsf{f})_\alpha[\{\mathsf{p}\}\times Q/\mathsf{e}^{(\mathsf{b})}]}{1-\partial(\mathsf{f})_\alpha(\checkmark)}\\
&= \partial(\mathsf{f})_\alpha[\{\mathsf{p}\}\times Q/\mathsf{e}^{(\mathsf{b})}]+\partial(\mathsf{f})_\alpha(\checkmark)\frac{r\partial(\mathsf{f})_\alpha[\{\mathsf{p}\}\times Q/\mathsf{e}^{(\mathsf{b})}]}{1-r\partial(\mathsf{f})_\alpha(\checkmark)-(1-r)}\\
&= \partial(\mathsf{f})_\alpha[\{\mathsf{p}\}\times Q/\mathsf{e}^{(\mathsf{b})}]+\partial(\mathsf{f})_\alpha(\checkmark)\frac{\partial((\mathsf{f}\oplus_r 1)+_{\mathsf{c}}\mathsf{g})_\alpha[\{\mathsf{p}\}\times Q/\mathsf{e}^{(\mathsf{b})}]}{1-\partial((\mathsf{f}\oplus_r 1)+_{\mathsf{c}}\mathsf{g})_\alpha(\checkmark)}\\
&= \partial(\mathsf{f})_\alpha[\{\mathsf{p}\}\times Q/\mathsf{e}^{(\mathsf{b})}]+\partial(\mathsf{f})_\alpha(\checkmark)\frac{\partial(\mathsf{e})_\alpha[\{\mathsf{p}\}\times Q/\mathsf{e}^{(\mathsf{b})}]}{1-\partial(\mathsf{e})_\alpha(\checkmark)}\\
&&& \text{(Induction hypothesis)}\\
&= \partial(\mathsf{f})_\alpha[\{\mathsf{p}\}\times Q/\mathsf{e}^{(\mathsf{b})}]+\partial(\mathsf{f})_\alpha(\checkmark)\partial\left(\mathsf{e}^{(\mathsf{b})}\right)_\alpha[\{\mathsf{p}\}\times Q]\\
&= \partial\left(\mathsf{f}\,;\mathsf{e}^{(\mathsf{b})}\right)_\alpha[\{\mathsf{p}\}\times Q] && \text{(Lemma 42)}\\
&= \partial\left(\mathsf{f}\,;\mathsf{e}^{(\mathsf{b})} +_{\mathsf{b}} 1\right)_\alpha[\{\mathsf{p}\}\times Q]\\
&= \partial\left(\mathsf{c}\,;(\mathsf{f}\,;\mathsf{e}^{(\mathsf{b})} +_{\mathsf{b}} 1)\right)_\alpha[\{\mathsf{p}\}\times Q] && \text{(Lemma 48)}
\end{aligned}
$$

(L6) 假设前提成立，并且由互模拟等价满足。特别地，我们有$(\mathsf{e},(\mathsf{f}\ \oplus_s 1)\ +_{\mathsf{c}}\mathsf{g})\ \in \Phi_\partial(\equiv)$。根据假设，我们有 $r(1-s)\neq 1$。我们也将t 写作 $\frac{rs}{1-r\ (1-s)}$ 的简写。

首先，考虑 $\alpha \leq_{\mathsf{BA}} \bar{\mathsf{c}}$ 的情形。我们有

$$\begin{aligned}\partial\left(\mathsf{c}\,;\mathsf{e}^{[r]}\right)_\alpha(x) &= \partial(\mathsf{c})_\alpha(x) + \partial(\mathsf{c})_\alpha(\checkmark)\partial\left(\mathsf{e}^{[r]}\right)_\alpha(x)\\ &= 1\\ &= \partial(\mathsf{c})_\alpha(x) + \partial(\mathsf{c})_\alpha(\checkmark)\partial\left(\mathsf{f}\,;\mathsf{e}^{[r]} \oplus_t 1\right)_\alpha(x)\\ &= \partial\left(\mathsf{c}\,;(\mathsf{f}\,;\mathsf{e}^{[r]} \oplus_t 1)\right)_\alpha(x)\end{aligned}$$

由于这两个分布都将所有概率质量分配给 x，因此满足引理 38 的条件。对于其余情况，假设 $\alpha \leq_{\mathsf{BA}} \mathsf{c}$。我们验证引理 38 的条件。**1.** 令 $o \in \{\,\} + 输出$。我们有

$$\begin{aligned}&\partial\left(\mathsf{c}\,;\mathsf{e}^{[r]}\right)_\alpha(o) = \partial\left(\mathsf{e}^{[r]}\right)_\alpha(o) && \text{(Lemma 48)}\\ &= \frac{r\partial(\mathsf{e})_\alpha(o)}{1 - r\partial(\mathsf{e})_\alpha(\checkmark)}\\ &= \frac{r\partial((\mathsf{f} \oplus_s 1) +_{\mathsf{c}} \mathsf{g})_\alpha(o)}{1 - r\partial((\mathsf{f} \oplus_s 1) +_{\mathsf{c}} \mathsf{g})_\alpha(\checkmark)} && \text{(Induction hypothesis)}\\ &= \frac{rs\partial(\mathsf{f})_\alpha(o)}{1 - rs\partial(\mathsf{f})_\alpha(\checkmark) - r(1-s)}\\ &= \frac{rs}{1-r(1-s)}\left(\frac{\partial(\mathsf{f})_\alpha(o)(1-r(1-s))}{1 - rs\partial(\mathsf{f})_\alpha(\checkmark) - r(1-s)}\right)\\ &= t\left(\frac{\partial(\mathsf{f})_\alpha(o)\,(1-r(1-s)) + rs\partial(\mathsf{f})_\alpha(\checkmark)\partial(\mathsf{f})_\alpha(o) - rs\partial(\mathsf{f})_\alpha(\checkmark)\partial(\mathsf{f})_\alpha(o)}{1 - rs\partial(\mathsf{f})_\alpha(\checkmark) - r(1-s)}\right)\\ &= t\left(\frac{\partial(\mathsf{f})_\alpha(o)\,(1 - rs\partial(\mathsf{f})_\alpha(\checkmark) - r(1-s)) + rs\partial(\mathsf{f})_\alpha(\checkmark)\partial(\mathsf{f})_\alpha(o)}{1 - rs\partial(\mathsf{f})_\alpha(\checkmark) - r(1-s)}\right)\\ &= t\left(\partial(\mathsf{f})_\alpha(o) + \partial(\mathsf{f})_\alpha(\checkmark)\frac{rs\partial(\mathsf{f})_\alpha(o)}{1 - rs\partial(\mathsf{f})_\alpha(\checkmark) - r(1-s)}\right)\\ &= t\left(\partial(\mathsf{f})_\alpha(o) + \partial(\mathsf{f})_\alpha(\checkmark)\frac{r\partial((\mathsf{f} \oplus_s 1) +_{\mathsf{c}} \mathsf{g})_\alpha(o)}{1 - r\partial((\mathsf{f} \oplus_s 1) +_{\mathsf{c}} \mathsf{g})_\alpha(\checkmark)}\right)\\ &= t\left(\partial(\mathsf{f})_\alpha(o) + \partial(\mathsf{f})_\alpha(\checkmark)\frac{r\partial(\mathsf{e})_\alpha(o)}{1 - r\partial(\mathsf{e})_\alpha(\checkmark)}\right) && \text{(Induction hypothesis)}\\ &= t\left(\partial(\mathsf{f})_\alpha(o) + \partial(\mathsf{f})_\alpha(\checkmark)\partial\left(\mathsf{e}^{[r]}\right)_\alpha(o)\right)\\ &= \partial\left(\mathsf{f}\,;\mathsf{e}^{[r]} \oplus_t 1\right)_\alpha(o)\\ &= \partial\left(\mathsf{c}\,;(\mathsf{f}\,;\mathsf{e}^{[r]} \oplus_t 1)\right)_\alpha(o) && \text{(Lemma 48)}\end{aligned}$$

至于输出 $\checkmark$ 的概率，我们有：

$$\begin{aligned}&\partial\left(\mathsf{c}\,;\mathsf{e}^{[r]}\right)_\alpha(\checkmark) = \partial\left(\mathsf{e}^{[r]}\right)_\alpha(\checkmark) && \text{(Lemma 48)}\\ &= \frac{1-r}{1 - r\partial(\mathsf{e})_\alpha(\checkmark)}\\ &= \frac{1-r}{1 - r\partial((\mathsf{f} \oplus_s 1) +_{\mathsf{c}} \mathsf{g})_\alpha(\checkmark)} && \text{(Induction hypothesis)}\\ &= \frac{1-r}{1 - rs\partial(\mathsf{f})_\alpha(\checkmark) - r(1-s)}\\ &= \frac{(1-r)\,(t\partial(\mathsf{f})_\alpha(\checkmark) - t\partial(\mathsf{f})_\alpha(\checkmark) + 1)}{1 - rs\partial(\mathsf{f})_\alpha(\checkmark) - r(1-s)}\end{aligned}$$

$$
\begin{aligned}
&= \frac{(1-r)\left(t\partial(\mathsf{f})_\alpha(\checkmark) - \frac{rs}{1-r(1-s)}\partial(\mathsf{f})_\alpha(\checkmark) + 1\right)}{1 - rs\partial(\mathsf{f})_\alpha(\checkmark) - r(1-s)} \\
&= \frac{(1-r)t\partial(\mathsf{f})_\alpha(\checkmark) - \frac{1-r}{1-r(1-s)}rs\partial(\mathsf{f})_\alpha(\checkmark) + (1-r(1-s))\frac{1-r}{1-r(1-s)}}{1 - rs\partial(\mathsf{f})_\alpha(\checkmark) - r(1-s)} \\
&= \frac{t\partial(\mathsf{f})_\alpha(\checkmark)(1-r) + \frac{1-r}{1-r(1-s)}\left(1 - rs\partial(\mathsf{f})_\alpha(\checkmark) - r(1-s)\right)}{1 - rs\partial(\mathsf{f})_\alpha(\checkmark) - r(1-s)} \\
&= t\partial(\mathsf{f})_\alpha(\checkmark)\frac{1-r}{1 - rs\partial(\mathsf{f})_\alpha(\checkmark) - r(1-s)} + \frac{1-r}{1-r(1-s)} \\
&= t\partial(\mathsf{f})_\alpha(\checkmark)\frac{1-r}{1 - r\partial((\mathsf{f} \oplus_s 1) +_\mathsf{c} \mathsf{g})_\alpha(\checkmark)} + (1-t) \\
&= t\partial(\mathsf{f})_\alpha(\checkmark)\frac{1-r}{1 - r\partial(\mathsf{e})_\alpha(\checkmark)} + (1-t) && \text{(Induction hyp论证)} \\
&= t\partial(\mathsf{f})_\alpha(\checkmark)\partial\left(\mathsf{e}^{[r]}\right)_\alpha(\checkmark) + (1-t) \\
&= \partial\left(\mathsf{f}\,;\mathsf{e}^{[r]} \oplus_t 1\right)_\alpha(\checkmark) \\
&= \partial\left(\mathsf{c}\,;(\mathsf{f}\,;\mathsf{e}^{[r]} \oplus_t 1)\right)_\alpha(\checkmark) && \text{(Lemma 48)}
\end{aligned}
$$

2. 设 $\mathsf{p} \in$ 动作集 和 $Q \in \mathtt{Exp}/\equiv_\circ$ 注意到

$$
\begin{aligned}
&\partial\left(\mathsf{c}\,;\mathsf{e}^{[r]}\right)_\alpha[\{\mathsf{p}\} \times Q] \\
&= \partial\left(\mathsf{e}^{[r]}\right)_\alpha[\{\mathsf{p}\} \times Q] && \text{(Lemma 48)} \\
&= \frac{r\partial(\mathsf{e})_\alpha[\{\mathsf{p}\} \times Q/\mathsf{e}^{[r]}]}{1 - r\partial(\mathsf{e})_\alpha(\checkmark)} \\
&= \frac{r\partial((\mathsf{f} \oplus_s 1) +_\mathsf{c} \mathsf{g})_\alpha[\{\mathsf{p}\} \times Q/\mathsf{e}^{[r]}]}{1 - r\partial((\mathsf{f} \oplus_s 1) +_\mathsf{c} \mathsf{g})_\alpha(\checkmark)} && \text{(Induction hypothesis)} \\
&= \frac{rs\partial(\mathsf{f})_\alpha[\{\mathsf{p}\} \times Q/\mathsf{e}^{[r]}]}{1 - rs\partial(\mathsf{f})_\alpha(\checkmark) - r(1-s)} \\
&= \frac{rs}{1-r(1-s)}\left(\frac{\partial(\mathsf{f})_\alpha[\{\mathsf{p}\} \times Q/\mathsf{e}^{[r]}](1-r(1-s))}{1 - rs\partial(\mathsf{f})_\alpha(\checkmark) - r(1-s)}\right) \\
&= t\left(\frac{\partial(\mathsf{f})_\alpha[\{\mathsf{p}\} \times Q/\mathsf{e}^{[r]}](1-r(1-s)) + rs\partial(\mathsf{f})_\alpha(\checkmark)\partial(\mathsf{f})_\alpha[\{\mathsf{p}\} \times Q/\mathsf{e}^{[r]}]}{1 - rs\partial(\mathsf{f})_\alpha(\checkmark) - r(1-s)}\right) \\
&\qquad - t\frac{rs\partial(\mathsf{f})_\alpha(\checkmark)\partial(\mathsf{f})_\alpha[\{\mathsf{p}\} \times Q/\mathsf{e}^{[r]}]}{1 - rs\partial(\mathsf{f})_\alpha(\checkmark) - r(1-s)} \\
&= t\left(\frac{\partial(\mathsf{f})_\alpha[\{\mathsf{p}\} \times Q/\mathsf{e}^{[r]}]\left(1 - rs\partial(\mathsf{f})_\alpha(\checkmark) - r(1-s)\right) + rs\partial(\mathsf{f})_\alpha(\checkmark)\partial(\mathsf{f})_\alpha[\{\mathsf{p}\} \times Q/\mathsf{e}^{[r]}]}{1 - rs\partial(\mathsf{f})_\alpha(\checkmark) - r(1-s)}\right) \\
&= t\left(\partial(\mathsf{f})_\alpha[\{\mathsf{p}\} \times Q/\mathsf{e}^{[r]}] + \partial(\mathsf{f})_\alpha(\checkmark)\frac{rs\partial(\mathsf{f})_\alpha[\{\mathsf{p}\} \times Q/\mathsf{e}^{[r]}]}{1 - rs\partial(\mathsf{f})_\alpha(\checkmark) - r(1-s)}\right) \\
&= t\left(\partial(\mathsf{f})_\alpha[\{\mathsf{p}\} \times Q/\mathsf{e}^{[r]}] + \partial(\mathsf{f})_\alpha(\checkmark)\frac{r\partial((\mathsf{f} \oplus_s 1) +_\mathsf{c} \mathsf{g})_\alpha[\{\mathsf{p}\} \times Q/\mathsf{e}^{[r]}]}{1 - r\partial((\mathsf{f} \oplus_s 1) +_\mathsf{c} \mathsf{g})_\alpha(\checkmark)}\right) \\
&= t\left(\partial(\mathsf{f})_\alpha[\{\mathsf{p}\} \times Q/\mathsf{e}^{[r]}] + \partial(\mathsf{f})_\alpha(\checkmark)\frac{r\partial(\mathsf{e})_\alpha[\{\mathsf{p}\} \times Q/\mathsf{e}^{[r]}]}{1 - r\partial(\mathsf{e})_\alpha(\checkmark)}\right) && \text{(Induction hypothesis)} \\
&= t\left(\partial(\mathsf{f})_\alpha[\{\mathsf{p}\} \times Q/\mathsf{e}^{[r]}] + \partial(\mathsf{f})_\alpha(\checkmark)\partial\left(\mathsf{e}^{[r]}\right)_\alpha[\{\mathsf{p}\} \times Q]\right) \\
&= \partial\left(\mathsf{f}\,;\mathsf{e}^{[r]} \oplus_t 1\right)_\alpha[\{\mathsf{p}\} \times Q] \\
&= \partial\left(\mathsf{c}\,;(\mathsf{f}\,;\mathsf{e}^{[r]} \oplus_t 1)\right)_\alpha[\{\mathsf{p}\} \times Q] && \text{(Lemma 48)} \quad \blacktriangleleft
\end{aligned}
$$

