arXiv:2512.21596v1 [cs.PL] 25 Dec 2025

概率编程中 ω-正则性质的定量验证

Peixin Wang[1], Jianhao Bai[1], Min Zhang[1], 和 C.-H. Luke Ong[2]

[1] 中国华东师范大学[2] 新加坡南洋理工大学

摘要。 概率编程提供了一种高级框架，可将统计模型表示为内置随机性和条件化机制的可执行程序。然而，现有推断技术通常只计算固定时间点（最常见的是终止时）的程序状态后验分布，因此无法捕捉概率行为随时间的演变。我们提出时序后验推断 （TPI），这是一种将概率编程与时序逻辑相结合的新框架，通过计算满足 ω-正则规约的执行轨迹上的后验分布，并以（可能具有时序性的）观测为条件，实现这一目标。为获得严谨的定量保证，我们开发了一种新方法，用于计算 ω-正则性质满足概率的上界和下界。我们的方法将 Rabin 接受条件分解为持久性和重复性部分，并构造随机屏障证书，对每个部分进行可靠界定。我们在原型工具 TPInfer 中实现了该方法，并在一组基准测试上进行评估，结果表明，该方法能够对概率模型中的丰富时序性质进行有效且高效的推断。

1 引言

概率编程（PP）通过将随机变量和概率选择直接嵌入程序代码，为描述随机模型提供了一种高级方法 [17,16]。给定观测后，PP 系统会自动应用贝叶斯定理，计算后验分布 [19,5], ，从而为推理潜在不确定性提供了严谨的机制。这使概率编程特别适用于现代人工智能系统；这类系统必须在噪声数据、随机动态和不完全信息下运行 [15]。

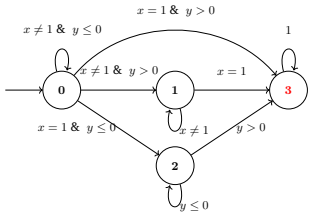
然而，概率编程中的标准后验推断（SPI）通常侧重于固定时间点的程序状态分布，尤其是程序终止时的状态分布 [30]。这隐含地假设概率程序几乎必然终止（AST） [6]，但这一假设可能并不成立 [12] ，而且无法捕捉程序执行过程中概率行为随时间演变的过程。为说明这一局限性，我们在下文给出一个简单示例。

示例 *1*。 考虑图 1 中的一个简单概率程序，其中 x 以随机方式在 0、1 之间切换其值，而 y 对 $x = 1$所在步骤进行计数。

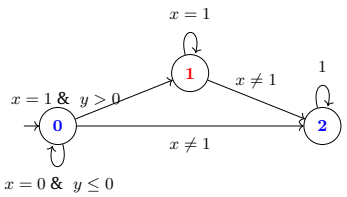
后验概率 $\Pr(x = 1 \mid y > 0)$ 表示在观测到 $y > 0$ 的条件下，x 在终止时等于 1 的概率。

$x \sim$ 伯努利分布(0.3); $y := 0$;
当 伯努利分布(0.5) **执行**
  若概率(0.6)**则**
    $x := 1 - x$
  若 $x = 1$ **则**
    $y := y + 1$
done

(a) 一个简单的概率程序



(b) 最终($x = 1$) & 最终($y > 0$)



(c) 全局($x = 1$) & 最终($y > 0$)

图 1：运行示例

在示例 1 中，这一局限性变得十分明显：我们关注的不仅是 x的最终值，还关注在最终观测到 $y > 0$的条件下，x 在整个执行过程中始终保持等于 1 的概率。这一时间要求由线性时序逻辑（LTL） [24]中的“总是”运算符 $\mathbf{G}$ 和“最终”运算符 $\mathbf{F}$刻画，从而得到后验概率 $\Pr(\mathbf{G}\, x = 1 \mid \mathbf{F} y > 0)$。[3] 事实上，后验概率 $\Pr(x = 1 \mid y > 0)$ 在 LTL 下等价于 $\Pr(\mathbf{F}\, x = 1 \mid \mathbf{F} y > 0)$，因此会产生不同的自动机。此外，概率系统中的许多重要性质，例如安全性（“坏事永远不会发生”）和活性（“好事最终会发生”），取决于程序状态如何随时间演化，而不是取决于单个终止状态，因此时序推理不可或缺 [2]。

研究动机。这一局限揭示了 SPI 与时序推理之间的差距。SPI 以变量为中心，侧重于终止状态；而时序推理以轨迹为中心，关注完整的执行过程。单靠其中任何一种，都无法表达关于时序行为的条件推理，也无法表达随时间展开的证据。为弥合这一差距，我们引入时序后验推断 (TPI)，用于计算满足 ω-正则规约 [29], 的执行轨迹的后验概率，并以（可能具有时序性质的）观测为条件。这将概率推断与时序推理统一起来，并支持对时序性质进行基于似然的分析。

[3] 这里我们假设程序终止时存在一个自环，因此可以得到能够用线性时序逻辑描述的无限轨迹。

TPI。给定 ω-正则性质 φ 和 ψ，**目标是计算**Pr($\varphi \mid \psi$)，即轨迹满足 φ 且以满足 ψ为条件的概率。

挑战。 TPI 面临两个主要挑战。(i) 它需要对完整的概率执行轨迹进行推理，而非孤立的状态；这类轨迹可能无界、分支繁多，并呈现长程时间依赖，因此其分布难以分析。以往的研究主要关注终止性 [6,9,13], 或敏感性等非时序性质 [3,33], 期望 [23,34,4], 等。(ii) 对于随机模型，计算 ω-正则性质的满足概率定量界本质上十分复杂：这些性质编码了无限时域持久性和重现条件，而对时间观测进行条件化会引入全局约束，大幅增加可接受轨迹结构的复杂性。 [7] 关注定性持久性和重现性。尽管 [1,18] 研究定量时序验证，但它们并未考虑用于时序推理的后验推断。近期一项工作 [36]提出了一个用于定量时序推断的余代数框架，但不支持自动计算。

我们的方法。 为应对这些挑战，我们采用自动机理论方法，以跟踪概率程序可能无限延展的时间演化。具体而言，我们将时序规范转换为确定性 Rabin 自动机（DRA） [29]„ 以结构化的方式推理无限执行轨迹，并识别与验证相关的时间模式。基于此，我们旨在计算观测条件化下 ω-正则性质满足概率的定量界。为使这一过程可处理，我们将 Rabin 接受条件分解为两个基本组成部分——持久性 和重复性——分别对应最终稳定或无限次发生的事件。对于每个组成部分，我们都构造了新的随机屏障证书 [26], 为满足这些时间模式的概率给出可靠的上界和下界。通过结合持久性和重复性的界，我们获得完整 ω-正则规范的定量保证，从而能够对具有随机动态的系统中的时间行为进行严格的概率推理。

贡献。 本文作出了以下贡献：

1. 我们提出了一种新的框架——时序后验推断，通过计算满足 ω-正则性质的执行轨迹上的后验分布，将概率推断与时序逻辑推理统一起来。2. 我们通过将 Rabin 接受条件分解为持久性和重复性两个组成部分，为 TPI 构建了自动机理论基础，从而能够系统地跟踪概率程序可能无限延续的时序演化。3. 我们为持久性和重复性组成部分提供了定量分析方法，并设计了相应的新型随机屏障证书，为它们的满足概率给出可靠的上界和下界。

4. 我们将该方法实现为原型工具 TPInfer，并在一套基准测试上进行评估，展示了其在随机系统中对时序性质进行定量推理的实用性和有效性。

所有省略的证明均放在附录中。

2 预备知识与概率编程

2.1 线性时序逻辑与ω-正则性质

线性时序逻辑（LTL） [24] 使用时序算子描述系统行为沿线性时间执行的演化方式。

LTL 的语法。设AP 为一个有限的原子命题集。无限轨迹上的 LTL 公式由以下文法定义：

$$\varphi ::= \top \mid a \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid \mathbf{X}\varphi \mid \varphi_1 \ \mathbf{U} \ \varphi_2$$

其中， $a \in AP$ 是一个原子命题，$\mathbf{X}$ 是“下一步”算子，$\mathbf{U}$ 是“直到”算子。其他标准时序算子均被定义为语法糖，例如$\mathbf{F}\varphi \equiv \top \ \mathbf{U}$ {v13>（最终），$\mathbf{G}\varphi \equiv \neg\mathbf{F}\neg\varphi$ （总是）。