▶ 注 49. 我们可以在 L5 的结论中代入 e，从而得到

$$\mathsf{c}\,;((\mathsf{f}\oplus_s 1)+_{\mathsf{c}}\mathsf{g}))^{(\mathsf{b})}\equiv \mathsf{c}\,;(\mathsf{f}\,;((\mathsf{f}\oplus_s 1)+_{\mathsf{c}}\mathsf{g})^{(\mathsf{b})}+_{\mathsf{b}}1)$$

根据同余关系，这与 L5 等价。类似的转换可将 L6 转换为等式公理。或者，也可以用以下准等式公理替换 L5 和 L6，并且可以证明该公理能够推出二者：

$$\frac{\mathsf{e}\equiv((\mathsf{f}\oplus_s \mathsf{e})\oplus_r 1)+_{\mathsf{c}}\mathsf{g}\qquad r(1-s)\neq 1}{\mathsf{e}\equiv(\mathsf{f}\oplus_{\frac{rs}{1-r(1-s)}}1)+_{\mathsf{c}}\mathsf{g}}$$

由于前提中再次出现 e，因此无法像替换 L5 和 L6 那样将此规则替换为公理。

D.1 可推导事实

▶ **引理 50**。 以下等价关系可由 $\equiv$ 对所有 e、f、g、h $\in$ Exp、b、c $\in$ BExp 以及 $r\in[0,1]$ 推导得出。
(DF1) $\mathsf{e}+_{\mathsf{b}}(\mathsf{f}+_{\mathsf{c}}\mathsf{g})\equiv(\mathsf{e}+_{\mathsf{b}}\mathsf{f})+_{\mathsf{b}+\mathsf{c}}\mathsf{g}$ (DF2) $\mathsf{e}+_{\mathsf{b}}0\equiv\mathsf{b}\,;\mathsf{e}$ (DF3) $\mathsf{b}\,;(\mathsf{e}+_{\mathsf{b}}\mathsf{f})\equiv\mathsf{b}\,;\mathsf{e}$ (DF4) $(\mathsf{e}+_{\mathsf{b}}\mathsf{f})+_{\mathsf{c}}\mathsf{g}\equiv(\mathsf{e}+_{\mathsf{bc}}\mathsf{f})+_{\mathsf{c}}\mathsf{g}$ (DF5) $(\mathsf{e}+_{\mathsf{b}}\mathsf{f})+_{\mathsf{c}}(\mathsf{g}+_{\mathsf{b}}\mathsf{h})\equiv(\mathsf{e}+_{\mathsf{c}}\mathsf{g})+_{\mathsf{b}}(\mathsf{f}+_{\mathsf{c}}\mathsf{h})$ (DF6) $\mathsf{b}\,;(\mathsf{e}+_{\mathsf{c}}\mathsf{f})\equiv\mathsf{b}\,;\mathsf{e}+_{\mathsf{c}}\mathsf{b}\,;\mathsf{f}$ (DF7) $\mathsf{b}\,;(\mathsf{e}+_{\mathsf{c}}\mathsf{f})\equiv\mathsf{b}\,;(\mathsf{b}\,;\mathsf{e}+_{\mathsf{c}}\mathsf{f})$ (DF8) $(\mathsf{e}+_{\mathsf{b}}\mathsf{f})\oplus_r\mathsf{g}\equiv(\mathsf{e}\oplus_r\mathsf{g})+_{\mathsf{b}}(\mathsf{f}\oplus_r\mathsf{g})$ (DF9) $(\mathsf{e}+_{\mathsf{b}}\mathsf{f})\oplus_r(\mathsf{g}+_{\mathsf{b}}\mathsf{h})\equiv(\mathsf{e}\oplus_r\mathsf{g})+_{\mathsf{b}}(\mathsf{f}\oplus_r\mathsf{h})$ (DF10) $\mathsf{b}\,;(\mathsf{e}\oplus_r\mathsf{f})\equiv\mathsf{b}\,;\mathsf{e}\oplus_r\mathsf{b}\,;\mathsf{f}$ (DF11) $\mathsf{e}\oplus_r(\mathsf{f}\oplus_s\mathsf{g})\equiv(\mathsf{e}\oplus_k\mathsf{f})\oplus_z\mathsf{g}$，其中 $k=\frac{r}{1-(1-r)(1-s)}$ 且 $l=1-(1-r)(1-s)$。(DF12) $\mathsf{e}+_1\mathsf{f}\equiv\mathsf{e}$

证明。 我们将 [64] （DF1）、（DF2）、（DF3）和（DF6）。其他等价关系的证明如下。

(DF4) 推导如下。

$$\begin{aligned}
(\mathsf{e}+_{\mathsf{b}}\mathsf{f})+_{\mathsf{c}}\mathsf{g}&\equiv\mathsf{c}\,;(\mathsf{e}+_{\mathsf{b}}\mathsf{f})+_{\mathsf{c}}\mathsf{g} && \text{(G2)}\\
&\equiv((\mathsf{e}+_{\mathsf{b}}\mathsf{f})+_{\mathsf{c}}0)+_{\mathsf{c}}\mathsf{g} && \text{(DF2)}\\
&\equiv(\mathsf{e}+_{\mathsf{bc}}(\mathsf{f}+_{\mathsf{c}}0))+_{\mathsf{c}}\mathsf{g} && \text{(G4)}\\
&\equiv((\mathsf{e}+_{\mathsf{bc}}\mathsf{f})+_{\mathsf{bc}+\mathsf{c}}0)+_{\mathsf{c}}\mathsf{g} && \text{(DF1)}\\
&\equiv((\mathsf{e}+_{\mathsf{bc}}\mathsf{f})+_{\mathsf{c}}0)+_{\mathsf{c}}\mathsf{g} && \text{(Boolean algebra)}\\
&\equiv\mathsf{c}\,;((\mathsf{e}+_{\mathsf{bc}}\mathsf{f})+_{\mathsf{c}}0)+_{\mathsf{c}}\mathsf{g} && \text{(G2)}\\
&\equiv\mathsf{c}\,;(\mathsf{e}+_{\mathsf{bc}}\mathsf{f})+_{\mathsf{c}}\mathsf{g} && \text{(DF3)}\\
&\equiv(\mathsf{e}+_{\mathsf{bc}}\mathsf{f})+_{\mathsf{c}}\mathsf{g} && \text{(G2)}
\end{aligned}$$

(DF5) 推导如下。

$$\begin{aligned}
(e +_b f) +_c (g +_b h) &\equiv e +_{bc} (f +_c (g +_b h)) && \text{(G4)}\\
&\equiv e +_{bc} ((g +_b h) +_{\bar{c}} f) && \text{(G3)}\\
&\equiv e +_{bc} (g +_{b\bar{c}} (h +_{\bar{c}} f)) && \text{(G4)}\\
&\equiv e +_{bc} (g +_{b\bar{c}} (f +_c h)) && \text{(G3)}\\
&\equiv (e +_{bc} g) +_{b\bar{c}+bc} (f +_c h) && \text{(DF1)}\\
&\equiv (e +_{bc} g) +_b (f +_c h) && \text{(Boolean algebra)}\\
&\equiv (e +_c g) +_b (f +_c h) && \text{(DF4)}
\end{aligned}$$

(DF7) 推导如下。

$$\begin{aligned}
b ; (e +_c f) &\equiv b ; e +_c b ; f && \text{(DF6)}\\
&\equiv bb ; e +_c b ; f && \text{(Boolean algebra)}\\
&\equiv b ; b ; e +_c b ; f && \text{(S8)}\\
&\equiv b ; (b ; e +_c f) && \text{(DF6)}
\end{aligned}$$

(DF8) 推导如下。

$$\begin{aligned}
(e +_b f) \oplus_r g &\equiv g \oplus_{1-r} (e +_b f) && \text{(P3)}\\
&\equiv (g \oplus_{1-r} e) +_b (g \oplus_{1-r} f) && \text{(D)}\\
&\equiv (e \oplus_r g) +_b (f \oplus_r g) && \text{(P3)}
\end{aligned}$$

(DF9) 推导如下。

$$\begin{aligned}
(e +_b f) \oplus_r (g +_b h) &\equiv ((e +_b f) \oplus_r g) +_b ((e +_b f) \oplus_r h) && \text{(D)}\\
&\equiv ((e \oplus_r g) +_b (f \oplus_r g)) +_b ((e +_b f) \oplus_r h) && \text{(DF8)}\\
&\equiv b ; ((e \oplus_r g) +_b (f \oplus_r g)) +_b ((e +_b f) \oplus_r h) && \text{(G2)}\\
&\equiv b ; (e \oplus_r g) +_b ((e +_b f) \oplus_r h) && \text{(DF3)}\\
&\equiv (e \oplus_r g) +_b ((e +_b f) \oplus_r h) && \text{(G2)}\\
&\equiv ((e +_b f) \oplus_r h) +_{\bar{b}} (e \oplus_r g) && \text{(G3)}\\
&\equiv ((f +_{\bar{b}} e) \oplus_r h) +_{\bar{b}} (e \oplus_r g) && \text{(G3)}\\
&\equiv ((f \oplus_r h) +_{\bar{b}} (e \oplus_r h)) +_{\bar{b}} (e \oplus_r g) && \text{(DF8)}\\
&\equiv \bar{b} ; ((f \oplus_r h) +_{\bar{b}} (e \oplus_r h)) +_{\bar{b}} (e \oplus_r g) && \text{(G2)}\\
&\equiv \bar{b} ; (f \oplus_r h) +_{\bar{b}} (e \oplus_r g) && \text{(DF3)}\\
&\equiv (f \oplus_r h) +_{\bar{b}} (e \oplus_r g) && \text{(G2)}\\
&\equiv (e \oplus_r g) +_b (f \oplus_r h) && \text{(G3)}
\end{aligned}$$

(DF10) 我们推导如下。

$$\begin{aligned}
b ; (e \oplus_r f) &\equiv (e \oplus_r f) +_b 0 && \text{(DF2)}\\
&\equiv (e \oplus_r f) +_b (0 \oplus_r 0) && \text{(P1)}\\
&\equiv (e +_b 0) \oplus_r (f +_b 0) && \text{(DF9)}\\
&\equiv b ; e \oplus_r b ; f
\end{aligned}$$

(DF11) 我们推导如下。

$$\begin{aligned}
\mathsf{e} \oplus_r (\mathsf{f} \oplus_s \mathsf{g}) &\equiv (\mathsf{f} \oplus_s \mathsf{g}) \oplus_{1-r} \mathsf{e} && \text{(P3)}\\
&\equiv (\mathsf{g} \oplus_{1-s} \mathsf{f}) \oplus_{1-r} \mathsf{e} && \text{(P3)}\\
&\equiv \mathsf{g} \oplus_{(1-r)(1-s)} (\mathsf{f} \oplus_{\frac{s(1-r)}{1-(1-r)(1-s)}} \mathsf{e}) && \text{(P4)}\\
&\equiv \mathsf{g} \oplus_{1-l} (\mathsf{f} \oplus_{1-k} \mathsf{e}) \qquad (k = \tfrac{r}{1-(1-r)(1-s)} \text{ and } l = 1-(1-r)(1-s)) &&\\
&\equiv (\mathsf{f} \oplus_{1-k} \mathsf{e}) \oplus_l \mathsf{g} && \text{(P3)}\\
&\equiv (\mathsf{e} \oplus_k \mathsf{f}) \oplus_l \mathsf{g} && \text{(P3)} \quad \blacktriangleleft
\end{aligned}$$

(D12) 我们推导如下。

$$\begin{aligned}
\mathsf{e} +_1 \mathsf{f} &\equiv 1 ; (\mathsf{e} +_1 \mathsf{f}) && \text{(S1)}\\
&\equiv \mathsf{e} && \text{(DF3)}
\end{aligned}$$

D.2 广义守卫和凸和系数

现在我们严格定义广义求和算子，并验证它们的行为符合预期。首先介绍守卫求和。

▶ **定义 51**。 考虑一个子集 $\Phi \subseteq$ 原子 以及一个集合 $\{$表达式$_\alpha\}_{\alpha\in\Phi}$，使得对于所有 $\alpha \in \Phi$，表达式$_\alpha \in$ Exp。广义受保护和 是一个按以下方式归纳定义的表达式。

$$\bigdoubleplus_{\alpha\in\Phi} \mathsf{e}_\alpha = \mathsf{e}_\gamma +_\gamma \left(\bigdoubleplus_{\alpha\in\Phi\setminus\{\gamma\}} \mathsf{e}_\alpha \right) \quad \textit{if } \gamma \in \Phi \qquad\qquad \bigdoubleplus_{\alpha\in\Phi} \mathsf{e}_\alpha = 0 \quad \textit{if } \Phi = \emptyset$$

在展开归纳定义时，从该集合中选择表达式的方式并不明确。然而，所有可能的选择方式都是等价的。

▶ **引理 52** ([64,引理 B.1]). 广义受保护和在 $\equiv$ 意义下是良定义的

我们首先回顾 [64] 中广义受保护和的性质。

▶ **引理 53** ([64, 引理 B.2])。 设 b,c $\in$ BExp 并设 $\{\mathsf{e}_\alpha\}_{\alpha\in\mathsf{At}}$ 为一个指标化集合，满足 e$_\alpha \in$ Exp 对所有 $\alpha \in$原子均成立。于是，

$$\mathsf{c} ; \bigdoubleplus_{\alpha\le_{\mathsf{BA}}\mathsf{b}} \mathsf{e}_\alpha \equiv \bigdoubleplus_{\alpha\le_{\mathsf{BA}}\mathsf{bc}} \mathsf{e}_\alpha$$

请注意，在上述引理中，与 [64] 类似，我们滥用记号，将 $\alpha \le_{\mathsf{BA}}$ c 写作集合$\{\alpha \mid \alpha \le_{\mathsf{BA}} \mathsf{c}\}$。由于集合T 是有限的，由它生成的布尔代数是原子的，因此每个c $\in$ BExp 都对应于原子的一个子集。

▶ **引理54** ([64, 引理B。4])。 设 $\Phi \subseteq$原子 和 $\{\mathsf{e}_\alpha\}_{\alpha\in\Phi}$ 是一个指标化集合，使得e$_\alpha \in$ Exp 对每个 $\alpha \in \Phi$ 都成立。那么，

$$\bigdoubleplus_{\alpha\in\Phi} \mathsf{e}_\alpha \equiv \bigdoubleplus_{\alpha\in\Phi} \alpha ; \mathsf{e}_\alpha$$

现在，我们陈述广义受保护和的其他性质，这些性质将在定理 14 的证明中使用。

▶ **引理 55.** 设 $\Phi \subseteq$ 原子 和 $\{\mathsf{e}_\alpha\}_{\alpha\in\Phi}$ 构成一个指标化集合，使得 $\mathsf{e}_\alpha \in \mathtt{Exp}$ 对每个$\alpha \in \Phi$ 都成立，并设 $\mathsf{f} \in \mathtt{Exp}$。那么，

$$\left(\bigdotplus_{\alpha\in\Phi} \mathsf{e}_\alpha\right);\mathsf{f} \equiv \bigdotplus_{\alpha\in\Phi} \mathsf{e}_\alpha;\mathsf{f}$$

证明。 根据 Φ 的大小进行归纳。对于基本情况，当 $\Phi = \emptyset$ 时，考虑以下内容。

$$\left(\bigdotplus_{\alpha\in\Phi} \mathsf{e}_\alpha\right);\mathsf{f} \equiv 0;\mathsf{f} \equiv 0 \equiv \bigdotplus_{\alpha\in\Phi} \mathsf{e}_\alpha;\mathsf{f}$$

对于归纳步骤，我们有

$$\begin{aligned}
\left(\bigdotplus_{\alpha\in\Phi} \mathsf{e}_\alpha\right);\mathsf{f} &\equiv \left(\mathsf{e}_\gamma +_\gamma \bigdotplus_{\alpha\in\Phi\setminus\{\gamma\}} \mathsf{e}_\alpha\right);\mathsf{f} && (\Phi \text{ is nonempty})\\
&\equiv \left(\mathsf{e}_\gamma;\mathsf{f} +_\gamma \left(\bigdotplus_{\alpha\in\Phi\setminus\{\gamma\}} \mathsf{e}_\alpha\right);\mathsf{f}\right) && (\mathsf{S5})\\
&\equiv \mathsf{e}_\gamma;\mathsf{f} +_\gamma \left(\bigdotplus_{\alpha\in\Phi\setminus\{\gamma\}} \mathsf{e}_\alpha;\mathsf{f}\right) && (\text{Induction hypothesis})\\
&\equiv \bigdotplus_{\alpha\in\Phi} \mathsf{e}_\alpha;\mathsf{f} && \blacktriangleleft
\end{aligned}$$

▶ **引理 56.** 令 $\Phi \subseteq$ 原子 且令 $\{\mathsf{e}_\alpha\}_{\alpha\in\Phi}$ 和 $\{\mathsf{f}_\alpha\}_{\alpha\in\Phi}$ 为带索引集合，使得e_α,$\mathsf{f}_\alpha \in \mathtt{Exp}$ 对每个 $\alpha \in \Psi$ 成立，并令 $r \in [0,1]$. 那么，

$$\left(\bigdotplus_{\alpha\in\Phi} \mathsf{e}_\alpha\right) \oplus_r \left(\bigdotplus_{\alpha\in\Phi} \mathsf{f}_\alpha\right) \equiv \bigdotplus_{\alpha\in\Phi} (\mathsf{e}_\alpha \oplus_r \mathsf{f}_\alpha)$$

证明。 按 Φ的大小进行归纳。对于基础情形，考虑以下内容。

$$\left(\bigdotplus_{\alpha\in\Phi} \mathsf{e}_\alpha\right) \oplus_r \left(\bigdotplus_{\alpha\in\Phi} \mathsf{f}_\alpha\right) \equiv 0 \oplus_r 0 \equiv 0 \equiv \bigdotplus_{\alpha\in\Phi} (\mathsf{e}_\alpha \oplus_r \mathsf{f}_\alpha)$$

对于归纳步骤，我们有♀♀♀♀♀♀

$$\begin{aligned}
\left(\bigdotplus_{\alpha\in\Phi} \mathsf{e}_\alpha\right) \oplus_r \left(\bigdotplus_{\alpha\in\Phi} \mathsf{f}_\alpha\right) &\equiv \left(\mathsf{e}_\gamma +_\gamma \bigdotplus_{\alpha\in\Phi\setminus\{\gamma\}} \mathsf{e}_\alpha\right) \oplus_r \left(\mathsf{f}_\gamma +_\gamma \bigdotplus_{\alpha\in\Phi\setminus\{\gamma\}} \mathsf{f}_\alpha\right)\\
&\equiv (\mathsf{e}_\gamma \oplus_r \mathsf{f}_\gamma) +_\mathsf{b} \left(\left(\bigdotplus_{\alpha\in\Phi\setminus\{\gamma\}} \mathsf{e}_\alpha\right) \oplus_r \left(\bigdotplus_{\alpha\in\Phi\setminus\{\gamma\}} \mathsf{f}_\alpha\right)\right) && (\mathsf{DF9})\\
&\equiv (\mathsf{e}_\gamma \oplus_r \mathsf{f}_\gamma) +_\mathsf{b} \left(\bigdotplus_{\alpha\in\Phi\setminus\{\gamma\}} (\mathsf{e}_\alpha \oplus_r \mathsf{f}_\alpha)\right) && (\text{Induction hypothesis})\\
&\equiv \bigdotplus_{\alpha\in\Phi} (\mathsf{e}_\alpha \oplus_r \mathsf{f}_\alpha) && \blacktriangleleft
\end{aligned}$$

▶ 注释 57. 就符号表示而言，给定 $\Phi, \Psi \subseteq$ 原子，使得 $\Psi \cap \Theta = \emptyset$，以及指标化集合 $\{\mathsf{e}_\alpha\}_{\alpha\in\Psi}$、$\{\mathsf{f}_\alpha\}_{\alpha\in\Phi}$，满足对于每个 $\alpha \in \Phi$，$\mathsf{e}_\alpha \in \mathtt{Exp}$，且对于每个 $\alpha \in \Psi$，f_α，我们将记作

$$\bigdoublebarwedge_{\alpha\in\Psi} \mathsf{e}_\alpha + \bigdoublebarwedge_{\alpha\in\Theta} \mathsf{f}_\alpha$$

表示如下内容

$$\bigdoublebarwedge_{\alpha\in\Phi\cup\Psi} \mathsf{g}_\alpha \qquad \text{where} \qquad \mathsf{g}_\alpha = \begin{cases} \mathsf{e}_\alpha & \text{if } \alpha \in \Phi \\ \mathsf{f}_\alpha & \text{if } \alpha \in \Psi \end{cases}$$

接下来介绍广义凸和。

▶**定义 58**。给定一个非空有限指标集 I 以及指标化集合 $\{r_i\}_{i\in I}$ 和 $\{\mathsf{e}_i\}_{i\in I}$，使得 $\mathsf{e}_i \in \mathtt{Exp}$，且对于所有满足 $\sum_{i\in I} r_i = 1$ 的 $i \in I$，都有 $r_i \in [0,1]$，我们将广义凸和 定义为由以下归纳定义给出的一个表达式

$$\bigoplus_{i\in I} r_i \cdot \mathsf{e}_i = \mathsf{e}_j \oplus_{r_j} \left(\bigoplus_{i\in I\setminus\{j\}} \frac{r_i}{1-r_j} \cdot \mathsf{e}_i \right) \quad \textit{for } j \in I \textit{ and } r_j \neq 1$$

$$\bigoplus_{i\in\{j\}} r_i \cdot \mathsf{e}_i = \mathsf{e}_j \quad \textit{otherwise}$$

同样，上述定义在从集合中选择表达式时存在歧义 ，
不过，该定义所有可能的展开都可以证明在 $\equiv$意义下等价。

▶**引理 59.** 广义凸和在 $\equiv$ 下定义良好

证明. 设 I 是一个有限非空指标集，$\{\mathsf{e}_i\}_{i\in I}$ 以及 $\{r_i\}_{i\in I}$ 是带索引集合，使得对所有 $i \in I$ 都有 $\mathsf{e}_i \in \mathtt{Exp}$ 且 $r_i \in [0,1]$。

我们通过对指标集的大小I进行归纳，证明广义和定义良好。当 $I = \{j\}$ 时，结论显然成立，因为此时广义和定义为 e_j。

当 $I = \{j,k\}$ 时，我们有

$$\begin{aligned} \mathsf{e}_j \oplus_{r_j} \left(\bigoplus_{i\in\{k\}} r_i \cdot \mathsf{e}_i \right) &\equiv \mathsf{e}_j \oplus_{r_j} \mathsf{e}_k \equiv \mathsf{e}_k \oplus_{1-r_j} \mathsf{e}_j && \text{(P3)} \\ &\equiv \mathsf{e}_k \oplus_{r_k} \mathsf{e}_j && (r_j + r_k = 1) \\ &\equiv \mathsf{e}_k \oplus_{r_k} \left(\bigoplus_{i\in\{j\}} r_i \cdot \mathsf{e}_i \right) \end{aligned}$$

对于归纳步骤，假设 $|I| > 2$ 且 $j,\ k \in I$。考虑以下内容。

$$\mathsf{e}_j \oplus_{r_j} \left(\bigoplus_{i \in I \setminus \{j\}} \frac{r_i}{1-r_j} \cdot \mathsf{e}_i \right) \equiv \mathsf{e}_j \oplus_{r_j} \left(\mathsf{e}_k \oplus_{\frac{r_k}{1-r_j}} \left(\bigoplus_{i \in I \setminus \{j,k\}} \frac{r_i}{(1-r_j)(1-r_k)} \cdot \mathsf{e}_i \right) \right)$$

$$\equiv \left(\mathsf{e}_j \oplus_{\frac{r_j}{r_j+r_k}} \mathsf{e}_k \right) \oplus_{r_j+r_k} \left(\bigoplus_{i \in I \setminus \{j,k\}} \frac{r_i}{(1-r_j)(1-r_k)} \cdot \mathsf{e}_i \right) \tag{DF11}$$

$$\equiv \left(\mathsf{e}_k \oplus_{\frac{r_k}{r_j+r_k}} \mathsf{e}_j \right) \oplus_{r_j+r_k} \left(\bigoplus_{i \in I \setminus \{j,k\}} \frac{r_i}{(1-r_j)(1-r_k)} \cdot \mathsf{e}_i \right) \tag{P3}$$

$$\equiv \mathsf{e}_k \oplus_{r_k} \left(\mathsf{e}_j \oplus_{\frac{r_j}{1-r_k}} \left(\bigoplus_{i \in I \setminus \{j,k\}} \frac{r_i}{(1-r_j)(1-r_k)} \cdot \mathsf{e}_i \right) \right) \tag{P4}$$

$$\equiv \mathsf{e}_k \oplus_{r_k} \left(\bigoplus_{i \in I \setminus \{k\}} \frac{r_i}{1-r_k} \cdot \mathsf{e}_i \right) \qquad \blacktriangleleft$$

▶ 注 60. 在记号方面，给定非空有限指标集 I 和 J，以及概率集合$\{r_i\}_{i \in I}$ 和 $\{s_j\}_{j \in J}$，还有满足 $\sum_{i \in I} r_i + \sum_{j \in J} s_j = 1$ 和 $I \cap J = \emptyset$ 的表达式集合$\{\mathsf{e}_i\}_{i \in I}$ 和 $\{\mathsf{f}_j\}_{j \in J}$，我们将记作

$$\bigoplus_{i \in I} r_i \cdot \mathsf{e}_i \oplus \bigoplus_{j \in I} s_i \cdot \mathsf{f}_i$$

以表示广义凸和

$$\bigoplus_{k \in I \cup J} t_k \cdot \mathsf{g}_k \qquad \text{where} \quad t_k = \begin{cases} r_k & \text{if } k \in I \\ s_k & \text{if } k \in J \end{cases} \quad \text{and} \quad \mathsf{g}_k = \begin{cases} \mathsf{e}_k & \text{if } k \in I \\ \mathsf{f}_k & \text{if } k \in J \end{cases}$$

当指标集 $I = \{j\}$ 为单元素集，且集合为 $\{r_i\}_{i \in I}, \{\mathsf{e}_i\}_{i \in I}$时，我们将简写为 $r_j \cdot \mathsf{e}_j$，而不写作 $\bigoplus_{i \in I} r_i \cdot \mathsf{e}_i$

▶**引理 61.** 设 I 为非空有限指标集，$\{r_i\}_{i \in I}$ 和 $\{\mathsf{e}_i\}_{i \in I}$ 为指标化集合，且满足 $r_i \in [0,1]$，并且对于所有 $i \in I$ 都有 $\mathsf{e}_i \in \mathtt{Exp}$，再设 $\mathsf{f} \in \mathtt{Exp}$。那么，

$$\left(\bigoplus_{i \in I} r_i \cdot \mathsf{e}_i \right) ; \mathsf{f} \equiv \bigoplus_{i \in I} r_i \cdot \mathsf{e}_i ; \mathsf{f}$$

P上界。 对指标集的大小进行归纳 I。对于基础情形，当 $I = \{j\}$ 我们有

$$\left(\bigoplus_{i \in I} r_i \cdot \mathsf{e}_i \right) ; \mathsf{f} \equiv \mathsf{e}_\mathsf{j} ; \mathsf{f} \equiv \bigoplus_{i \in I} r_i \cdot \mathsf{e}_i ; \mathsf{f}$$