LTL 的语义。 令 $Words(\varphi) = \{\sigma = (A_0, A_1, \dots) \in (2^{AP})^\omega \mid \sigma \models \varphi\}$ 为由 φ诱导的线性时序逻辑性质。用 $\sigma^{i+} = (A_i, A_{i+1}, \dots)$ 表示一个从索引 $i \geq 0$开始的词。于是，满足关系 $\sigma \models \varphi$ 归纳定义如下：

$$\begin{array}{lll}
\sigma \models \top & \sigma \models a \text{ iff } a \in A_0 & \sigma \models \neg\varphi \text{ iff } \sigma \not\models \varphi \\
\sigma \models \varphi_1 \wedge \varphi_2 \text{ iff } \sigma \models \varphi_1 \text{ and } \sigma \models \varphi_2 & & \sigma \models \mathbf{X}\varphi \text{ iff } \sigma^{1+} \models \varphi \\
\sigma \models \varphi_1 \ \mathbf{U} \ \varphi_2 \text{ iff } \exists j \geq 0.\ \sigma^{j+} \models \varphi_2 \text{ and } \forall\, 0 \leq i < j.\ \sigma^{i+} \models \varphi_1 & & \\
\sigma \models \mathbf{F}\varphi \text{ iff } \exists j \geq 0.\ \sigma^{j+} \models \varphi & & \sigma \models \mathbf{G}\varphi \text{ iff } \forall j \geq 0.\ \sigma^{j+} \models \varphi
\end{array}$$

ω-正则性质 [29] 构成一个丰富的类别，涵盖了线性时序逻辑。它们由 ω-自动机识别，这类自动机使用专门的接受条件来接受无限词。下面介绍本文使用的 ω-自动机。

确定性 Rabin 自动机。 一个确定性 *Rabin* 自动机 （DRA）是一个元组 $\mathcal{A} = (Q, q_0, \Sigma, \delta, Acc)$，其中 Q 是有限状态集， $q_0 \in Q$ 是初始状态， Σ 是有限字母表， $\delta\colon\ Q \times \Sigma \to Q$ 是转移关系，而$Acc = \{(E_i, F_i) \mid E_i, F_i \subseteq Q, E_i \cap F_i = \emptyset, 1 \leq i \leq M\}$ 是接受条件。

确定性 Rabin 自动机的语义。 $\mathcal{A}$, $\sigma = (\sigma_0, \sigma_1, \dots) \in \Sigma^\omega$的一个词是一个由字母组成的无限序列。词 σ, $\rho = (q_0, q_1, \dots) \in Q^\omega$上的一次运行是一个由状态组成的无限序列，并且对所有 $i \in \mathbb{N}_0$，均有 $q_{i+1} = \delta(q_i, \sigma_i)$。用 Ξ 表示$\mathcal{A}$的所有运行的集合。令 Inf(ρ) 表示 ρ 中被无限次访问的状态集合。词 σ 上的运行 ρ 是接受运行，当且仅当存在某个 $i \in [1, M]$，使得 Inf(ρ) $\cap E_i = \emptyset$ 且 Inf(ρ) $\cap F_i \neq \emptyset$；此时，词 σ 被 $\mathcal{A}$接受。 $\mathcal{A}$的语言记作 $\mathcal{L}(\mathcal{A})$，是所有被 $\mathcal{A}$接受的词的集合。

2.2 概率编程

我们假设读者熟悉概率论中的一些概念，例如概率测度、随机变量和期望值。

概率编程语言的语法。 我们考虑标准的命令式概率编程语言（PPL），它包含常见的循环、条件和顺序结构。其语法如下:

$$S ::= \textbf{跳过} \mid x := E \mid x \sim D \mid \textbf{当}\, B\, \textbf{执行}\ S\, \textbf{结束} \mid \textbf{如果}\ B\, \textbf{则}\ S_1\, \textbf{否则}\ S_2\, \textbf{结束} \mid \textbf{如果概率}(p)\, \textbf{则}\ S_1\, \textbf{否则}\, S_2\, \textbf{结束} \mid S_1;\ S_2 B ::= \textbf{真} \mid \neg B \mid B_1\, \textbf{且}\, B_2 \mid E_1 \le E_2 E :: = x \mid c \mid E_1 + E_2 \mid E_1 \times E_2 \quad D ::= \textbf{均匀}(a, b) \mid \cdots$$

其中 $a, b \in \mathbb{R}$ 为常量， $p \in [0,1]$，元变量 S、 B、 E和D 分别表示语句、条件、算术表达式和分布（离散或连续）。语句“$x \sim D$”是一个采样赋值，它从分布 D 中抽取一个样本值 r，然后将其赋给 x。语句“**如果概率**(p) **则** S_1 **否则** S_2 **结束** ”是一个概率分支语句，它以概率 p执行 S_1 ，或以概率 $1-p$执行 S_2。

设 $V = \{x_1, \ldots, x_n\}$ 是一组实值程序变量， $R = \{r_1, \ldots, r_m\}$ 是一组实值样本变量。

概率编程语言语义。 给定一个概率程序 P，可以将其建模为一个概率转移系统 (PTS) $\Pi = (L,\ V,\ R,\ \mathcal{D}_R,\ \mathcal{T},\ \ell_{\text{init}},\ \ell_{\text{out}},\ \mathcal{D}_0)$，其中:

- L 是一个有限的位置集合， $\ell_{\text{init}} \in L$ 是初始位置，$\ell_{\text{out}} \in L$ 是终止位置；
- V 、 R 分别是有限的程序变量集和样本变量集；
- $\mathcal{D}_R$ 是一个函数，为每个样本变量 $r \in R$ 指定一个概率分布 $\mathcal{D}(r)$，而 $\mathcal{D}_R$ 可视为 R 中所有样本变量的联合分布；
- $\mathcal{T}$ 是一个有限的转移集合。每个转移 $\tau \in \mathcal{T}$ 都是一个元组 $(\ell, \phi, f_1, \ldots, f_u)$，满足：(i) ℓ 是源位置；(ii) ϕ 是关于 V 的守卫谓词；(iii) 每个分支的形式为 $f_j := (p_j, \text{Up}_j, \ell_j)$，其中 (a) $p_j \in (0,1]$ 是分支概率，(b) $\text{Up}_j : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$ 是程序赋值的更新函数，(c) ℓ_j 是目标位置；
- $\mathcal{D}_0$ 是程序赋值上的初始概率分布。

我们假设所有概率转移系统都满足无恶魔限制。也就是说，对于每个位置 ℓ，(1) 从 ℓ 出发的任意两个不同转移的守卫条件互斥：对于 $i \neq j$， $\phi_i \wedge \phi_j \equiv \text{false}$；(2) 所有转移的 $\phi_1, \ldots, \phi_k$ 守卫条件是完备互斥的： $\bigvee_{i=1}^{k} \phi_i \equiv \text{true}$。

概率转移系统的状态 是一个元组 $s = (\ell, \mathbf{v})$，其中 $\ell \in L$ 是位置， $\mathbf{v} \in \mathbb{R}^n$ 是程序赋值。我们用 S表示状态空间。转移$\tau = (\ell, \phi, f_1, \ldots, f_l)$在状态 $s = (\ell, \mathbf{v})$处是使能的 ，当且仅当 $\mathbf{v} \models \phi$。概率转移系统的一条轨迹 是一个由状态组成的无限序列，即 $\pi = (s_0, s_1, \ldots)$。概率转移系统的语义

定义如下：（1）从初始状态 $s_0 = (\ell_{\text{init}}, \mathbf{v}_0)$开始，其中 $\mathbf{v}_0 \sim \mathcal{D}_0$；（2）在第 n 步，若状态为 $s_n = (\ell_n, \mathbf{v}_n)$且 $\ell_n = \ell_{\text{out}}$，则 $s_{n+1} = (\ell_{\text{out}}, \mathbf{v}_n)$；否则，选取一个唯一的使能转移 $\tau = (\ell_n, \phi, f_1, \ldots, f_w)$，并以概率 $p_j(\mathbf{r}_n)$选择一个分支 f_j，更新为 $s_{n+1} = (\ell_{n+1}, \mathbf{v}_{n+1})$，其中 $\ell_{n+1} = \ell_j$ 且 $\mathbf{v}_{n+1} = \text{Up}_j(\mathbf{v}_n, \mathbf{r}_n)$，其中 $\mathbf{r}_n \sim \mathcal{D}_n$。

不变式。给定一个概率转移系统 Π，不变式 是一个函数 I，它为每个位置 $\ell \in L$分配一个关于程序变量的谓词 $I(\ell)$。如果存在轨迹 $\pi = (s_0, s_1, \ldots)$，使得对于某个 $n \in \mathbb{N}$ 有 $s_n = (\ell, \mathbf{v})$，则状态 $(\ell, \mathbf{v})$ 是可达的。不变式 I 对可达状态进行过近似。

概率转移系统 Π 的执行通过上述描述的概率执行以及一般状态空间马尔可夫链 [22]等标准构造，在程序轨迹上定义了一个概率空间。我们用 $\mathbb{P}_{\mathbf{v}_{\text{init}}}(-)$ 表示该概率空间中的概率测度。

2.3 时序后验推断

考虑一个概率程序 P及其概率转移系统 Π。设 $AP = \{p_0, p_1, \ldots, p_N\}$为一个有限的原子命题集，其中的元素是关于程序变量的谓词，形式为 $exp(\cdot) \geq 0$，其中 $exp\colon\ \mathbb{R}^n \to \mathbb{R}$。定义一个标记函数 $Lb : S \to 2^{AP}$，使得对于 Π的任意轨迹 $\pi = (s_0, s_1, \ldots)$，都有一个对应的词 $\sigma_\pi = (Lb(s_0), Lb(s_1)\ldots)$，其中每个 $Lb(s_t) \in 2^{AP}$。令 $Words(\Pi)$ 表示由 Π诱导的所有词的集合。

给定一个 ω-正则性质 φ 及其语言 $\mathcal{L}(\varphi)$，当且仅当词$(\Pi) \subseteq \mathcal{L}(\varphi)$。接下来，我们形式化时间后验分布的概念。

定义 1（TPD）。概率转移系统 Π 的时间后验分布（*TPD*）TPD_Π 定义如下：

$$\text{TPD}_\Pi(\varphi, \psi) := \frac{Z_\Pi(\varphi, \psi)}{Z_\Pi(\psi)} = \frac{\int_{\mathcal{V}} \mathbb{P}_{\mathbf{v}_{\text{init}}}(\Pi \models \varphi \wedge \psi) \mu_{\text{init}}(\mathrm{d}\mathbf{v}_{\text{init}})}{\int_{\mathcal{V}} \mathbb{P}_{\mathbf{v}_{\text{init}}}(\Pi \models \psi) \mu_{\text{init}}(\mathrm{d}\mathbf{v}_{\text{init}})} \tag{1}$$

其中，φ、ψ 是两个 ω-正则性质，μ_{init} 是由初始概率分布 $\mathcal{D}_0$诱导的概率测度，而 $\mathcal{V} := \{s \in S \mid s \in U \wedge \mu_{\text{init}}(U) > 0\}$是 μ_{init}的支撑集。为简洁起见，我们滥用记号，用$\Pr(\varphi \mid \psi)$表示 *TPD*。当 $0 < Z_\Pi(\psi) < \infty$时，*TPD* 是可积的。

问题陈述。给定一个概率转移系统 Π 和两个 ω-正则性质 φ，ψ，我们希望找到上界和下界 l，$u \in [0, 1]$，使得 $\text{TPD}_\Pi(\varphi, \psi) \in [l, u]$。

请注意，SPI 关注的是程序终止时的瞬时性质。事实上，程序轨迹由一系列程序状态组成，用于描述程序随时间范围变化的时间行为。例如，在示例 1 中，$x = 1$ 会一直持续到程序终止。我们强调，我们的问题并非易解，且比 SPI 更复杂，因为要定量追踪概率程序的无限时间行为十分困难。根据条件 (1)，该问题可以归结为求出 ω-正则性质满足概率的定量界限，下一节将对此进行讨论。

3 理论结果

本节中，我们提出一种自动机理论方法，使得针对 TPD 的时间推理变得可行。随后，我们将介绍新的随机屏障证书，以建立 ω-正则性质满足概率的定量界限。

3.1 基于自动机的分解

众所周知，任何 ω-正则性质 φ 在 AP 上都可以转换为一个确定性 Rabin 自动机 $\mathcal{A}_\varphi = (Q,\ q_0,\ 2^{AP},\ \delta,$ 接受条件$)$，该自动机接受与 φ相同的语言，即 $\mathcal{L}(\varphi) = \mathcal{L}(\mathcal{A}_\varphi)$（参见 [10]）。

FOV 和 IOV 集。给定 $\mathcal{A}_\varphi$的一个子集 $U \subseteq Q$，若对于任意运行 $\rho \in \Xi$，$\mathrm{Inf}(\rho) \cap U = \emptyset$，则 U 是有限次访问（FOV）的，称为一个*FOV* 集。若对于任意运行 $\rho \in \Xi$，$\mathrm{Inf}(\rho) \cap U \neq \emptyset$，则 U 是无限次访问（IOV）的，称为一个*IOV* 集。

考虑一个带有标记函数 Lb 的概率转移系统 Π 以及一个确定性 Rabin 自动机 $\mathcal{A}_\varphi$。我们通过两类积系统来分解对 φ的满足性。

FOV 和 IOV 乘积。对于子集 $U \subseteq Q$，Π 和 $\mathcal{A}_\varphi$ 在集合 U 上的一个 *FOV* 乘积 定义为满足以下条件的随机过程 $\Pi \otimes \mathcal{A}_\varphi^U = \{X_n\}_{n \in \mathbb{N}_0}$：

- $X_0 = (s_0,\ q_0,\ 0)$，$s_0 = (\ell_{\mathrm{init}},\ \mathbf{v}_0) \in S_0$，其中 $\mathbf{v}_0 \sim \mathcal{D}_0$；$-$对于所有 $n \geq 0$，$X_n = (s_n,\ q_n,\ l_n)$，其中 $X_{n+1} = (s_{n+1},\ q_{n+1},\ l_{n+1})$ 是 s_n 的后继，并且 s_{n+1} 由 Π 的语义确定（见第 2.2 节），$q_{n+1} = \delta(q_n,\ Lb(s_n))$；如果 $q_{n+1} \in U$，则为 $l_{n+1} = l_n + 1$，否则为 $l_{n+1} = l_n$。

同理，Π 和 $\mathcal{A}_\varphi$ 在集合 U 上的一个 *IOV* 乘积 定义为满足以下条件的随机过程 $\Pi \otimes \mathcal{A}_\varphi^U = \{X_n\}_{n \in \mathbb{N}_0}$：

- $X_0 = (s_0,\ q_0,\ 0)$，$s_0 = (\ell_{\mathrm{init}},\ \mathbf{v}_0) \in S_0$与 $\mathbf{v}_0 \sim \mathcal{D}_0$配合；$-$对于所有 $n \geq 0$，$X_n = (s_n,\ q_n,\ l_n)$，其中 $X_{n+1} = (s_{n+1},\ q_{n+1},\ l_{n+1})$ 是 s_n 的后继，使得 s_{n+1} 由 Π的语义决定（见第 2.2 节），$q_{n+1} = \delta(q_n,\ Lb(s_n))$；当 $q_{n+1} \in U$时为 $l_{n+1} = 0$，否则为 $l_{n+1} = l_n + 1$。

这两个乘积的主要区别在于，我们分别使用一个计时变量l 来计算 FOV 乘积中进入 U 的次数，以及 IOV 乘积中连续离开 U 的次数。

一个乘积轨迹 $\theta = (X_0,\ X_1,\ \ldots)$是由乘积状态 X_i构成的无限序列，所有乘积轨迹的集合记作 Θ。令 $\theta[2] = (q_0,\ q_1,\ \ldots)$ 为由 θ诱导的确定性 Rabin 自动机的相应运行。同理，$\theta[3] = (h_0,\ h_1,\ \ldots)$。

命题 1 $\Pi \otimes \mathcal{A}_\varphi^U$ U $\theta[2] \cap$。给定一个 *FOV* 乘积，它是 $U = \emptyset$ $\theta \in \Theta$ $max\ \theta[3] < \infty$ $\theta \in \Theta$ 一个 *FOV* 集，即，对于任意乘积轨迹，$\mathrm{Inf}()$成立，当且仅当对于任意，() 成立。

命题 2 $\Pi \otimes \mathcal{A}_\varphi^U$ U $\theta[2] \cap$。给定一个 *IOV* 乘积，它是 $U \neq \emptyset$ $\theta \in \Theta$ $max\ \theta[3] < \infty$ $\theta \in \Theta$ 一个 *IOV* 集，当且仅当对于任意乘积轨迹，$\mathrm{Inf}()$，即对于任意() 。

回顾第 2.1 节， $\mathcal{A}_\varphi$ 的 Rabin 接受条件为$Acc = \{(E_i, F_i) \mid E_i, F_i \subseteq Q, E_i \cap F_i = \emptyset, 1 \le i \le M\}$；在词 σ 上的运行 ρ 是接受的，当且仅当对于某个 $i \in [1, M]$，$\mathrm{Inf}(\rho) \cap E_i = \emptyset$ 且 $\mathrm{Inf}(\rho) \cap F_i \neq \emptyset$。注意，集合 E_i 只会被访问有限次，这对应于持久性；而集合 F_i 则会被无限次访问，这与重复性有关。