对于归纳步骤，考虑以下内容

$$\begin{aligned}
\left(\bigoplus_{i\in I} r_i\cdot \mathsf{e}_i\right);\mathsf{f} &\equiv \left(\mathsf{e}_j \oplus_{r_j} \left(\bigoplus_{i\in I\setminus\{j\}} \frac{r_i}{1-r_j}\cdot \mathsf{e}_i\right)\right);\mathsf{f} && (j\in I)\\
&\equiv \mathsf{e}_j;\mathsf{f} \oplus_{r_j} \left(\bigoplus_{i\in I\setminus\{j\}} \frac{r_i}{1-r_j}\cdot \mathsf{e}_i\right);\mathsf{f} && (\mathsf{S6})\\
&\equiv \mathsf{e}_j;\mathsf{f} \oplus_{r_j} \left(\bigoplus_{i\in I\setminus\{j\}} \frac{r_i}{1-r_j}\cdot \mathsf{e}_i;\mathsf{f}\right) && (\text{Induction hypothesis})\\
&\equiv \bigoplus_{i\in I} r_i\cdot \mathsf{e}_i;\mathsf{f} && \blacktriangleleft
\end{aligned}$$

►**引理 62.** 设 I 是一个非空指标集，$\{r_i\}_{i\in I}$ 和 $\{\mathsf{e}_i\}_{i\in I}$ 是指标化集合，且对所有 $i\in I$、$i\in[0,1]$ 和 $\mathsf{e}_i\in \mathsf{Exp}$均成立。设 e 是一个表达式，使得 $\mathsf{e}=\mathsf{e}_k$，其中某个$k\in I$。则有

$$\bigoplus_{i\in I} r_i\cdot \mathsf{e}_i \equiv \bigoplus_{j\in J} s_j\cdot \mathsf{f}_j$$

$$\textit{where } J=\{\mathsf{e}\}\cup\{i\in I\mid \mathsf{e}_i\neq \mathsf{e}\},\ \{\mathsf{f}_j\}_{j\in J}=\begin{cases}\mathsf{e} & \textit{if } j=\mathsf{e}\\ \mathsf{e}_i & \textit{if } j=i\end{cases} \textit{ and } \{s_j\}_{j\in J}=\begin{cases}\sum_{\mathsf{e}_i=\mathsf{e}} r_i & \textit{if } j=\mathsf{e}\\ r_i & \textit{if } j=i\end{cases}$$

证明。 不失一般性，我们可以假设 $I=\{1,\dots,n\}$ 对于某个 $n\in\mathbb{N}$ 并且根据引理 59，我们可以放心地假设存在 $k\in\mathbb{N}$ 使得对所有 $i\in I$，若 $i\le k$ 则有 $\mathsf{e}_i=\mathsf{e}$，且对所有 $i\in I$ 若 $i>k$ 则有 $\mathsf{e}_i\neq\mathsf{e}$。

我们对 k 进行归纳。若 $k=1$，则所需性质立即成立。对于归纳步骤，考虑以下情况。

$$\begin{aligned}
\bigoplus_{i\in I} r_i\cdot \mathsf{e}_i &\equiv \mathsf{e}_k \oplus_{r_k} \left(\bigoplus_{i\in I\setminus\{k\}} \frac{r_i}{1-r_k}\cdot \mathsf{e}_i\right) && (k\in I)\\
&\equiv \mathsf{e} \oplus_{r_k} \left(\bigoplus_{i\in I\setminus\{k\}} \frac{r_i}{1-r_k}\cdot \mathsf{e}_i\right) && (\mathsf{e}=\mathsf{e}_k)
\end{aligned}$$

在归纳步骤中，我们将使用以下简写

$$n=\sum_{\mathsf{e}_i=\mathsf{e}}^{i<k} r_i \qquad m=\frac{n}{1-r_k}$$

利用归纳假设，我们可以将上述表达式重写为

$$\begin{aligned}
&\mathsf{e} \oplus r_k \left(\mathsf{e} \oplus_m \left(\bigoplus_{i \in I \setminus \{\mathsf{e}, k\}} \frac{r_i}{(1-r_k)(1-m)} \cdot \mathsf{e}_i \right) \right) \\
&\quad \equiv \left(\mathsf{e} \oplus_{\frac{r_k}{r_k+m}} \mathsf{e} \right) \oplus_{r_k+n} \left(\bigoplus_{i \in I \setminus \{\mathsf{e}, k\}} \frac{r_i}{(1-r_k)(1-m)} \cdot \mathsf{e}_i \right) && \text{(DF11)} \\
&\quad \equiv \mathsf{e} \oplus_{r_k+n} \left(\bigoplus_{i \in I \setminus \{\mathsf{e}, k\}} \frac{r_i}{(1-r_k)(1-m)} \cdot \mathsf{e}_i \right) && \text{(P1)} \\
&\quad \equiv \mathsf{e} \oplus_{r_k+n} \left(\bigoplus_{i \in I \setminus \{\mathsf{e}, k\}} \frac{r_i}{1-(r_k+n)} \cdot \mathsf{e}_i \right) \\
&\quad \equiv \mathsf{e} \oplus_{r_k+n} \left(\bigoplus_{j \in J \setminus \{\mathsf{e}\}} \frac{s_j}{1-(r_k+n)} \cdot \mathsf{f}_j \right) \equiv \bigoplus_{j \in J} s_j \cdot \mathsf{f}_j && \blacktriangleleft
\end{aligned}$$

▶**引理 63**。 设 I 为一个非空有限指标集，$\{r_i\}_{i \in I}$ 和 $\{\mathsf{e}_i\}_{i \in I}$ 为带索引集合，使得 $r_i \in [0,1]$ 且对于所有 $i \in I$，均有 $\mathsf{e}_i \in \mathtt{Exp}$。令 $E = \bigcup_{i \in I} \{\mathsf{e}_i\}$。那么，

$$\bigoplus_{i \in I} r_i \cdot \mathsf{e}_i \equiv \bigoplus_{\mathsf{e} \in E} \left(\sum_{\mathsf{e}_i = \mathsf{e}} r_i \right) \cdot \mathsf{e}$$

证明。 对 E 的大小进行归纳。在基础情形中，当 E 是单元素集合时，根据引理 62，结论立即成立。在归纳步骤中，考虑如下情况。设 $\mathsf{g} \in E$ 是任意表达式，并令 $J = \{\mathsf{g}\} \cup \{i \in I \mid \mathsf{e}_i \neq \mathsf{g}\}$，

$$m = \sum_{\mathsf{e}_i = \mathsf{g}} r_i \qquad \text{and} \qquad \{\mathsf{f}_j\}_{j \in J} = \begin{cases} \mathsf{e} & \text{if } j = \mathsf{g} \\ \mathsf{e}_i & \text{if } j = i \end{cases} \qquad \text{and} \qquad \{s_j\}_{j \in J} = \begin{cases} m & \text{if } j = \mathsf{g} \\ r_i & \text{if } j = i \end{cases}$$

我们现在已经得到，

$$\begin{aligned}
\bigoplus_{i \in I} r_i \cdot \mathsf{e}_i &\equiv \bigoplus_{j \in J} s_j \cdot \mathsf{f}_j && \text{(Lemma 62)} \\
&\equiv \mathsf{g} \oplus_m \left(\bigoplus_{j \in J \setminus \{\mathsf{g}\}} \frac{s_j}{1-m} \cdot \mathsf{f}_j \right) \\
&\equiv \mathsf{g} \oplus_m \left(\bigoplus_{\mathsf{e} \in E \setminus \{\mathsf{g}\}} \left(\sum_{\mathsf{e}_i = \mathsf{e}} \frac{r_i}{1-m} \right) \cdot \mathsf{e} \right) && \text{(Induction hypothesis)} \\
&\equiv \bigoplus_{\mathsf{e} \in E} \left(\sum_{\mathsf{e}_i = \mathsf{e}} r_i \right) \cdot \mathsf{e} && \blacktriangleleft
\end{aligned}$$

▶**引理 64**。 设 I 为一个非空有限指标集，$\{r_i\}_{i \in I}$ 和 $\{\mathsf{e}_i\}_{i \in I}$ 为指标化集合，使得 $r_i \in [0,1]$ 且对于所有 $i \in I$，均有 $\mathsf{e}_i \in \mathtt{Exp}$。设 $E = \bigcup_{i \in I} \{\mathsf{e}_i\}$。那么，

$$\bigoplus_{i \in I} r_i \cdot \mathsf{e}_i \equiv \bigoplus_{[\mathsf{e}]_\equiv \in E/\equiv} \left(\sum_{\mathsf{e}_i \equiv \mathsf{e}} r_i \right) \cdot \mathsf{e}$$

证明。 将严格相等替换为$\equiv$，可以得到一个与引理 62 类似的结果。利用该结果，可以通过调整引理 63 来证明所需结果。 ◀

D.3 基本定理

▶ **定理 14** (基本定理)。 对于每个 $\mathsf{e} \in \mathtt{Exp}$， 都有ՠբեջ

$$\mathsf{e} \equiv \mathop{\mathbin{+\!\!\!-}}_{\alpha \in \mathsf{At}} \left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{e})_\alpha)} \partial(\mathsf{e})_\alpha(d) \cdot \mathtt{exp}(d) \right)$$

其中 $\mathtt{exp}$ 定义了一个函数 $2 +$ 输出 $+$动作集 $\times \mathtt{Exp} \to \mathtt{Exp}$， 其定义为

$\mathtt{exp}(\,) = 0 \quad \mathtt{exp}(\checkmark) = 1 \quad \mathtt{exp}(v) = v \quad \mathtt{exp}(\mathsf{a},\mathsf{f}) = \mathsf{a}$； $\mathsf{f}\,(v \in$输出， $\mathsf{a} \in$动作集 和 $\mathsf{f} \in \mathtt{Exp}$)**证明**。 我们对 $\mathsf{e} \in \mathtt{Exp}$的构造进行结构归纳。基例显然成立，因此我们只证明其中一个。

$\boxed{\mathsf{e} = \mathsf{a}}$

$$\begin{aligned}
\mathsf{a} &\equiv \mathop{\mathbin{+\!\!\!-}}_{\alpha \in \mathsf{At}} \mathsf{a} && \text{(G1)}\\
&\equiv \mathop{\mathbin{+\!\!\!-}}_{\alpha \in \mathsf{At}} \mathsf{a}\,;1 && \text{(S2)}\\
&\equiv \mathop{\mathbin{+\!\!\!-}}_{\alpha \in \mathsf{At}} \left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{a})_\alpha)} \partial(\mathsf{a})_\alpha(d) \cdot \mathtt{exp}(d) \right) && \text{(Def. of } \partial)
\end{aligned}$$

现在，我们可以继续进行归纳步骤。

$\boxed{\mathsf{e} = \mathsf{f} +_{\mathsf{b}} \mathsf{g}}$

$$\begin{aligned}
\mathsf{e} &\equiv \mathsf{f} +_{\mathsf{b}} \mathsf{g}\\
&\equiv \left(\mathop{\mathbin{+\!\!\!-}}_{\alpha \in \mathsf{At}} \left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\alpha)} \partial(\mathsf{f})_\alpha(d) \cdot \mathtt{exp}(d) \right) \right)\\
&\qquad +_{\mathsf{b}} \left(\mathop{\mathbin{+\!\!\!-}}_{\alpha \in \mathsf{At}} \left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{g})_\alpha)} \partial(\mathsf{g})_\alpha(d) \cdot \mathtt{exp}(d) \right) \right) && \text{(Ind. hypothesis)}\\
&\equiv \mathsf{b}\,; \left(\mathop{\mathbin{+\!\!\!-}}_{\alpha \in \mathsf{At}} \left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\alpha)} \partial(\mathsf{f})_\alpha(d) \cdot \mathtt{exp}(d) \right) \right)\\
&\qquad +_{\mathsf{b}} \bar{\mathsf{b}}\,; \left(\mathop{\mathbin{+\!\!\!-}}_{\alpha \in \mathsf{At}} \left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{g})_\alpha)} \partial(\mathsf{g})_\alpha(d) \cdot \mathtt{exp}(d) \right) \right) && \text{(G3 and G2)}\\
&\equiv \mathsf{b}\,;\mathsf{b}\,; \left(\mathop{\mathbin{+\!\!\!-}}_{\alpha \in \mathsf{At}} \left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\alpha)} \partial(\mathsf{f})_\alpha(d) \cdot \mathtt{exp}(d) \right) \right)\\
&\qquad +_{\mathsf{b}} \bar{\mathsf{b}}\,;\bar{\mathsf{b}}\,; \left(\mathop{\mathbin{+\!\!\!-}}_{\alpha \in \mathsf{At}} \left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{g})_\alpha)} \partial(\mathsf{g})_\alpha(d) \cdot \mathtt{exp}(d) \right) \right) && \text{(Boolean algebra and S8)}\\
&\equiv \mathsf{b}\,; \left(\mathop{\mathbin{+\!\!\!-}}_{\alpha \leq_{\mathsf{BA}} \mathsf{b}} \left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\alpha)} \partial(\mathsf{f})_\alpha(d) \cdot \mathtt{exp}(d) \right) \right)\\
&\qquad +_{\mathsf{b}} \bar{\mathsf{b}}\,; \left(\mathop{\mathbin{+\!\!\!-}}_{\alpha \leq_{\mathsf{BA}} \bar{\mathsf{b}}} \left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{g})_\alpha)} \partial(\mathsf{g})_\alpha(d) \cdot \mathtt{exp}(d) \right) \right) && \text{(Lemma 53)}
\end{aligned}$$

$$\equiv \mathsf{b}\,;\left(\bigplus_{\alpha\leq_{\mathsf{BA}}\mathsf{b}}\left(\bigoplus_{d\in\mathsf{supp}(\partial(\mathsf{f}+_{\mathsf{b}}\mathsf{g})_\alpha)}\partial(\mathsf{f}+_{\mathsf{b}}\mathsf{g})_\alpha(d)\cdot\mathsf{exp}(d)\right)\right)$$
$$+_{\mathsf{b}}\,\bar{\mathsf{b}}\,;\left(\bigplus_{\alpha\leq_{\mathsf{BA}}\bar{\mathsf{b}}}\left(\bigoplus_{d\in\mathsf{supp}(\partial(\mathsf{f}+_{\mathsf{b}}\mathsf{g})_\alpha)}\partial(\mathsf{f}+_{\mathsf{b}}\mathsf{g})_\alpha(d)\cdot\mathsf{exp}(d)\right)\right) \quad \text{(Def. of } \partial\text{)}$$

$$\equiv \left(\bigplus_{\alpha\in\mathsf{At}}\left(\bigoplus_{d\in\mathsf{supp}(\partial(\mathsf{f}+_{\mathsf{b}}\mathsf{g})_\alpha)}\partial(\mathsf{f}+_{\mathsf{b}}\mathsf{g})_\alpha(d)\cdot\mathsf{exp}(d)\right)\right)$$
$$+_{\mathsf{b}}\left(\bigplus_{\alpha\in\mathsf{At}}\left(\bigoplus_{d\in\mathsf{supp}(\partial(\mathsf{f}+_{\mathsf{b}}\mathsf{g})_\alpha)}\partial(\mathsf{f}+_{\mathsf{b}}\mathsf{g})_\alpha(d)\cdot\mathsf{exp}(d)\right)\right) \quad \text{(Lemma 53)}$$

$$\equiv \bigplus_{\alpha\in\mathsf{At}}\left(\bigoplus_{d\in\mathsf{supp}(\partial(\mathsf{f}+_{\mathsf{b}}\mathsf{g})_\alpha)}\partial(\mathsf{f}+_{\mathsf{b}}\mathsf{g})_\alpha(d)\cdot\mathsf{exp}(d)\right) \quad \text{(G4)}$$