推论 1. 如果对于任意 $\theta \in \Theta$，在 *FOV* 乘积 $\Pi \otimes \mathcal{A}_\varphi^{E_i}$ 中都有 $max(\theta[3]) < \infty$，那么 E_i 是一个 *FOV* 集。如果对于任意 $\theta \in \Theta$，在 *IOV* 乘积 $\Pi \otimes \mathcal{A}_\varphi^{F_i}$ 中都有 $max(\theta[3]) < \infty$，那么 F_i 是一个 *IOV* 集。最后，可以得出结论：$\Pi \models \varphi$。

3.2 定量时序验证

实际上，要确定推论 1 中的条件“$max(\theta[3]) < \infty$”是否成立并不容易。为便于计算，下面给出 FOV 集和 IOV 集的变体。

***k*次 FOV 集和 IOV 集**。设 $k \in \mathbb{N}_0$ 为一个非负常数。集合 $U \subseteq Q$ 是 k次 *FOV* 集，当且仅当对于任意 $\theta \in \Theta$，U 至多被访问 k 次，即 $max(\theta[3]) \le k$。类似地，集合 $U \subseteq Q$ 是 k 次 *IOV* 集，当且仅当对于所有 $\theta \in \Theta$，$Q \setminus U$ 连续被访问至多 k 次，即 $max(\theta[3]) \le k$。

给定一个概率转移系统 Π，其标记函数为 Lb，以及一个确定性 Rabin 自动机 $\mathcal{A}_\varphi$，其集合为 $U \subseteq Q$。给定 Π 的状态 $s = (\ell, \mathrm{v})$，其后继状态 s' 按如下方式计算：(1) 选取在 s处唯一的使能转移 $\tau = (\ell, \phi, f_1, \ldots, f_u)$，该转移包含 $u \ge 1$个形如 $f_j = (p_j, \mathrm{Up}^j, \ell_j)$ 的分支；(2) 以概率$p_j(\mathrm{r})$ 选择第 j 个分支，然后当 $\ell \neq \ell_{\mathrm{out}}$ 时执行 $s' = g(s,\mathrm{r}) = \mathrm{Up}^j(\mathrm{v}, \mathrm{r})$，其中 $\mathrm{r} \sim \mathcal{D}$；否则执行 $s' = g(s, \mathrm{r}) = s$。给定 $\Pi \otimes \mathcal{A}_\varphi^U$ 的一个乘积状态 (s, q)，其后继状态为 (s', q')，其中 $q' = \delta(q, \mathrm{Lb}(s))$。

定理 1（ *k*-时间 FOV 集的下界）。假设存在一个 *FOV* 乘积 $\Pi \otimes \mathcal{A}_\varphi^U$ 的屏障证书（屏障证书）η：$S \times Q \times \mathbb{N} \to \mathbb{R}$，使得对于两个常数 $\gamma \in (0、1)$ 和 $k \in \mathbb{N}_0$，以下条件成立：

$$\eta(s,\ q,\ l) \ge 0 \qquad \forall s \in S, q \in Q, l \in \mathbb{N}_0 \qquad (2)$$

$$\eta(s,\ q_0,\ 0) \le \gamma \qquad \forall s \in S_0 \qquad (3)$$

$$\eta(s,\ q,\ k+1) \ge 1 \qquad \forall s \in S, q \in U \qquad (4)$$

$$\mathbb{E}_{\mathbf{r}\sim\mathcal{D}}[\eta(g(s,\ \mathbf{r})\ q',\ l')] \le \eta(s,\ q,\ \ell) \qquad \forall s \in S,\ q \in Q,\ l \in [0, k] \qquad (5)$$

其中，当 $q' \in U$ 时 $l' = l + 1$，否则为 l。那么，对于任意初始乘积状态$(s_0, q_0, 0)$ 其中 $s_0 \in S_0$，我们有 $\mathbb{P}_{s_0}[U$ 是一个 k 次 *FOV* 集$] \ge 1 - \eta(s_0, q_0, 0) =: l_i^{fin}$。

直观解释。注意，条件 (5) 是一种超鞅型条件。这确保屏障证书在每个时间步的期望不增，可利用 Ville 不等式 [32] 建立满足概率的下界。

定理 2（ k次 FOV 集的上界）。假设存在一个 *FOV* 乘积 $\Pi \otimes \mathcal{A}_{\varphi}^{U}$ 的屏障证书 $\eta\colon\ S \times Q \times \mathbb{N} \to \mathbb{R}$，使得对于某些常数 $\alpha \in (0,\ 1)$、$0 \leq \lambda < \gamma \leq 1$ 和 $k \in \mathbb{N}$，以下条件成立：

$$0 \leq \eta(s,\ q,\ l) \leq 1 \qquad \forall s \in S, q \in Q, l \in \mathbb{N}_0 \qquad (6)$$

$$\eta(s,\ q_0,\ 0) \geq \gamma \qquad \forall s \in S_0 \qquad (7)$$

$$\eta(s,\ q,\ k+1) \leq \lambda \qquad \forall s \in S, q \in U \qquad (8)$$

$$\alpha \cdot \mathbb{E}_{\mathbf{r} \sim \mathcal{D}}[\eta(g(s,\ \mathbf{r})\ q',\ l')] \geq \eta(s,\ q,\ \ell) \qquad \forall s \in S, q \in Q, l \in [0,k] \qquad (9)$$

其中，$l' = l + 1$ 若 $q' \in U$ 且 l，否则。于是，对于任意初始乘积状态（$s_0, q_0, 0$），其中 $s_0 \in S_0$，我们有 $\mathbb{P}_{s_0}[U$ 是一个 k次 *FOV* 集$] \leq 1 - \eta$（$s_0, q_0, 0$）$=:\ u_i^{fin}$。

直观解释。条件（9）是一个次鞅型条件，它要求屏障证书的期望在经过一个时间步后增加。我们利用它通过可选停止定理（OST） [37]证明满足概率的上界。

定理 3（次 IOV 集的下界）。假设 *IOV* 乘积 $\Pi \otimes \mathcal{A}_{\varphi}^{U}$ 存在一个屏障证书 h：$S \times Q \times \mathbb{N} \to \mathbb{R}$，使得对于两个常数 $\gamma \in$（0,1）和 $k \in \mathbb{N}$，以下条件成立：

$$h(s,\ q,\ l) \geq 0 \qquad \forall s \in S, q \in Q, l \in \mathbb{N}_0 \qquad (10)$$

$$h(s,\ q_0,\ 0) \leq \gamma \qquad \forall s \in S_0 \qquad (11)$$

$$h(s,\ q,\ k+1) \geq 1 \qquad \forall s \in S, q \in Q \setminus U \qquad (12)$$

$$\mathbb{E}_{\mathbf{r} \sim \mathcal{D}}[h(g(s,\ \mathbf{r})\ q',\ l')] \leq h(s,\ q,\ l) \qquad \forall s \in S, q \in Q, l \in [0,k] \qquad (13)$$

其中，$l' = 0$ 当 $q' \in U$ 且 $l' = l + 1$ 时，否则为 $l' = l + 1$。那么，对于任意初始乘积状态 $(s_0, q_0, 0)$ 其中 $s_0 \in S_0$，我们有 $\mathbb{P}_{s_0}[U$ 是一个 k 次 *IOV* 集$] \geq 1 - h($ $s_0, q_0, 0) =:\ l_i^{inf}$。

定理 4（ k 次 IOV 集的上界）。假设存在 *IOV* 乘积 $\Pi \otimes \mathcal{A}_{\varphi}^{U}$ 的屏障证书 h：$S \times Q \times \mathbb{N} \to \mathbb{R}$，使得对于某些常数 $\gamma \in (0,\ 1)$、$0 \leq \lambda < \gamma \leq 1$ 和 $k \in \mathbb{N}$，以下条件成立：

$$0 \leq h(s,q,l) \leq 1 \qquad \forall s \in S, q \in Q, l \in \mathbb{N}_0 \qquad (14)$$

$$h(s,q_0,0) \geq \gamma \qquad \forall s \in S_0 \qquad (15)$$

$$h(s,q,k+1) \leq \lambda \qquad \forall s \in S, q \in Q \setminus U \qquad (16)$$

$$\alpha \cdot \mathbb{E}_{\mathbf{r} \sim \mathcal{D}}[h(g(s,\mathbf{r}),q',l')] \geq h(s,q,l) \qquad \forall s \in S, q \in Q, l \in [0,k] \qquad (17)$$

其中，若 $q' \in U$，则为 $l' = 0$；否则为 $l' = l + 1$。那么，对于任意满足 $s_0 \in S_0$ 的初始乘积状态$(s_0, q_0, 0)$，有 $\mathbb{P}_{s_0}[U$ 是一个 k 次 *IOV* 集$] \leq 1 - h(s_0, q_0,$ $0) =:\ u_i^{inf}$。

下面给出关于在 k 次 FOV 和 IOV 集下满足 ω-正则性质的收敛定理。令 $(E_i, F_i) \in Acc$ 为 $\mathcal{A}_\varphi$ 中 Rabin 接受条件的一个元素。E_i 是一个 FOV 集，满足对于任意 $\theta \in \Theta$，$max(\theta[3]) = m^* < \infty$；$F_i$ 是一个 IOV 集，满足对于任意 $\theta \in \Theta$，$max(\theta[3]) = n^* < \infty$。

定理 5（收敛性）。对于任意初始状态 $s_0 \in S_0$，当 $k \to m^*$满足定理 *1* 和定理 *2* 中的条件时，我们有 $\mathbb{P}_{s_0}[E_i$ 是一个 *FOV* 集$] \in [l_i^{fin}, u_i^{fin}]$；当$k \to n^*$ 满足定理 *3* 和定理 *4* 中的条件时，我们有 $\mathbb{P}_{s_0}[F_i$ 是一个 *IOV* 集$] \in [l_i^{inf}, u_i^{inf}]$。因此，$\mathbb{P}_{s_0}[\Pi \models \varphi] \in [l_i^{fin} \cdot l_i^{inf}, u_i^{fin} \cdot u_i^{inf}]$。

4 算法方法

本节中，我们给出用于综合第 3 节中屏障证书的基于模板的自动化算法。

输入与假设。我们的算法的输入包括一个带有标记函数 Lb 的概率转移系统 Π、一个表示 ω-正则性质 φ 的确定性 Rabin 自动机 $\mathcal{A}_\varphi$（$\mathcal{A}_\varphi$ 中的状态可以是自然数）、一个不变式 I、[4]，以及技术变量d, k，它们用于指定多项式模板的次数和屏障证书的计数（例如，参见定理 1）。我们关注多项式概率转移系统，因此假设 Π 中的所有守卫条件和更新，以及所有不变式 $I(\ell)$ 都是关于程序变量的多项式表达式。

输出。我们的算法的任务是综合第 3.2 节中的多项式屏障证书 η，h 以及由此得到的定量界。

概述。我们的算法是一种标准的基于模板的方法 [9,34,35]。我们为第 3.2 节中的每个屏障证书设置一个带有未知系数的多项式模板。接下来，将每个屏障证书的条件编码为带有未知系数的多项式不等式蕴含关系。然后，通过应用经典的 Farkas 引理 [11] 或 Putinar 正定性定理 [27]，我们将综合问题归约为线性规划（LP）或半定规划（SDP）。最后，通过调用 LP 或 SDP 求解器来求解该规划问题。下面给出我们的算法的四个步骤。为简洁起见，我们仅展示定理 1 中的屏障证书，其他证书可以用相同方式推导。

步骤 1 - 设置模板。对于每个位置 $\ell \in L$，我们的算法设置一个模板 $\eta(\ell)$，该模板是一个多项式，由程序变量上次数不超过 d 的所有可能单项式组成，每个单项式都带有一个未知系数。例如，在示例 1 中，程序有两个程序变量 x，y，并且如定理 1 所要求，还需要两个额外变量 q，l。设 $d = 1$，则对于每个位置 ℓ_i，算法设置 $\eta(\ell_i) = c_{i,0} + c_{i,1} \cdot x + c_{i,2} \cdot y + c_{i,3} \cdot q + c_{i,4} \cdot l$ 其中 $c_{i,j}$'s 为未知系数。

步骤 2 - 构造蕴含关系。算法使用来自

[4] 我们假设输入中提供了一个不变式。不变式生成是一个独立且研究充分的问题，可以使用 [28,8] 实现自动化。

步骤 1中的模板，符号化地计算定理 1 中屏障证书的条件。注意，所有这些条件都是关于程序变量的多项式不等式之间的蕴含关系，其系数未知。也就是说，它们的形式为“$\forall$x. A(x) $\Rightarrow$ b(x)”，其中 A 是关于变量的一组多项式不等式，而 B 也是关于变量的多项式不等式，但其系数未知。例如，对于示例 1 中的程序，算法符号化地计算条件 (3)，其中 q, $l = 0$ 在初始位置处，即

$$\forall(x, y, q, l).\ (x \geq 0) \wedge (y \geq 0) \Rightarrow c_{0,0} + c_{0,1} \cdot x + c_{0,2} \cdot y \leq \gamma. \tag{18}$$

步骤 3 - 量词消去。 在上一步之后，我们得到一个形如“$\bigwedge_i$($\forall$x. A_i(x) $\rightarrow$ B_i(x))”的约束系统。随后，算法消去每个约束中关于 x 的全称量化。下面展示 A_i, B_i 为线性不等式的情形。例如，算法将条件 (18) 重写为 $\kappa_1 \cdot x + \kappa_2 \cdot y = \gamma - c_{0,0} - c_{0,1} \cdot x - c_{0,2} \cdot y$，其中包含新的未知系数 $\kappa_i \geq 0$。根据 Farkas 引理 [11], ，我们可以可靠地得到一个新的线性方程组：

$$0 = \gamma - c_{0,0}, \qquad \kappa_1 = -c_{0,1}, \qquad \kappa_2 = -c_{0,2}.$$

对于多项式情形，请读者参阅 [35]。

步骤 4 - 求解约束系统。由于屏障证书的所有条件都已转换为线性约束或半正定约束，我们调用线性规划求解器或半定规划求解器，对屏障证书中的下界/上界进行优化，并综合模板的未知系数。例如，在示例 1 中，我们计算定理 1 中的下界，并调用线性规划求解器最大化目标函数 $\eta(s_0, q_0, 0) = c_{0,0} + c_{0,1} \cdot 1 + c_{0,2} \cdot 0$，其初始状态为 $s_0 = (\ell_{\text{init}}, 1, 0)$。

定理 6（可靠性）。如果我们的算法为多项式模板中的未知系数找到有效解，那么它将返回 k-时间 *FOV* 集和 *IOV* 集上概率的下界或上界。

证明。如果该算法能够综合定理 1 中的 BC，那么就可以得到 U 是 k-时间 FOV 集的概率下界。定理 2 至 4 同样成立。

5 评估

我们将该方法实现为一个名为 TPInfer 的原型系统。实验旨在针对以下几个目标评估我们方法的有效性，包括：

1. ω-正则性质的定量验证。2. 时序后验推断的定量验证。
3. 超参数 d, k 的影响。

5.1 基准测试与设置

我们在五个概率程序上评估了该方法的有效性，这些程序都包含具有无限次迭代的循环。具体而言，ex3 和 ex4 取自 PSI， [14], 1d-asym-rwl 取自 [39], ，其余两个程序则是本研究提出的新示例。我们验证的 ω-正则性质分为两类：一类可用线性时序逻辑表示，另一类只能用自动机表示（即 RE1 和 RE2）。所有实验均在一台运行 Ubuntu 22.04 的工作站上执行，该工作站配备 32 核 AMD Ryzen Threadripper CPU、128GB 内存和一块 24564MiB 图形处理器。

5.2 ω-正则性质的定量验证效果

我们首先验证该方法在为 Rabin 持续性和重复接受综合屏障证书方面的有效性，并验证利用这些证书计算可靠的上界和下界的能力，以界定概率程序满足给定 ω-正则性质的概率。结果汇总于表 1。对于每个 ω-正则规约，我们计算与其相应 Rabin 持续性和重复接受条件相关的概率，并据此综合出满足概率的认证下界和上界。

如表中所示，基于仿真的概率（Sim.）始终落在综合得到的下界（L.B.）和上界（U.B.）所定义的区间内。这从经验上证实了验证结果的正确性和紧致性。仿真结果与认证界限相吻合，表明本方法构造的随机屏障证书能够捕捉系统的关键概率行为，即使对于需要对无限执行进行推理的性质也是如此。

总而言之，结果验证了我们方法的可靠性，并展现了其定量验证多种 ω-正则性质的实际能力。

5.3 时序后验推断的定量验证效果

表 2 展示了我们的方法在定量验证所考虑的 ω-正则性质的时序后验概率方面的有效性。对于每项性质，我们的方法通过合成随机屏障证书，计算出经过认证的概率下界和上界；这些概率界能够可靠地包络真实的后验概率。