$\boxed{\mathsf{e}=\mathsf{f}\ \oplus_r \mathsf{g}}$

$$\mathsf{e}\equiv \mathsf{f}\oplus_r \mathsf{g}$$
$$\equiv \left(\bigplus_{\alpha\in\mathsf{At}}\left(\bigoplus_{d\in\mathsf{supp}(\partial(\mathsf{f})_\alpha)}\partial(\mathsf{f})_\alpha(d)\cdot\mathsf{exp}(d)\right)\right)$$
$$\oplus_r\left(\bigplus_{\alpha\in\mathsf{At}}\left(\bigoplus_{d\in\mathsf{supp}(\partial(\mathsf{g})_\alpha)}\partial(\mathsf{g})_\alpha(d)\cdot\mathsf{exp}(d)\right)\right) \quad \text{(Ind. hypothesis)}$$
$$\equiv \left(\bigplus_{\alpha\in\mathsf{At}}\left(\bigoplus_{d\in\mathsf{supp}(\partial(\mathsf{f})_\alpha)}\partial(\mathsf{f})_\alpha(d)\cdot\mathsf{exp}(d)\right)\oplus_r\left(\bigoplus_{d\in\mathsf{supp}(\partial(\mathsf{g})_\alpha)}\partial(\mathsf{g})_\alpha(d)\cdot\mathsf{exp}(d)\right)\right)$$
(L理 56)

注意，对于每个原子 $\alpha\in$At，广义受保护和中的表达式都可以利用公理 P4 重新排列为一个广义凸和。对于每个$\alpha\in$ At，我们将定义指标集 $I_\alpha=\mathsf{supp}(\partial(\mathsf{e})_\alpha)+\mathsf{supp}(\partial(\mathsf{f})_\alpha)$，其中我们用 $+$ 表示余积。令

$$r_i=\begin{cases}r\partial(\mathsf{f})_\alpha(i) & \text{if } i\in\mathsf{supp}(\partial(\mathsf{f})_\alpha)\\ (1-r)\partial(\mathsf{g})_\alpha(i) & \text{if } i\in\mathsf{supp}(\partial(\mathsf{g})_\alpha)\end{cases}$$

由此我们可以得到以下结果

$$\mathsf{f}\oplus_r\mathsf{g}\equiv\bigplus_{\alpha\in\mathsf{At}}\left(\bigoplus_{i\in I}r_i\cdot\mathsf{exp}(i)\right)$$

现在我们应用引理 63，通过将概率相加来移除凸和中的重复元素。由此得到以下结果

$$\bigplus_{\alpha\in\mathsf{At}}\left(\bigoplus_{d\in\mathsf{supp}(\partial(\mathsf{f})_\alpha)\cup\mathsf{supp}(\partial(\mathsf{g})_\alpha)}(r\partial(\mathsf{f})_\alpha(d)+(1-r)\partial(\mathsf{g})_\alpha(d))\cdot\mathsf{exp}(d)\right)$$

这恰好等同于

$$\bigplus_{\alpha\in\mathsf{At}}\left(\bigoplus_{d\in\mathsf{supp}(\partial(\mathsf{f}\oplus_r\mathsf{g})_\alpha)}\partial(\mathsf{f}\oplus_r\mathsf{g})_\alpha(d)\cdot\mathsf{exp}(d)\right)$$

56 模概率双模拟的概率守卫 KAT：完备性与复杂性

$\boxed{\mathsf{e} = \mathsf{f}\,;\mathsf{g}}$

$$
\begin{aligned}
&\mathsf{e} \equiv \mathsf{f}\,;\mathsf{g} \\
&\equiv \left(\bigplus_{\alpha\in\mathsf{At}}\left(\bigoplus_{d\in\mathsf{supp}(\partial(\mathsf{f})_\alpha)} \partial(\mathsf{f})_\alpha(d)\cdot\mathsf{exp}(d)\right)\right);\mathsf{g} && \text{(Induction hypothesis)}\\
&\equiv \left(\bigplus_{\alpha\in\mathsf{At}}\left(\bigoplus_{d\in\mathsf{supp}(\partial(\mathsf{f})_\alpha)} \partial(\mathsf{f})_\alpha(d)\cdot\mathsf{exp}(d)\right);\mathsf{g}\right) && \text{(Lemma 55)}\\
&\equiv \left(\bigplus_{\alpha\in\mathsf{At}}\left(\bigoplus_{d\in\mathsf{supp}(\partial(\mathsf{f})_\alpha)} \partial(\mathsf{f})_\alpha(d)\cdot\mathsf{exp}(d)\,;\mathsf{g}\right)\right) && \text{(Lemma 61)}
\end{aligned}
$$

我们可以展开广义凸和，得到如下结果

$$
\bigplus_{\alpha\in\mathsf{At}}\left(\partial(\mathsf{f})_\alpha(\checkmark)\cdot 1\,;\mathsf{g} \oplus \bigoplus_{d\in\mathsf{Out}\cup\{\mathsf{X}\}} \partial(\mathsf{f})_\alpha(d)\cdot\mathsf{exp}(d)\,;\mathsf{g} \oplus \bigoplus_{d\in\mathsf{supp}(\partial(\mathsf{f})_\alpha)\cap\mathsf{Act}\times\mathsf{Exp}} \partial(\mathsf{f})_\alpha(d)\cdot\mathsf{exp}(d)\,;\mathsf{g}\right)
$$

现在，应用 S2、S4 和 S7，以及 DF7，得到

$$
\bigplus_{\alpha\in\mathsf{At}}\left(\partial(\mathsf{f})_\alpha(\checkmark)\cdot\alpha\,;\mathsf{g} \oplus \bigoplus_{d\in\mathsf{Out}\cup\{\mathsf{X}\}} \partial(\mathsf{f})_\alpha(d)\cdot\mathsf{exp}(d) \oplus \bigoplus_{d\in\mathsf{supp}(\partial(\mathsf{f})_\alpha)\cap\mathsf{Act}\times\mathsf{Exp}} \partial(\mathsf{f})_\alpha(d)\cdot\mathsf{exp}(d)\,;\mathsf{g}\right)
$$

根据归纳假设和 DF3，对于每个 $\alpha \in$ 原子，我们可以将 $\alpha\,;\mathsf{g}$ 写为

$$
\bigoplus_{d\in\mathsf{supp}(\partial(\mathsf{g})_\alpha)} \partial(\mathsf{g})_\alpha(d)\cdot\mathsf{exp}(d)
$$

因此，将其代入前一个方程，并使用 P4 和 S3，我们可以将整个表达式改写为单个广义凸和。对于每个 $\alpha \in$原子，令 I_α 为定义如下的指标集

$$
I_\alpha = \mathsf{supp}(\partial(\mathsf{g})_\alpha) + (\mathsf{supp}(\partial(\mathsf{f})_\alpha) \cap (\{\,\} \cup \text{✗输出})) + \{(\mathsf{a},\mathsf{f}';\mathsf{g}) \mid (\mathsf{a},\mathsf{f}') \in \mathsf{supp}(\partial(\mathsf{f})_\alpha) \cap \text{动作集} \times \mathsf{Exp}\}
$$

对于每个 α，令 $\{r_i\}_{i\in I_\alpha}$ 是一个指标化集合，使得 $r_i \in [0,1]$ 对每个 $i \in I_\alpha$ 都由以下内容给出

$$
r_i = \begin{cases} \partial(\mathsf{f})_\alpha(\checkmark)\partial(\mathsf{g})_\alpha(i) & \text{if } i \in \mathsf{supp}(\partial(\mathsf{g})_\alpha) \\ \partial(\mathsf{f})_\alpha(i) & \text{if } i \in \mathsf{supp}(\partial(\mathsf{f})_\alpha) \cap (\{\mathsf{X}\} \cup \mathsf{Out}) \\ \partial(\mathsf{f})_\alpha(\mathsf{a},\mathsf{f}') & \text{if } i = (\mathsf{a},\mathsf{f}'\,;\mathsf{g}) \text{ and } (\mathsf{a},\mathsf{f}') \in \mathsf{supp}(\partial(\mathsf{f})_\alpha) \cap \mathsf{Act}\times\mathsf{Exp} \end{cases}
$$

这使我们能够写出以下内容

$$
\mathsf{f}\,;\mathsf{g} \equiv \bigplus_{\alpha\in\mathsf{At}}\left(\bigoplus_{i\in I_\alpha} r_i\cdot\mathsf{exp}(i)\right)
$$

应用 63 并对重复元素的概率求和，恰好得到所需结果

$$\mathsf{f}\,;\mathsf{g} \equiv \bigplus_{\alpha\in\mathsf{At}} \left(\bigplus_{d\in \mathsf{supp}(\partial(\mathsf{f};\mathsf{g})_\alpha)} \partial(\mathsf{f}\,;\mathsf{g})_\alpha(d)\cdot \exp(d) \right)$$

$\boxed{\mathsf{e} \equiv \mathsf{f}^{(\mathsf{b})}}$我们想要证明

$$\mathsf{f}^{(\mathsf{b})} \equiv \bigplus_{\alpha\in\mathsf{At}} \left(\bigoplus_{d\in \mathsf{supp}\left(\partial\left(\mathsf{f}^{(\mathsf{b})}\right)_\alpha\right)} \partial\left(\mathsf{f}^{(\mathsf{b})}\right)_\alpha(d)\cdot \exp(d) \right)$$

根据引理54和公理G1，我们可以将上述内容写为

$$\bigplus_{\alpha\in\mathsf{At}} \alpha\,;\mathsf{f}^{(\mathsf{b})} \equiv \bigplus_{\alpha\in\mathsf{At}} \left(\alpha\,; \left(\bigoplus_{d\in \mathsf{supp}\left(\partial\left(\mathsf{f}^{(\mathsf{b})}\right)_\alpha\right)} \partial\left(\mathsf{f}^{(\mathsf{b})}\right)_\alpha(d)\cdot \exp(d) \right) \right)$$

因此，只需证明对于所有 $\alpha \in$原子，我们都有

$$\alpha\,;\mathsf{f}^{(\mathsf{b})} \equiv \alpha\,; \left(\bigoplus_{d\in \mathsf{supp}\left(\partial\left(\mathsf{f}^{(\mathsf{b})}\right)_\alpha\right)} \partial\left(\mathsf{f}^{(\mathsf{b})}\right)_\alpha(d)\cdot \exp(d) \right)$$

¯首先，考虑 $\gamma \leq_{\mathsf{BA}} \mathsf{b}$。我们有

$$\begin{aligned}
\gamma\,;\mathsf{f}^{(\mathsf{b})} &\equiv \gamma\,; \left(\mathsf{f}\,;\mathsf{f}^{(\mathsf{b})} +_{\mathsf{b}} 1\right) && \text{(L1)}\\
&\equiv \left(\mathsf{f}\,;\mathsf{f}^{(\mathsf{b})} +_{\mathsf{b}} 1\right) +_\gamma 1 && \text{(DF2)}\\
&\equiv \mathsf{f}\,;\mathsf{f}^{(\mathsf{b})} +_{\gamma\mathsf{b}} (1 +_\gamma 0) && \text{(G4)}\\
&\equiv \mathsf{f}\,;\mathsf{f}^{(\mathsf{b})} +_0 (1 +_\gamma 0) && (\gamma \leq_{\mathsf{BA}} \bar{\mathsf{b}})\\
&\equiv (1 +_\gamma 0) +_1 \mathsf{f}\,;\mathsf{f}^{(\mathsf{b})} && \text{(G3)}\\
&\equiv (1 +_\gamma 0) && \text{(DF12)}\\
&\equiv \gamma\,;1 && \text{(DF2)}\\
&\equiv \gamma\,; \left(\bigoplus_{d\in \mathsf{supp}\left(\partial\left(\mathsf{f}^{(\mathsf{b})}\right)_\gamma\right)} \partial\left(\mathsf{f}^{(\mathsf{b})}\right)_\gamma(d)\cdot \exp(d) \right) && \text{(Def. of } \partial)
\end{aligned}$$

现在，考虑 $\gamma \leq_{\mathsf{BA}} \mathsf{c}$ 使得 $\partial(\mathsf{f})\gamma(\checkmark) = 1$。根据归纳假设，我们有

$$\begin{aligned}
\mathsf{f} &\equiv \bigplus_{\alpha\in\mathsf{At}} \left(\bigoplus_{d\in \mathsf{supp}(\partial(\mathsf{f})_\alpha)} \partial(\mathsf{f})_\alpha(d)\cdot \exp(d) \right) && \text{(Ind. hypothesis)}\\
&\equiv 1 +_\gamma \bigplus_{\alpha\in\mathsf{At}\setminus\{\gamma\}} \left(\bigoplus_{d\in \mathsf{supp}(\partial(\mathsf{f})_\alpha)} \partial(\mathsf{f})_\alpha(d)\cdot \exp(d) \right)\\
&\equiv \bigplus_{\alpha\in\mathsf{At}\setminus\{\gamma\}} \left(\bigoplus_{d\in \mathsf{supp}(\partial(\mathsf{f})_\alpha)} \partial(\mathsf{f})_\alpha(d)\cdot \exp(d) \right) +_{\bar{\gamma}} 1 && \text{(G3)}
\end{aligned}$$