如表 2 所示，基于仿真的概率始终落在合成区间内，这表明我们得到的界限有效且具有参考价值。这种一致性进一步证实，所提出的基于屏障证书的方法能够准确刻画含有无界循环的程序的概率行为，即使是在推理以 ω-正则框架定义的复杂时序性质时也是如此。用于计算后验概率的屏障证书参数也与表 1 中使用的参数保持一致。这些结果彰显了我们

表 1： ω-正则性质定量验证结果

Task	性质	Sim.	L.B.	U.B.	E.d.	F.d.	k	时间（秒）
ex3	最终(b=0)	0.5	0.50000	0.75356	1	3	3	1012.94
	最终(b=0)&最终(n≥2)	0.2493	0.17385	0.37294	1	3	4	28944.35
	全局最终(b=1)	0.668	0.66670	0.87391	1	3	3	1664.72
	全局最终(b=1)&全局最终(n≥2)	0.2493	0.18394	0.36288	1	3	3	1881.14
ex4	最终(c2=1)	0.6665	0.61804	0.85172	1	3	4	2395.88
	全局(c1=0)&最终(c2=1)	0.3335	0.29054	0.53084	3	3	4	6946.69
	全局最终(c2=1)	0.6665	0.61903	0.89802	1	3	7	14393.83
	全局最终(c1=0& c2=1)	0.3333	0.30193	0.49660	1	3	5	7165.65
一维非对称随机游走	最终(n≥4)	0.109	0.01962	0.10990	1	3	3	1531.05
	全局(x≤5)&最终(n≥4)	0.1068	0.09477	0.24967	3	3	3	3140.63
	全局最终(x=0 → n≥4)	0.1094	0.05140	0.13178	1	3	3	1399.08
	全局最终(n≥3)	0.2502	0.18586	0.31765	1	3	4	1611.56
RE1	最终(y>0)	0.3563	0.27042	0.36236	1	3	2	5512.71
	全局(x=1)&最终(y>0)	0.1255	0.09462	0.19100	3	3	2	15791.58
RE2	(n≤2)*(x=1)	0.8749	0.86578	0.94964	3	3	2	2620.16
	(n≤3)*(x=1)	0.9375	0.93582	0.97739	3	3	3	2940.68

备注。**仿真**。：通过仿真得到的概率。**下界**：经认证的下界。**上界**：经认证的上界。**E.d.**：对应于 Ei 的屏障证书的多项式次数。**F.d.**：对应于 Fi 的屏障证书的多项式次数。**k**：屏障证书的计数。

定量验证方法的可靠性，以及其在实际概率分析中的适用性。

5.4 多项式次数 d 和计数 k的影响

表3展示了多项式次数 d 和计数 k 对屏障证书综合性能的影响。当使用较低的多项式次数时，多项式基的表达能力会受到限制，这可能导致综合过程无法找到可行的证书，进而出现失败案例。这一局限反映出低次多项式可能无法充分刻画不变量的几何结构。

具体而言，增大 k 有助于改进保证，因为证书能够刻画更长的执行行为，从而使计算得到的概率界逐渐稳定。下界和上界收敛至基于仿真的概率，表明定量验证结果（另见定理 5）与经验执行结果相一致。

表 2：后验概率的定量验证结果

Task	性质	Sim.	L.B.	U.B.
ex3	最终(n $\geq$ 2) | 最终(b = 0)	0.5001	0.23071	0.74588
	全局最终(n $\geq$ 2) | 全局最终(b = 1)	0.2493	0.21048	0.54429
ex4	全局(c1 = 0) | 最终(c2 = 1)	0.5000	0.34113	0.85891
	全局最终(c1 = 0&c2 = 1) | 全局最终(c2 = 1)	0.4998	0.33622	0.80222
一维非对称随机游走	全局(x $\leq$ 5)|最终(n $\geq$ 4)	0.9743	0.86227	1
	全局最终(x = 0 $\rightarrow$ n $\geq$ 4) | 全局最终(n $\geq$ 3)	0.4375	0.16181	0.70903
RE1	全局(x = 1) |最终(y > 0)	0.4005	0.26112	0.70632
RE2	(n $\leq$ 2)*(x = 1) | (n $\leq$ 3)*(x = 1)	0.9329	0.88581	1

备注。**仿真**：通过仿真得到的概率。**下界**：经认证的下界。**上界**：经认证的上界。

然而，表3也揭示了一种权衡：增大 d 和 k 会显著增加综合时间。这是意料之中的，因为更高次的多项式会扩大优化问题的搜索空间，而更大的访问次数界则会给证书综合带来更复杂的约束。

还值得注意的是，由于数值优化求解器存在浮点精度问题，合成得到的紧下界有时可能会超过基于仿真的概率估计。这种差异只会出现在边界情形中，并不影响该方法的可靠性，因为在求解器的精度模型范围内，经认证的界在数学上仍然有效。

6 相关工作

概率程序的形式化验证。概率程序的形式化验证已通过语义、推理原则和自动化分析框架得到了广泛研究。奠基性工作提出了最弱后期望语义和程序逻辑，用于推理概率行为 [20]。后续研究则发展出自动化技术，利用排序超鞅和基于期望的推理来证明几乎必然终止性和安全性 [6,9,13]。这些方法关注不动点处基于状态的性质——通常是终止时的性质——并不支持对执行轨迹上的时间事件进行后验推理。我们的工作则通过引入以观测为条件的时序性质后验推断，与这些方法有所不同。

随机系统的屏障证书。屏障证书为证明连续系统、混合系统和随机系统的安全性提供了充分条件。原始框架引入屏障函数，以排除不安全集合中的轨迹 [26]，后来又利用类李雅普诺夫条件和平方和条件将其扩展至随机动态 [25,38]。尽管这些方法在证明不变性方面十分强大

表3：改变 k 和 d 对综合性能的影响

Task	性质	Sim.	L.B.	U.B.	d	k	time
ex3	F(b = 0)	0	0	0.7996	3	1	197.0999
		0.5	0.5002	**fail**	3	2	531.289
		0.5	0.5000	0.7535	3	3	1012.9471
		0.5	0.5077	0.8645	3	4	1662.5991
		0.5	0.5020	0.8835	3	5	2426.8311
RE2	(n $\leq$ 2)* (x = 1)	0.8749	0.6551	0.9778	2	1	34.7432
		0.8749	**fail**	0.9829	2	2	94.5126
		0.8749	**fail**	0.9821	2	3	184.5404
		0.8749	0.8713	0.9675	3	1	233.3126
		0.8749	0.8657	0.9496	3	2	639.6580
		0.8749	0.8721	0.8901	3	3	1267.5365

备注。**仿真**：通过仿真计算概率。**下界**：F1 的经认证下界。**上界**：F1 的经认证上界。

并能证明安全性，但它们无法量化后验概率，也无法纳入观测证据。相比之下，我们的方法直接针对由概率程序轨迹诱导的时序后验概率进行推理。

时序逻辑验证。线性时序逻辑（LTL）和 ω-正则规格等时序逻辑，是用于描述无限行为上的安全性和活性属性的标准工具 [31]。对于概率系统，PRISM 等模型检测器 [21] 和概率时序逻辑 [2] 会计算满足某个时序规格的先验概率。这些方法并未纳入基于观测的贝叶斯条件化，也无法对时间事件进行后验推理。我们的工作补充了这方面的研究，使人们能够对概率程序的执行轨迹进行时序后验推断。

7 结论

我们提出了时序后验推断，将经典后验推断扩展到概率程序的完整执行轨迹。通过结合程序语义与时序逻辑，我们的方法支持在观测证据下，对安全性、活性及其他 ω-正则性质进行后验推理。我们提出了定量证明证书和自动化综合算法，并展示了该方法在标准推断失效的程序上的有效性。这为统一贝叶斯条件化与时序验证提供了有原则的基础，也为进一步扩展到更丰富的性质和更大规模的模型奠定了方向。

参考文献

1. Abate, A., Giacobbe, M., Roy, D.：定量超鞅证书。载于：国际计算机辅助验证会议。第 3–28 页。Springer (2025) 2. Baier, C., Katoen, J.P.：模型检测原理。MIT出版社 (2008) 3. Barthe, G., Espitau, T., Grégoire, B., Hsu, J., Strub, P.：证明概率程序的期望敏感性。ACM 程序设计语言学报**2**(POPL)，57:1–57:29 (2018 3158145 4 10 1145)。https://doi.org/ . / . Batz, K., Chen, M., Junges, S., Kaminski, B.L., Katoen, J., Matheja, C.：通过归纳综合归纳不变量验证概率程序。载于：Sankaranarayanan, S., Sharygina, N. (编者)《系统构造与分析工具和算法》——第29届国际会议，TACAS 2023，作为欧洲软件理论与实践联合会议 ETAPS 2022 的一部分举行，法国巴黎，2023年4月22日至27日，论文集，第二部分。计算机科学讲义，第13994卷，第410–429页。Springer (2023)。https://doi.org/10.1007/978-3-031-30820-8_25, https://doi.org/10.1007/ 978-3-031-30820-8_255. Bishop, C.M., Nasrabadi, N.M.：模式识别与机器学习，第4卷。Springer (2006) 6. Chakarov, A., Sankaranarayanan, S.：利用鞅进行概率程序分析。载于：国际计算机辅助验证会议。第511–526页。Springer (2013) 7. Chakarov, A., Voronin, Y.L., Sankaranarayanan, S.：几乎必然持续性与重复性性质的演绎证明。载于：系统构造与分析工具和算法国际会议。第260–279页。Springer (2016) 8. Chatterjee, K., Fu, H., Goharshady, A.K., Goharshady, E.K.：非确定性递归程序的多项式不变量生成。载于：第41届 ACM SIGPLAN 程序设计语言设计与实现会议论文集。第672–687页 (2020) 9. Chatterjee, K., Fu, H., Novotn`y, P., Hasheminezhad, R.：仿射概率程序定性与定量终止问题的算法分析。载于：第43届 ACM SIGPLAN-SIGACT 程序设计原理研讨会论文集。第327–342页 (2016) 10. Duret-Lutz, A., Renault, E., Colange, M., Renkin, F., Gbaguidi Aisse, A., Schlehuber-Caissier, P., Medioni, T., Martin, A., Dubois, J., Gillard, C., 等：从 Spot 2.0 到 Spot 2.10：有哪些新变化？载于：国际计算机辅助验证会议。第174–187页。Springer (2022) 11. Farkas, J.：简单不等式理论。《纯粹与应用数学杂志》（Crelles Journal）**1902**(124)，1–27 (1902) 12. Feng, S., Chen, M., Su, H., Kaminski, B.L., Katoen, J.P., Zhan, N.：可能发散的概率程序的下界。《ACM 程序设计语言学报》**7**(OOPSLA1)，696–726 (2023) 13. Fu, H., Chatterjee, K.：非确定性概率程序的终止性。载于：Enea, C., Piskac, R. (编者)《验证、模型检测与抽象解释》——第20届国际会议，VMCAI 2019，葡萄牙卡斯凯什，2019年1月13日至15日，论文集。计算机科学讲义，第11388卷，第468–490 2019 10 1007 978 3 030 11245 5_22 页。Springer ( )。https://doi.org/ . / - - - - . Gehr, T., Misailovic, S., Vechev, M.：Psi：概率程序的精确符号推断。载于：国际计算机辅助验证会议。第62–83页。Springer (2016)

15. Ghahramani, Z.：概率机器学习与人工智能。Nature**521**(7553), 452–459 (2015) 16. Goodman, N., Mansinghka, V., Roy, D.M., Bonawitz, K., Tenenbaum, J.B.：Church：一种生成模型语言。arXiv 预印本 arXiv:1206.3255 (2012) 17. Gordon, A.D., Henzinger, T.A., Nori, A.V., Rajamani, S.K.：概率编程。在：软件工程的未来论文集，第 167–181 页 (2014) 18. Henzinger, T.A., Mallik, K., Sadeghi, P., Žikelić, Đ.：用于定量 ω-正则验证与控制的超鞅证书。在：国际计算机辅助验证会议，第 29–55 页。Springer (2025) 19. Jaynes, E.T.：概率论：科学逻辑。剑桥大学出版社 (2003) 20. Kaminski, B.L., Katoen, J.P., Matheja, C., Olmedo, F.：针对概率程序预期运行时间的最弱前置条件推理。在：欧洲编程研讨会，第 364–389 页。Springer (2016) 21. Kwiatkowska, M., Norman, G., Parker, D.：PRISM 4.0：概率实时系统验证。在：国际计算机辅助验证会议，第 585–591 页。Springer (2011) 22. Meyn, S.P., Tweedie, R.L.：马尔可夫链与随机稳定性。施普林格科学与商业媒体 (2012) 23. Ngo, V.C., Carbonneaux, Q., Hoffmann, J.：有界期望：概率程序的资源分析。在：Foster, J.S., Grossman, D. (编) ACM SIGPLAN 第 39 届编程语言设计与实现会议论文集，PLDI 2018，美国宾夕法尼亚州费城，2018年6月18日至22日。第 496–512 页。ACM (2018)。https://doi.org/10.1145/3192366.3192394 24. Pnueli, A.：程序的时序逻辑。第 18 届计算机科学基础年度研讨会 (FOCS)，第 46–57 页 (1977) 25. Prajna, P., Jadbabaie, A., Pappas, G.J.：使用屏障证书进行最坏情况与随机安全性验证的框架。IEEE 自动控制汇刊**52**(8), 1415–1428 (2007)。https://doi.org/10.1109/TAC.2007.901844 26. Prajna, S., Jadbabaie, A.：使用屏障证书验证混合系统安全性。在：混合系统：计算与控制国际研讨会，第 477–492 页。Springer (2004) 27. Putinar, M.：紧半代数集上的正多项式。印第安纳大学数学期刊**42**(3), 969–984 (1993) 28. Solving, C.：使用非线性方法生成线性不变式。计算机辅助验证：论文集，第 420 页 (2003) 29. Thomas, W.：无限对象上的自动机。在：van Leeuwen, J. (编)《理论计算机科学手册》B 卷，第 133–191 页。爱思唯尔 (1990) 30. Van De Meent, J.W., Paige, B., Yang, H., Wood, F.：概率编程导论。arXiv 预印本 arXiv:1809.10756 (2018) 31. Vardi, M.Y., Wolper, P.：程序自动验证的自动机理论方法。在：计算机科学逻辑研讨会论文集 (LICS)，第 332–344 页。IEEE (1986)。https://doi.org/10.1109/LICS.1986.1674816 32. Ville, J.：对集体概念的批判性研究 (1939) 33. Wang, P., Fu, H., Chatterjee, K., Deng, Y., Xu, M.：证明具有随机化的变量依赖终止时间的概率程序的期望敏感性。ACM 程序设计语言学报**4**(POPL), 25:1–25:30 (2020)。https://doi.org/10.1145/3371093

34. Wang, P., Fu, H., Goharshady, A.K., Chatterjee, K., Qin, X., Shi, W.：非确定性概率程序的成本分析。在：McKinley, K.S., Fisher, K. (编) ACM SIGPLAN 第 40 届编程语言设计与实现会议论文集，PLDI 2019，美国亚利桑那州凤凰城，2019年6月22日至26日。第 204–220 页。ACM (2019)。https://doi.org/10.1145/3314221.3314581, https: // doi.org/10 3314581 35 1145 3314221 . / . . Wang, P., Yang, T., Fu, H., Li, G., Ong, C.L.：通过多项式求解对贝叶斯概率编程进行静态后验推断。ACM 程序设计语言学报 **8**(PLDI), 1361–1386 (2024)。https://doi.org/10.1145/3656432, https://doi. org/10 3656432 36 1145. / . Watanabe, K., Junges, S., Rot, J., Hasuo, I.：定量时序推断中乘积构造的一种统一方法。ACM 程序设计语言会议论文集**9**(OOPSLA1), 1575–1603 (2025) 37. Williams, D.：鞅概率论。剑桥大学出版社 (1991) 38. Xue, B., Fränzle, M., Zhan, N.：对具有时变不确定性的多项式系统可达集进行内逼近。IEEE 自动控制汇刊**65**(4), 1468–1483 (2020) 39. Zaiser, F., Murawski, A.S., Ong, C.H.L.：循环离散概率程序后验分布的保证界。ACM 程序设计语言会议论文集**9**(POPL), 1104–1135 (2025)

附录

A 概率论

我们首先回顾概率论中的一些概念。

随机变量与随机过程。概率空间是一个三元组 $(\Omega, \mathcal{F}, \mathbb{P})$，其中 Ω 是非空样本空间，$\mathcal{F}$ 是定义在Ω上的 σ-代数，而 $\mathbb{P}(\cdot)$是定义在 $\mathcal{F}$上的概率测度，即满足以下性质的函数 $\mathbb{P}$: $\mathcal{F} \to [0,1]$：(1) $\mathbb{P}(\emptyset) = 0$，(2)$\mathbb{P}(\Omega - A) = 1 - \mathbb{P}[A]$，以及(3)$\mathbb{P}(\cup_{i=0}^{\infty} A_i) = \sum_{i=0}^{\infty} \mathbb{P}(A_i)$，其中 $\{A_i\}_{i=0}^{\infty}$ 是$\mathcal{F}$中任意一列两两不相交的集合。