为简单起见，我们将上述项记作 $\mathsf{f} \equiv \mathsf{m} +_{\bar{\gamma}} 1_\circ$。现在，考虑如下内容

$$
\begin{aligned}
\gamma \,;\, \mathsf{f}^{(\mathsf{b})} &\equiv \gamma \,;\, (\mathsf{m} +_{\bar{\gamma}} 1) \\
&\equiv \gamma \,;\, (\bar{\gamma} \,;\, \mathsf{m})^{(\mathsf{b})} && \text{(L3)} \\
&\equiv \gamma \,;\, ((\bar{\gamma} \,;\, \mathsf{m}) \,;\, (\bar{\gamma} \,;\, \mathsf{m})^{(\mathsf{b})} +_{\mathsf{b}} 1) && \text{(L1)} \\
&\equiv \gamma \,;\, (\bar{\gamma} \,;\, (\mathsf{m} \,;\, (\bar{\gamma} \,;\, \mathsf{m})^{(\mathsf{b})}) +_{\mathsf{b}} 1) && \text{(S3)} \\
&\equiv \gamma \,;\, (\gamma \,;\, \bar{\gamma} \,;\, (\mathsf{m} \,;\, (\bar{\gamma} \,;\, \mathsf{m})^{(\mathsf{b})}) +_{\mathsf{b}} 1) && \text{(DF7)} \\
&\equiv \gamma \,;\, (0 \,;\, (\mathsf{m} \,;\, (\bar{\gamma} \,;\, \mathsf{m})^{(\mathsf{b})}) +_{\mathsf{b}} 1) && \text{(S8)} \\
&\equiv \gamma \,;\, (0 +_{\mathsf{b}} 1) && \text{(S4)} \\
&\equiv (0 +_{\mathsf{b}} 1) +_{\gamma} 0 && \text{(DF2)} \\
&\equiv 0 +_{\gamma \mathsf{b}} (1 +_{\gamma} 0) && \text{(G4)} \\
&\equiv 0 +_{\gamma} (1 +_{\gamma} 0) && \text{(Boolean algebra)} \\
&\equiv (1 +_{\gamma} 0) +_{\bar{\gamma}} 0 && \text{(G3)} \\
&\equiv \bar{\gamma} \,;\, (1 +_{\gamma} 0) && \text{(DF2)} \\
&\equiv \bar{\gamma} \,;\, (0 +_{\bar{\gamma}} 1) && \text{(G3)} \\
&\equiv \bar{\gamma} \,;\, 0 && \text{(DF3)} \\
&\equiv 0 +_{\bar{\gamma}} 0 && \text{(DF2)} \\
&\equiv 0 +_{\gamma} 0 && \text{(G3)} \\
&\equiv \gamma \,;\, 0 && \text{(DF2)} \\
&\equiv \gamma \,;\, \left(\bigoplus_{d \in \mathsf{supp}\left(\partial\left(\mathsf{f}^{(\mathsf{b})}\right)_\gamma\right)} \partial\left(\mathsf{f}^{(\mathsf{b})}\right)_\gamma (d) \cdot \exp(d) \right) && \text{(Def. of } \partial\text{)}
\end{aligned}
$$

最后考虑 $\gamma \leq_{\mathsf{BA}} \mathsf{b}$ 使得 $\partial(\mathsf{f})_\alpha(\checkmark) < 1_\circ$。根据归纳假设，我们有

$$
\begin{aligned}
\mathsf{f} &\equiv \bigplus_{\alpha \in \mathsf{At}} \left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\alpha)} \partial(\mathsf{f})_\alpha(d) \cdot \exp(d) \right) && \text{(Ind. hypothesis)} \\
&\equiv \left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\gamma)} \partial(\mathsf{f})_\alpha(d) \cdot \exp(d) \right) +_{\gamma} \bigplus_{\alpha \in \mathsf{At}} \left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\alpha)} \partial(\mathsf{f})_\alpha(d) \cdot \exp(d) \right) \\
&\equiv \left(1 \oplus_{\partial(\mathsf{f})_\gamma(\checkmark)} \bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\gamma)} \frac{\partial(\mathsf{f})_\alpha(d)}{1 - \partial(\mathsf{f})_\gamma(\checkmark)} \cdot \exp(d) \right) \\
&\qquad +_{\gamma} \bigplus_{\alpha \in \mathsf{At}} \left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\alpha)} \partial(\mathsf{f})_\alpha(d) \cdot \exp(d) \right) \\
&\equiv \left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\gamma)} \frac{\partial(\mathsf{f})_\alpha(d)}{1 - \partial(\mathsf{f})_\gamma(\checkmark)} \cdot \exp(d) \oplus_{1 - \partial(\mathsf{f})_\gamma(\checkmark)} 1 \right) \\
&\qquad +_{\gamma} \bigplus_{\alpha \in \mathsf{At}} \left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\alpha)} \partial(\mathsf{f})_\alpha(d) \cdot \exp(d) \right) && \text{(P3)}
\end{aligned}
$$

我们可以使用公理 L5，得到如下结果

$$
\begin{aligned}
\gamma ; \mathsf{f}^{(\mathsf{b})} &\equiv \gamma ; \left(\left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\gamma)} \frac{\partial(\mathsf{f})_\alpha(d)}{1 - \partial(\mathsf{f})_\gamma(\checkmark)} \cdot \mathsf{exp}(d) \right) ; \mathsf{f}^{(\mathsf{b})} +_{\mathsf{b}} 1 \right) \\
&\equiv \gamma ; \left(\left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\gamma)} \frac{\partial(\mathsf{f})_\alpha(d)}{1 - \partial(\mathsf{f})_\gamma(\checkmark)} \cdot \mathsf{exp}(d) ; \mathsf{f}^{(\mathsf{b})} \right) +_{\mathsf{b}} 1 \right) && \text{(Lemma 61)} \\
&\equiv \left(\left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\gamma)} \frac{\partial(\mathsf{f})_\alpha(d)}{1 - \partial(\mathsf{f})_\gamma(\checkmark)} \cdot \mathsf{exp}(d) ; \mathsf{f}^{(\mathsf{b})} \right) +_{\mathsf{b}} 1 \right) +_\gamma 0 && \text{(DF2)} \\
&\equiv \left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\gamma)} \frac{\partial(\mathsf{f})_\alpha(d)}{1 - \partial(\mathsf{f})_\gamma(\checkmark)} \cdot \mathsf{exp}(d) ; \mathsf{f}^{(\mathsf{b})} \right) +_{\gamma\mathsf{b}} (1 +_\gamma 0) && \text{(G4)} \\
&\equiv \left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\gamma)} \frac{\partial(\mathsf{f})_\alpha(d)}{1 - \partial(\mathsf{f})_\gamma(\checkmark)} \cdot \mathsf{exp}(d) ; \mathsf{f}^{(\mathsf{b})} \right) +_\gamma (1 +_\gamma 0) && \text{（布尔代数）} \\
&\equiv (0 +_{\bar\gamma} 1) +_{\bar\gamma} \left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\gamma)} \frac{\partial(\mathsf{f})_\alpha(d)}{1 - \partial(\mathsf{f})_\gamma(\checkmark)} \cdot \mathsf{exp}(d) ; \mathsf{f}^{(\mathsf{b})} \right) && \text{(G3)} \\
&\equiv \bar\gamma ; (0 +_{\bar\gamma} 1) +_{\bar\gamma} \left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\gamma)} \frac{\partial(\mathsf{f})_\alpha(d)}{1 - \partial(\mathsf{f})_\gamma(\checkmark)} \cdot \mathsf{exp}(d) ; \mathsf{f}^{(\mathsf{b})} \right) && \text{(G2)} \\
&\equiv \bar\gamma ; 0 +_{\bar\gamma} \left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\gamma)} \frac{\partial(\mathsf{f})_\alpha(d)}{1 - \partial(\mathsf{f})_\gamma(\checkmark)} \cdot \mathsf{exp}(d) ; \mathsf{f}^{(\mathsf{b})} \right) && \text{(DF3)} \\
&\equiv (0 +_{\bar\gamma} 0) +_{\bar\gamma} \left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\gamma)} \frac{\partial(\mathsf{f})_\alpha(d)}{1 - \partial(\mathsf{f})_\gamma(\checkmark)} \cdot \mathsf{exp}(d) ; \mathsf{f}^{(\mathsf{b})} \right) && \text{(DF2)} \\
&\equiv 0 +_{\bar\gamma} \left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\gamma)} \frac{\partial(\mathsf{f})_\alpha(d)}{1 - \partial(\mathsf{f})_\gamma(\checkmark)} \cdot \mathsf{exp}(d) ; \mathsf{f}^{(\mathsf{b})} \right) && \text{(G1)} \\
&\equiv \left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\gamma)} \frac{\partial(\mathsf{f})_\alpha(d)}{1 - \partial(\mathsf{f})_\gamma(\checkmark)} \cdot \mathsf{exp}(d) ; \mathsf{f}^{(\mathsf{b})} \right) +_\gamma 0 && \text{(G3)} \\
&\equiv \gamma ; \left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\gamma)} \frac{\partial(\mathsf{f})_\alpha(d)}{1 - \partial(\mathsf{f})_\gamma(\checkmark)} \cdot \mathsf{exp}(d) ; \mathsf{f}^{(\mathsf{b})} \right) && \text{(DF2)}
\end{aligned}
$$

我们可以展开广义凸和，得到以下结果

$$
\begin{aligned}
\gamma ; \Bigg(& \bigoplus_{d \in \mathsf{Out} \cup \{X\}} \frac{\partial(\mathsf{f})_\alpha(d)}{1 - \partial(\mathsf{f})_\gamma(\checkmark)} \cdot \mathsf{exp}(d) ; \mathsf{f}^{(\mathsf{b})} \\
& \oplus \bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\alpha) \cap \mathsf{Act} \times \mathsf{Exp}} \frac{\partial(\mathsf{f})_\alpha(d)}{1 - \partial(\mathsf{f})_\gamma(\checkmark)} \cdot \mathsf{exp}(d) ; \mathsf{f}^{(\mathsf{b})} \Bigg)
\end{aligned}
$$

现在，我们可以使用公理 S4 和 S7，得到

$$\gamma\,;\left(\bigoplus_{d\in \mathsf{Out}\cup\{X\}}\frac{\partial(\mathsf{f})_\alpha(d)}{1-\partial(\mathsf{f})_\gamma(\checkmark)}\cdot \exp(d)\ \oplus\bigoplus_{\substack{d\in \mathsf{supp}(\partial(\mathsf{f})_\alpha)\\ \cap \mathsf{Act}\times\mathsf{Exp}}}\frac{\partial(\mathsf{f})_\alpha(d)}{1-\partial(\mathsf{f})_\gamma(\checkmark)}\cdot \exp(d)\,;\mathsf{f}^{(\mathsf{b})}\right)$$

这恰好与.....相同

$$\gamma\,;\left(\bigoplus_{d\in \mathsf{supp}\left(\partial\left(\mathsf{f}^{(\mathsf{b})}\right)_\gamma\right)}\partial\left(\mathsf{f}^{(\mathsf{b})}\right)_\gamma(d)\cdot\exp(d)\right)$$

$\mathsf{e}\equiv\mathsf{f}^{[r]}$ 首先，注意我们可以安全地假设 $r<1_\circ$ 如果 $r=1$，那么我们可以使用公理 L4 得到 $\mathsf{f}^{[1]}\equiv\mathsf{f}^{(1)}$，并将其视为守卫循环。与上述情况类似，我们证明对于所有 $\alpha\in$原子，都有

$$\alpha\,;\mathsf{f}^{[r]}\equiv\alpha\,;q\left(\bigoplus_{d\in \mathsf{supp}\left(\partial\left(\mathsf{f}^{[r]}\right)_\alpha\right)}\partial\left(\mathsf{f}^{[r]}\right)_\alpha(d)\cdot\exp(d)\right)$$

现在，考虑 $\gamma\in$原子，使得 $\partial(\mathsf{f})\gamma(\checkmark)=1_\circ$ 在这种情况下，我们有

$$\begin{aligned}
\mathsf{f}&\equiv\bigdotplus_{\alpha\in\mathsf{At}}\left(\bigoplus_{d\in\mathsf{supp}(\partial(\mathsf{f})_\alpha)}\partial(\mathsf{f})_\alpha(d)\cdot\exp(d)\right) && \text{(Ind. hypothesis)}\\
&\equiv 1+_\gamma\bigdotplus_{\alpha\in\mathsf{At}\setminus\{\gamma\}}\left(\bigoplus_{d\in\mathsf{supp}(\partial(\mathsf{f})_\alpha)}\partial(\mathsf{f})_\alpha(d)\cdot\exp(d)\right)\\
&\equiv(1\oplus_1 0)+_\gamma\bigdotplus_{\alpha\in\mathsf{At}\setminus\{\gamma\}}\left(\bigoplus_{d\in\mathsf{supp}(\partial(\mathsf{f})_\alpha)}\partial(\mathsf{f})_\alpha(d)\cdot\exp(d)\right) && \text{(P2)}\\
&\equiv(0\oplus_o 1)+_\gamma\bigdotplus_{\alpha\in\mathsf{At}\setminus\{\gamma\}}\left(\bigoplus_{d\in\mathsf{supp}(\partial(\mathsf{f})_\alpha)}\partial(\mathsf{f})_\alpha(d)\cdot\exp(d)\right) && \text{(P3)}
\end{aligned}$$

现在，我们可以应用公理 L6，得到如下结果

$$\begin{aligned}
\gamma\,;\mathsf{f}^{[r]}&\equiv\gamma\,;(0\,;\mathsf{f}^{[r]}\oplus_0 1)\\
&\equiv\gamma\,;(1\oplus_1 0\,;\mathsf{f}^{[r]}) && \text{(P3)}\\
&\equiv\gamma\,;1 && \text{(P2)}\\
&\equiv\gamma\,;\left(\bigoplus_{d\in\mathsf{supp}\left(\partial\left(\mathsf{f}^{[r]}\right)_\gamma\right)}\partial\left(\mathsf{f}^{[r]}\right)_\gamma(d)\cdot\exp(d)\right) && \text{(Def. of }\partial\text{)}
\end{aligned}$$

现在，考虑 $\gamma\in$原子，其满足 $\partial(\mathsf{f})\gamma(\checkmark)<1_\circ$

$$\mathsf{f}\equiv\bigdotplus_{\alpha\in\mathsf{At}}\left(\bigoplus_{d\in\mathsf{supp}(\partial(\mathsf{f})_\alpha)}\partial(\mathsf{f})_\alpha(d)\cdot\exp(d)\right)\qquad\text{(Induction hypothesis)}$$

$$
\begin{aligned}
&\equiv \left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\gamma)} \partial(\mathsf{f})_\gamma(d) \cdot \exp(d) \right) \\
&\qquad +_\gamma \left(\bigdot_{\alpha \in \mathsf{At} \setminus \{\gamma\}} \left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\alpha)} \partial(\mathsf{f})_\alpha(d) \cdot \exp(d) \right) \right) \\
&\equiv \left(1 \oplus_{1-\partial(\mathsf{f})_\gamma(\checkmark)} \left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\gamma) \setminus \{\checkmark\}} \frac{\partial(\mathsf{f})_\gamma(d)}{1-\partial(\mathsf{f})_\gamma(\checkmark)} \cdot \exp(d) \right) \right) \\
&\qquad +_\gamma \left(\bigdot_{\alpha \in \mathsf{At} \setminus \{\gamma\}} \left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\alpha)} \partial(\mathsf{f})_\alpha(d) \cdot \exp(d) \right) \right) \\
&\equiv \left(\left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\gamma) \setminus \{\checkmark\}} \frac{\partial(\mathsf{f})_\gamma(d)}{1-\partial(\mathsf{f})_\gamma(\checkmark)} \cdot \exp(d) \right) \oplus_{1-\partial(\mathsf{f})_\gamma(\checkmark)} 1 \right) \\
&\qquad +_\gamma \left(\bigdot_{\alpha \in \mathsf{At} \setminus \{\gamma\}} \left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\alpha)} \partial(\mathsf{f})_\alpha(d) \cdot \exp(d) \right) \right) \qquad \text{(P3)}
\end{aligned}
$$

现在我们可以应用 L5，得到如下结果

$$
\begin{aligned}
\gamma ; \mathsf{f}^{[r]} &\equiv \gamma ; \left(\left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\gamma) \setminus \{\checkmark\}} \frac{\partial(\mathsf{f})_\gamma(d)}{1-\partial(\mathsf{f})_\gamma(\checkmark)} \cdot \exp(d) \right) ; \mathsf{f}^{[r]} \oplus_{\frac{r(1-\partial(\mathsf{f})_\gamma(\checkmark))}{1-r\partial(\mathsf{f})_\gamma(\checkmark)}} 1 \right) \\
&\equiv \gamma ; \left(\left(\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\gamma) \setminus \{\checkmark\}} \frac{\partial(\mathsf{f})_\gamma(d)}{1-\partial(\mathsf{f})_\gamma(\checkmark)} \cdot \exp(d) ; \mathsf{f}^{[r]} \right) \oplus_{\frac{r(1-\partial(\mathsf{f})_\gamma(\checkmark))}{1-r\partial(\mathsf{f})_\gamma(\checkmark)}} 1 \right) \qquad \text{(Lemma 61)}
\end{aligned}
$$

我们可以展开这个凸和，并应用 S3、S4 和 S7 公理，得到如下结果

$$
\begin{aligned}
\gamma ; \Bigg(\Bigg(&\bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\gamma) \cap (\mathsf{Out} \cup \{\checkmark\})} \frac{\partial(\mathsf{f})_\gamma(d)}{1-\partial(\mathsf{f})_\gamma(\checkmark)} \cdot \exp(d) \\
&\oplus \bigoplus_{d \in \mathsf{supp}(\partial(\mathsf{f})_\gamma) \cap \mathsf{Act} \times \mathsf{Exp}} \frac{\partial(\mathsf{f})_\gamma(d)}{1-\partial(\mathsf{f})_\gamma(\checkmark)} \cdot \exp(d) ; \mathsf{f}^{[r]} \Bigg) \oplus_{\frac{r(1-\partial(\mathsf{f})_\gamma(\checkmark))}{1-r\partial(\mathsf{f})_\gamma(\checkmark)}} 1 \Bigg)
\end{aligned}
$$

我们可以将该表达式重新整理为广义凸和。令 I_γ 为按以下方式定义的指标集。

$$
I_\gamma = \{\checkmark\} + (\mathsf{supp}(\partial(\mathsf{f})_\gamma) \cap (\mathsf{Out} \cup \{\checkmark\})) + \{(\mathsf{a}, \mathsf{f}' ; \mathsf{f}^{[r]}) \mid (\mathsf{a}, \mathsf{f}') \in \mathsf{supp}(\partial(\mathsf{f})_\gamma)\}
$$

现在，令 $\{r_i\}^{i \in I_\gamma}$ 为一个指标化集合，使得 $r_i \in [0,1]$ 对每个 $i \in I_\gamma$ 都成立。我们按以下方式定义此类集合

$$
r_i = \begin{cases}
\frac{1-r}{1-\partial(\mathsf{f})_\gamma(\checkmark)} & \text{if } i = \checkmark \\
\frac{\partial(\mathsf{f})_\gamma(i)}{1-\partial(\mathsf{f})_\gamma(\checkmark)} & \text{if } i \in \mathsf{supp}(\partial(\mathsf{f})_\gamma) \cap (\mathsf{Out} \cap \{\checkmark\}) \\
\frac{\partial(\mathsf{f})_\gamma(\mathsf{a},\mathsf{f}')}{1-\partial(\mathsf{f})_\gamma(\checkmark)} & \text{if } i = (\mathsf{a}, \mathsf{f}' ; \mathsf{f}^{[r]}) \text{ and } (\mathsf{a}, \mathsf{f}') \in \mathsf{supp}(\partial(\mathsf{f})_\alpha)
\end{cases}
$$

注意，I_γ 恰好是 $\mathsf{supp}\left(\partial\left(\mathsf{f}^{[r]}\right)_\gamma\right)$，与这些元素相关联的概率

恰好与 $\partial\left(\mathsf{f}^{[r]}\right)_\gamma$ 所赋予的概率相同。因此，我们有

$$\gamma\,;\mathsf{f}^{[r]} \equiv \gamma\,;\left(\bigoplus_{d\in\mathsf{supp}\left(\partial\left(\mathsf{f}^{[r]}\right)_\gamma\right)} \partial\left(\mathsf{f}^{[r]}\right)_\gamma(d)\cdot\exp(d)\right)$$

◀

E 第 6 节的证明

为了证明定理 21，我们使用以下引理。

▶ 引理 65（[57, 命题 5.8]）。设 (X,β) 是一个 *ProbGKAT* 自动机，$R\subseteq X\times X$ 是 (X,β) 上的双模拟等价，且 $[-]_R\colon X\to X/R$ 是典范商映射。那么，存在唯一的转移映射 $\beta\colon X/R\times At\to D_\omega(2+Out+Act\times X/R)$，使得 $[-]_R$ 成为从 (X,β) 到 $(X/R,\beta)$ 的 *ProbGKAT* 自动机同态。

证明。（定理 21）。首先，回顾如下内容。设 $\partial\colon \mathtt{Exp}/{\equiv}\to \mathsf{G}(\mathtt{Exp}/{\equiv})$ 是由引理 65 给出的唯一 G-余代数结构映射，它使商映射 $[-]_\equiv\colon \mathtt{Exp}\to\mathtt{Exp}/{\equiv}$ 成为 G-余代数同态。给定函数 $h\colon X\to\mathtt{Exp}$，复合映射 $[-]_\equiv\circ h$ 是从 (X,β) 到 $(\mathtt{Exp}/{\equiv},\partial)$ 的 G-余代数同态，当且仅当下图交换

$$\begin{array}{ccc} X & \xrightarrow{[-]_\equiv\circ h} & \mathtt{Exp}/{\equiv} \\ {\scriptstyle\beta}\downarrow & & \downarrow{\scriptstyle\bar\partial} \\ \mathcal{G}X & \xrightarrow[\mathcal{G}([-]_\equiv\circ h)]{} & \mathcal{G}(\mathtt{Exp}/{\equiv}) \end{array} \qquad \bar\partial\circ[-]_\equiv\circ h = \mathcal{G}([-]_\equiv\circ h)\circ\beta \tag{1}$$

现在，由于 $[-]_\equiv$ 是余代数同态，$\partial\circ[-]_\equiv = G[-]_\equiv\circ\partial$。这告诉我们，(1) 等价于

$$\mathcal{G}[-]_\equiv\circ\partial\circ h = \mathcal{G}([-]_\equiv\circ h)\circ\beta$$

我们可以用更具体的方式展开上述方程：对于所有 $x\in X$ 和 $\alpha\in$原子，1. $\beta(x)_\alpha(o) = \partial(h(x))_\alpha(o)$，其中 $o\in 2+$ 可以是任意输出；以及 2. 对于任意 $(\mathsf{a},[\mathsf{e}'])\in$ 动作集 $\times\,\mathtt{Exp}/{\equiv}$，

$$\sum_{h(x')\equiv\mathsf{e}'}\beta(x)_\alpha(\mathsf{a},x') = \sum_{\mathsf{f}\equiv\mathsf{e}'}\partial(h(x))_\alpha(\mathsf{a},\mathsf{f})$$

从右向左，假设 $[-]_\equiv\circ h$ 是同态。令 (X,τ) 为与 (X,β) 相关联的 Salomaa 系统，并令 $h^\#$ 为 h 在 $\mathtt{Exp}(X)$ 中表达式上的唯一扩展。我们要证明，对于所有 $x\in X$，$h(x)\equiv(h^\#\circ\tau)(x)$。由定理 14 可知，对于所有 $x\in X$，

$$h(x)\equiv\bigdotplus_{\alpha\in\mathsf{At}}\left(\bigoplus_{d\in\mathsf{supp}(\partial(h(x))_\alpha)}\partial(h)_\alpha(d)\cdot\exp(d)\right)$$

我们可以展开凸和，并使用引理 64 将支撑集中模 $\equiv$ 等价的元素归为一组。对于所有 $x\in X$，我们得到以下结果

$$h(x)\equiv\bigdotplus_{\alpha\in\mathsf{At}}\left(\bigoplus_{d\in 2+\mathsf{Out}}\partial(h(x))_\alpha(d)\cdot d\oplus\bigoplus_{(a,[\mathsf{e}']_\equiv)\in E_\alpha}\left(\sum_{\mathsf{f}\equiv\mathsf{e}'}\partial(h(x))_\alpha(\mathsf{a},\mathsf{f})\right)\cdot\mathsf{a}\,;\mathsf{e}'\right) \tag{2}$$

其中，对于每个 $\alpha \in$ 原子，我们有

$$E_\alpha = \{(\mathsf{a}, Q) \in \mathsf{Act} \times \mathtt{Exp}/{\equiv} \mid \mathsf{e}' \in Q, \partial(h(x))_\alpha(\mathsf{a}, \mathsf{e}') > 0\}$$

同样，对于所有 $x \in X$，方程右侧可写为如下形式。

$$(h^\# \circ \tau)(x) \equiv \bigplus_{\alpha \in \mathsf{At}} \left(\bigoplus_{d \in 2+\mathsf{Out}} \beta(x)_\alpha(d) \cdot d \oplus \bigoplus_{(\mathsf{a},\mathsf{f}) \in \mathsf{supp}(\beta(x)_\alpha)} \beta(x)_\alpha(\mathsf{a}, f) \cdot \mathsf{a} \,;\, h(f) \right)$$

我们使用引理 64 将支撑集中模 $\equiv$ 等价的元素归为一组，并对它们各自对应的概率求和。

$$(h^\# \circ \tau)(x) \equiv \bigplus_{\alpha \in \mathsf{At}} \left(\bigoplus_{d \in 2+\mathsf{Out}} \beta(x)_\alpha(d) \cdot d \oplus \bigoplus_{(\mathsf{a}, [\mathsf{e}']_\equiv) \in F_\alpha} \left(\sum_{h(x') \equiv \mathsf{e}'} \beta(x)_\alpha(\mathsf{a}, x') \right) \cdot \mathsf{a} \,;\, \mathsf{e}' \right) \quad (3)$$

其中，对于每个 $\alpha \in$原子，我们定义

$$F_\alpha = \{(\mathsf{a}, Q) \in \mathsf{Act} \times \mathtt{Exp}/{\equiv} \mid h(x') \in Q, \beta(x)_\alpha(\mathsf{a}, x') > 0\}$$

我们证明，对于每个 $x \in X$，式 (2) 和式 (3) 中的表达式完全相同。为此，我们将论证，对于每个原子 $\alpha \in$At，广义凸和的指标集相同，并且两个指标集中元素的等价类所对应的概率也相同。

固定任意的 $\alpha \in$ 原子。给定 $d \in 2 +$ 输出，若 $d \in \mathsf{supp}(\partial(h(x)))_\alpha$，则根据满足同态条件 (1) 的性质，有 $d \in \mathsf{supp}(\beta(x)\alpha)$。反向结论可通过对称论证得到。此外，对于所有此类 d，我们有 $\partial(h(x))_\alpha(d) = \beta(x)\alpha(d)$。

现在考虑 (a Q) $\in$动作集 $\times \mathtt{Exp}/{\equiv}$。若 $(a, Q) \in E_\alpha$，则存在某个 $\mathsf{e}' \in \mathtt{Exp}$，使得 $\partial(h(x))_\alpha$(a,e′) > 0。根据同态条件 (2)，存在某个 $x' \in X$ 满足 $h(x') \equiv \mathsf{e}'$ 且 $\beta(x)_\alpha$(a x') > 0，因此 (a Q) $\in F_\alpha$。反向可通过对称论证得出，因此 $E_\alpha = F_\alpha$。注意，由于条件 (2)，与每个 (a Q) $\in$ 动作集 $\times \mathtt{Exp}/{\equiv}$ 相关联的概率都相同。

由于两个表达式中的所有广义凸和都将相同的概率赋给相同的元素，我们得到 $h(x) \equiv (h^\# \circ \tau)(x)$，对所有 $x \in X$ 均如此，证毕。

从左到右，假设 h 是一个在 $\equiv$ 以内的解。我们先证明 $(\partial \circ h^\# \circ \tau)(x) = (\mathcal{G}(h) \circ \beta)(x)$ 对所有 $x \in X$ 均成立。回想一下，对所有 $x \in X$，

$$(h^\# \circ \tau)(x) \equiv \bigplus_{\alpha \in \mathsf{At}} \left(\bigoplus_{d \in 2+\mathsf{Out}} \beta(x)_\alpha(d) \cdot d \oplus \bigoplus_{(\mathsf{a}, f) \in \mathsf{supp}(\beta(x)_\alpha)} \beta(x)_\alpha(\mathsf{a}, f) \cdot \mathsf{a} \,;\, h(f) \right)$$

将转移映射应用于该表达式，对于所有 $\alpha \in$原子，可分为两种情况。

1. 对于 $o \in 2 +$ 输出，$(\partial \circ h^\# \circ \tau)(x)(o) = \beta(x)_\alpha(o) = (\mathsf{G}(h) \circ \beta)(x)_\alpha(o)$ 2. 对于所有 (a, e′) $\in$ 动作集 $\times \mathtt{Exp}$,

$$(\partial \circ h^\# \circ \tau)(x)(\mathsf{a}, \mathsf{e}') = \sum_{h(x') = \mathsf{e}'} \beta(x)_\alpha(\mathsf{a}, x') = (\mathcal{G}(h) \circ \beta)(x)_\alpha(\mathsf{a}, \mathsf{e}')$$

由此证明 $(\partial \circ h^\# \circ \tau) = (\mathcal{G}(h) \circ \beta)$。现在在两边后复合 $G[-]_\equiv$，并考虑以下

$$\begin{aligned}
&\mathcal{G}[-]_\equiv \circ \partial \circ h^\# \circ \tau = \mathcal{G}[-]_\equiv \circ \mathcal{G}(h) \circ \beta \\
&\mathcal{G}[-]_\equiv \circ \partial \circ h^\# \circ \tau = \mathcal{G}([-]_\equiv \circ h) \circ \beta && (\mathcal{G} \text{ is a functor}) \\
&\bar{\partial} \circ [-]_\equiv \circ h^\# \circ \tau = \mathcal{G}([-]_\equiv \circ h) \circ \beta && ([-]_\equiv \text{ 是同态}) \\
&\bar{\partial} \circ [-]_\equiv \circ h = \mathcal{G}([-]_\equiv \circ h) \circ \beta && (h \equiv h^\# \circ \tau)
\end{aligned}$$

因此， $[-]_{\equiv} \circ h$ 是从 (X, β) 到 $(\mathsf{Exp}/\equiv, \partial)$ 的 $\mathcal{G}$-余代数同态，证毕 .

◀

▶ **引理 23.** 对于每个 ProbGKAT 自动机，(X, β)是一个(X, d_X) 超度量伪度量空间，即对于所有 $x, y, z \in X$，都有 $d_X(x, z) = \max\{d_X(x, y)\ d_X(y, z)\}$。

证明。 $d(x, x) = 0$ 立即成立，因为 (X, β) 上的最大双模拟是一个等价关系，因此对于所有 $x \in X$，我们有 $x \sim x$。

为证明对称性，假设对于某个 $k \in \mathbb{R}^+$， $d(x, y) = k$ 。如果 $k = 0$ ，那么 $x \sim_\beta y$；但由于 (X, β) 上的最大双模拟是一个等价关系（这是因为 G 保持弱拉回），我们有 $y \sim_\beta x$，这意味着 $d(y, x) = 0$。对于剩余情形，不失一般性，我们可以假设对于某个 $n \in \mathbb{N}$， $k = 2^{-n}$ 。在这种情况下，$x \sim_\beta^{(n)} y$；但同样根据引理 38，每个分层双模拟关系都是等价关系。因此， $y \in \sim_\beta^{(n)} x$ ，且 n 是满足 $y \in \sim_\beta^{(n)} x$ 的最大数值。由此可得， $d(y, x) = 2^{-n} = k = d(x, y)$，证毕。

对于加强的三角不等式，首先考虑 $d(x, y) = 2^{-k}$ 且 $d(y, z) = 2^{-l}$的情形。它们分别意味着 $x \in \sim_\beta^{(k)} y$和 $y \in \sim_\beta^{(l)} z$。我们有 (x, y)、$(y, z) \in \sim_\beta^{(\min(k,l))}$ 。由于所有分层双模拟关系都是等价关系，根据传递性可得 $x \in \sim_\beta^{(\min(k,l))} z$ ，且 $\min(k, l)$ 是满足 $x \in \sim_\beta^{(n)} z$的最大自然数。因此， $d(x, z) = 2^{-\min(k,l)} = \max(2^{-k}, 2^{-l}) = \max(d(x, y)\ d(y, z))$。

当 $d(x,\ y) = d(y,\ z) = 0$时，我们有 $x \sim_\beta y$和 $y \sim_\beta z$。由于最大的双模拟是一个等价关系，因此有 $x \sim_\beta z$，这意味着 $d(x,\ y) = 0 = \max(d(x,\ y)\ d(y,\ z))$。

对于下一个情形，令 $d(x,\ y) = 0$且 $d(y,\ z) = 2^{-k}$。于是 $x \sim_\beta y$且 $(y,\ z) \in \sim_\beta^{(k)}$。特别地，我们还有 $(x,\ y) \in \sim_\beta^{(k)}$ 。由传递性可得 $x \in \sim_\beta^{(k)} z$，而 k 是满足 $x \in \sim_\beta^{(k)} z$的最大数。因此， $d(x,\ z) = 2^{-k} = \max(d(x,\ y)\ d(y,\ z))$

唯一剩下的情形是对称的。 ◀

为证明引理 24，我们先证明，Salomaa 系统中的代换相对于用于定义 $(\mathsf{Exp},\ \partial)$ 上关系细化链的算子具有良好的性质。

▶ 引理 66。设 $(X, \tau\colon X \to \mathsf{Exp}(X))$ 是一个 *Salomaa* 系统，且 $R \subseteq \mathsf{Exp} \times \mathsf{Exp}$ 是一个同余关系。考虑两个映射 $m, n\colon X \to \mathsf{Exp}$ ，它们满足对所有 $x \in X$，均有 $(m(x)\ n(x)) \in R$ 。那么，对所有 $x \in X$，都有 $((m^\#\circ\ \tau)(x), (n^\#\circ\ \tau)(x)) \in \Phi_\partial(R)$。

证明。 不失一般性，我们可以假设对于所有 $x \in X$，

$$\tau(x) = \bigdash_{\alpha \in \mathsf{At}} \left(\bigoplus_{i \in I_\alpha^x} p_i \cdot \mathsf{f}_i \oplus \bigoplus_{j \in J_\alpha^x} r_j \cdot \mathsf{g}_j x_j \right)$$

对于任意 $x \in X$ 和 $\alpha \in$ 原子， I_α^x 和 J_α^x 是互不相交的指标集，使得$\{p_i\}_{i \in I_\alpha^x}$ 和 $\{r_j\}_{j \in J_\alpha^x}$ 是满足以下条件的概率带索引集合

$$\sum_{i \in I_\alpha^x} p_i + \sum_{j \in J_\alpha^x} r_j = 1$$

$\{\mathsf{f}_i\}_{i \in I_\alpha^x}$和 $\{\mathsf{g}_j\}_{j \in J_\alpha^x}$是 Exp 中元素的带索引集合。此外，由于 (X, τ) 是 Salomaa 的，我们有 $\mathsf{E}(\mathsf{g}_j) = 0$ 对所有 $j \in J_\alpha^x$ 都成立。根据引理 44，我们有$\partial(\mathsf{g}_j)_\alpha(\checkmark) = 0$ 对所有 $j \in J_\alpha^x$ 都成立。$\{x_j\}_{j \in J_\alpha^x}$ 是由不定元（ X 的元素）构成的带索引集合。

注意，对于所有 $x \in X$，

$$(m^{\#} \circ \tau)(x) = \bigdoublebarwedge_{\alpha \in \mathsf{At}} \left(\bigoplus_{i \in I_\alpha^x} p_i \cdot \mathsf{f}_i \oplus \bigoplus_{j \in J_\alpha^x} r_j \cdot \mathsf{g}_j \,;\, m(x_j) \right)$$

$$(n^{\#} \circ \tau)(x) = \bigdoublebarwedge_{\alpha \in \mathsf{At}} \left(\bigoplus_{i \in I_\alpha^x} p_i \cdot \mathsf{f}_i \oplus \bigoplus_{j \in J_\alpha^x} r_j \cdot \mathsf{g}_j \,;\, n(x_j) \right)$$

在论证的其余部分，我们使用引理 38。任取 $x \in X$ 和 $\alpha \in$原子。**1.** 对于 $o \in \{\,\} +$ 输出，我们有

$$\begin{aligned}
\partial((f^{\#} \circ m)(x))_\alpha(o) &= \sum_{i \in I_\alpha^x} p_i \partial(\mathsf{f}_i)_\alpha(o) + \sum_{j \in J_\alpha^x} r_j \partial(\mathsf{g}_j \,;\, m(x_j))_\alpha(o) \\
&= \sum_{i \in I_\alpha^x} p_i \partial(\mathsf{f}_i)_\alpha(o) + \sum_{j \in J_\alpha^x} r_j (\partial(\mathsf{g}_j)_\alpha(o) + \partial(\mathsf{g}_j)_\alpha(\checkmark) \partial(m(x_j))_\alpha(o)) \\
&= \sum_{i \in I_\alpha^x} p_i \partial(\mathsf{f}_i)_\alpha(o) + \sum_{j \in J_\alpha^x} r_j \partial(\mathsf{g}_j)_\alpha(o) && (\mathsf{E}(\mathsf{g}_j) = 0) \\
&= \sum_{i \in I_\alpha^x} p_i \partial(\mathsf{f}_i)_\alpha(o) + \sum_{j \in J_\alpha^x} r_j (\partial(\mathsf{g}_j)_\alpha(o) + \partial(\mathsf{g}_j)_\alpha(\checkmark) \partial(n(x_j))_\alpha(o)) \\
&= \partial((f^{\#} \circ n)(x))_\alpha(o)
\end{aligned}$$

现在，考虑 $o = \checkmark$ 的情形。我们有如下

$$\begin{aligned}
\partial((f^{\#} \circ m)(x))_\alpha(\checkmark) &= \sum_{i \in I_\alpha^x} p_i \partial(\mathsf{f}_i)_\alpha(\checkmark) + \sum_{j \in J_\alpha^x} r_j \partial(\mathsf{g}_j \,;\, m(x_j))_\alpha(\checkmark) \\
&= \sum_{i \in I_\alpha^x} p_i \partial(\mathsf{f}_i)_\alpha(o) + \sum_{j \in J_\alpha^x} r_j \partial(\mathsf{g}_j)_\alpha(\checkmark) \partial(m(x_j))_\alpha(\checkmark) \\
&= \sum_{i \in I_\alpha^x} p_i \partial(\mathsf{f}_i)_\alpha(o) && (\mathsf{E}(\mathsf{g}_j) = 0) \\
&= \sum_{i \in I_\alpha^x} p_i \partial(\mathsf{f}_i)_\alpha(o) + \sum_{j \in J_\alpha^x} r_j \partial(\mathsf{g}_j)_\alpha(\checkmark) \partial(n(x_j))_\alpha(\checkmark) \\
&= \partial((f^{\#} \circ n)(x))_\alpha(\checkmark)
\end{aligned}$$

2. 设 $(\mathsf{a}\ Q) \in$ 动作集 $\times\, \mathtt{Exp}/R$。我们有

$$\begin{aligned}
&\partial((f^{\#} \circ m)(x))_\alpha[\{\mathsf{a}\} \times Q] \\
&= \sum_{i \in I_\alpha^x} p_i \partial(\mathsf{f}_i)_\alpha[\{\mathsf{a}\} \times Q] + \sum_{j \in J_\alpha^x} r_j \partial(\mathsf{g}_j \,;\, m(x_j))_\alpha[\{\mathsf{a}\} \times Q] \\
&= \sum_{i \in I_\alpha^x} p_i \partial(\mathsf{f}_i)_\alpha[\{\mathsf{a}\} \times Q] \\
&\qquad + \sum_{j \in J_\alpha^x} r_j \left(\partial(\mathsf{g}_j)_\alpha[\{\mathsf{a}\} \times Q/m(x_j)] + \partial(\mathsf{g}_j)_\alpha(\checkmark) \partial(m(x_j))_\alpha[\{\mathsf{a}\} \times Q] \right) \\
&= \sum_{i \in I_\alpha^x} p_i \partial(\mathsf{f}_i)_\alpha[\{\mathsf{a}\} \times Q] + \sum_{j \in J_\alpha^x} r_j \partial(\mathsf{g}_j)_\alpha[\{\mathsf{a}\} \times Q/m(x_j)] && (\mathsf{E}(\mathsf{g}_j) = 0) \\
&= \sum_{i \in I_\alpha^x} p_i \partial(\mathsf{f}_i)_\alpha[\{\mathsf{a}\} \times Q] + \sum_{j \in J_\alpha^x} r_j \partial(\mathsf{g}_j)_\alpha[\{\mathsf{a}\} \times Q/n(x_j)] && (\text{Lemma 45})
\end{aligned}$$

$$= \sum_{i \in I_\alpha^x} p_i \partial(\mathsf{f}_i)_\alpha[\{\mathsf{a}\} \times Q]$$
$$+ \sum_{j \in J_\alpha^x} r_j \left(\partial(\mathsf{g}_j)_\alpha[\{\mathsf{a}\} \times Q/m(x_j)] + \partial(\mathsf{g}_j)_\alpha(\checkmark)\partial(n(x_j))_\alpha[\{\mathsf{a}\} \times Q]\right)$$
$$= \partial((f^\# \circ n)(x))_\alpha[\{\mathsf{a}\} \times Q] \quad \blacktriangleleft$$

▶ **引理 24**。 给定一个 *Salomaa* 系统 $(X, \tau\colon\ X \to \mathtt{Exp}(X))$，映射 $\bar{\tau}\colon \mathtt{Exp}^n \to \mathtt{Exp}^n$从伪度量空间 $(\mathtt{Exp}^n, d)$ 到其自身是 $\frac{1}{2}$-利普希茨的。

证明。 注意，关系细化链中的所有元素都是同余关系。因此，我们可以使用引理 66。回想一下，给定 $e, f \in \mathtt{Exp}^n$，使得 $e = (\mathsf{e}_1, \ldots, \mathsf{e}_n)$ 和$f = (\mathsf{f}_1, \ldots, \mathsf{f}_n)$，我们有

$$d((\mathsf{e}_1, \ldots, \mathsf{e}_n), (\mathsf{f}_1, \ldots, \mathsf{f}_n)) = \max\{d(\mathsf{e}_1, \mathsf{f}_1), \ldots, d(\mathsf{e}_n, \mathsf{f}_n)\}$$

和之前一样，我们稍微滥用一下记号，也将 $e, f\colon X \to \mathtt{Exp}$ 用于表示函数 $e(x_k) = \mathsf{e}_k$，并将 $f(x_k) = \mathsf{f}_k$ 用于表示 $1 \le k \le n$。

假设对于某个 $m \in \mathbb{N}$，有 $d((\mathsf{e}1, \ldots, \mathsf{e}_n), (\mathsf{f}1, \ldots, \mathsf{f}_n)) \le 2^{-m}$。根据积度量的定义，$2^{-m} \ge \max\{d(\mathsf{e}_1, \mathsf{f}1) \ldots, d(\mathsf{e}_n, \mathsf{f}_n)\}$，因此对于 $1 \le i \le n$，有 $\mathsf{e}_i \sim_\partial^{(m)} \mathsf{f}_i$。根据引理 66，对于所有 $1 \le i \le n$，有 $((e^\# \circ \tau)(x_i), (f^\# \circ \tau)(x_i)) \in \Phi_\partial\left(\sim_\partial^{(m)}\right) = \sim_\partial^{(m+1)}$。因此，对于所有 $1 \le i \le n$，有 $d((e \circ \tau)(x_i), (f \circ \tau)(x_i)) \le 2^{-(m+1)}$。由此可得

$$d(\bar{\tau}(\mathsf{e}_1, \ldots, \mathsf{e}_n), \bar{\tau}(\mathsf{f}_1, \ldots, \mathsf{f}_n)) \le 2^{-(m+1)} = \frac{1}{2}\left(\frac{1}{2^m}\right)$$

由此可得，$\bar{\tau}$ 是 $\frac{1}{2}$-利普希茨的。 $\blacktriangleleft$