给定概率空间 $(\Omega, \mathcal{F}, \mathbb{P})$，随机变量是一个函数 $X: \Omega \to \mathbb{R} \cup \{\infty\}$，且该函数是 $\mathcal{F}$-可测的；也就是说，对于每个 $a \in \mathbb{R}$，都有 $\{\omega \in \Omega | X(\omega) \leq a\} \in \mathcal{F}$。此外，离散时间随机过程是 $(\Omega, \mathcal{F}, \mathbb{P})$中随机变量构成的序列 $\{X_n\}_{n=0}^{\infty}$。

条件期望。设 $(\Omega, \mathcal{F}, \mathbb{P})$ 是一个概率空间，且 X 是 $(\Omega, \mathcal{F}, \mathbb{P})$ 上的随机变量。随机变量 X 的期望值记为 $\mathbb{E}[X]$，是 X 关于 $\mathbb{P}$ 的勒贝格积分。如果 X 的取值范围是一个可数集 A，那么 $\mathbb{E}[X] = \sum_{\omega \in A} \omega \cdot \mathbb{P}(X = \omega)$。给定一个子σ-代数$\mathcal{F}' \subseteq \mathcal{F}$，对于给定的 $\mathcal{F}'$，X 的条件期望是一个 $\mathcal{F}'$-可测随机变量 Y，满足对任意 $A \in \mathcal{F}'$，都有：

$$\mathbb{E}[X \cdot \mathbb{I}_A] = \mathbb{E}[Y \cdot \mathbb{I}_A] \tag{19}$$

这里，$\mathbb{I}_A: \Omega \to \{0,1\}$ 是 A的示性函数，定义为：若 $\omega \in A$，则 $\mathbb{I}_A(\omega) = 1$；若 $\omega \notin A$，则 $\mathbb{I}_A(\omega) = 0$。此外，只要条件期望存在，它也几乎必然唯一；也就是说，对于给定的 $\mathcal{F}'$，若 $\mathcal{F}'$-可测随机变量Y 和 Y' 都是 X 的条件期望，则有$\mathbb{P}(Y = Y') = 1$。

滤过与停时。概率空间 $(\Omega, \mathcal{F}, \mathbb{P})$ 的一个滤过是一个无限序列 $\{\mathcal{F}_n\}_{n=0}^{\infty}$，满足对于每个 n，三元组 $(\Omega, \mathcal{F}_n, \mathbb{P})$ 都是一个概率空间，且 $\mathcal{F}_n \subseteq \mathcal{F}_{n+1} \subseteq \mathcal{F}$。相对于滤过 $\{\mathcal{F}_n\}_{n=0}^{\infty}$ 的停时是一个随机变量 $T: \Omega \to \mathbb{N}_0 \cup \{\infty\}$，满足对于每个$i \in \mathbb{N}_0$，都有 $\{\omega \in \Omega | T(\omega) \leq i\} \in \mathcal{F}_i$。直观来说，$T$ 返回某个随机过程表现出所需行为并应当“停止”的时间步。

离散时间随机过程 $\{X_n\}_{n=0}^{\infty}$在 $(\Omega, \mathcal{F}, \mathbb{P})$ 中适应于滤过 $\{\mathcal{F}_n\}_{n=0}^{\infty}$，如果对于所有 $n \geq 0$，X_n都是 $(\Omega, \mathcal{F}_n, \mathbb{P})$ 中的一个随机变量。

停止过程。设 $\{X_n\}_{n=0}^{\infty}$ 是适应于滤过$\{\mathcal{F}_n\}_{n=0}^{\infty}$ 的随机过程，且 T 是相对于 $\{\mathcal{F}_n\}_{n=0}^{\infty}$的停时。停止过程 $\tilde{}\{X_n\}_{n=0}^{\infty}$ 定义为

$$\tilde{X}_n = \begin{cases} X_n, & \text{for } n < T, \\ X_T, & \text{for } n \geq T. \end{cases}$$

鞅。相对于滤过 $\{\mathcal{F}_n\}_{n=0}^{\infty}$的离散时间随机过程 $\{X_n\}_{n=0}^{\infty}$ 称为鞅（分别称为上鞅、下鞅），若对所有 $n \geq 0$， $\mathbb{E}[|X_n|] < \infty$ 均成立，且几乎必然（即以概率 1）有 $\mathbb{E}[X_{n+1}|\mathcal{F}_n] = X_n$（分别为 $\mathbb{E}[X_{n+1}|\mathcal{F}_n] \leq X_n$、 $\mathbb{E}[X_{n+1}|\mathcal{F}_n] \geq X_n$）。

定理 7（可选停止定理（OST） [37]）。考虑相对于滤过 $\{\mathcal{F}_n\}_{n=0}^{\infty}$ 的停止时间 T，以及适应于 $\{\mathcal{F}_n\}_{n=0}^{\infty}$ 的鞅（分别为超鞅、下鞅） $\{X_n\}_{n=0}^{\infty}$。那么，如果满足以下任一条件，则有 $\mathbb{E}[|X_T|] < \infty$ 和$\mathbb{E}[X_T] = \mathbb{E}[X_0]$ （分别为 $\mathbb{E}[X_T] \leq \mathbb{E}[X_0]$、 $\mathbb{E}[X_T] \geq \mathbb{E}[X_0]$）：

– T 有界，即存在某个常数 c，使得 $T < c$；– $\mathbb{E}[T] < \infty$，且存在常数 c，使得对所有 $n \in \mathbb{N}$， $|X_{n+1} - X_n| \leq c$；~– 相对于 T 的停止过程 $\{X_n\}_{n=0}^{\infty}$ 有界，即存在某个常数 c，使得对所有 $n \in \mathbb{N}$， $|X_n| \leq c$。

定理 8（Ville 不等式 [32]）。对于任意非负上鞅$\{X_n\}_{n=0}^{\infty}$ 和任意实数 $c > 0$,

$$\mathbb{P}[\sup_{n\geq 0} X_n \geq c] \leq \frac{\mathbb{E}[X_0]}{c}.$$

此定理也称为 Doob 非负上鞅不等式。

B 第 3 节的补充材料

命题 1 $\Pi \otimes \mathcal{A}_{\varphi}^{U}$ $U = \emptyset$ $\theta[2]$ $\cap$给定一个 FOV 乘积， $\theta \in \Theta$ $max\ \theta[3] < \infty$ 是一个 $\theta \in \Theta$ FOV 集，即对于任意乘积轨迹，Inf( )，当且仅当对于任意，( )。

证明。显然，在 FOV 乘积中，对于任意乘积轨迹 $\theta \in \Theta$， $max(\theta[3]) < \infty$ 蕴含 $\text{Inf}(\theta[2]) \cap U = \emptyset$，反之亦然。□

命题 2 $\Pi \otimes \mathcal{A}_{\varphi}^{U}$ $U \neq \emptyset$ $\theta[2]$ $\cap$给定一个 IOV 乘积， $\theta \in \Theta$ $max\ \theta[3] < \infty$ 是一个 $\theta \in \Theta$ IOV 集，即对于任意乘积轨迹，Inf( )，当且仅当对于任意，( )。

证明。 不难看出，在 IOV 乘积中，对于任意乘积轨迹$\theta \in \Theta$， $max(\theta[3]) < \infty$ 蕴含 $\text{Inf}(\theta[2]) \cap U = \emptyset$，反之亦然。□

推论 1 如果对于 FOV 乘积 $\Pi \otimes \mathcal{A}_{\varphi}^{E_i}$ 中的任意 $\theta \in \Theta$， $max(\theta[3]) < \infty$，那么 E_i 是一个 FOV 集。如果对于 IOV 乘积$\Pi \otimes \mathcal{A}_{\varphi}^{F_i}$中的任意 $\theta \in \Theta$， $max(\theta[3]) < \infty$，那么 F_i 是一个 IOV 集。最后，可以得出 $\Pi \models \varphi$。

证明。 根据命题 1 和 2，可以证明 E_i 是一个 FOV 集，且 F_i 是一个 IOV 集。因此，根据第 2.1 节中的 Rabin 接受条件，可以得出 Π 满足 ω-正则性质 φ。

定理 1（关于 k-时间 FOV 集的下界）。假设存在一个 FOV 乘积 $\Pi \otimes \mathcal{A}_\varphi^U$ 的屏障证书（BC） $\eta\colon\ S \times Q \times \mathbb{N} \to \mathbb{R}$，使得对于两个常数 $\gamma \in (0,1)$ 和 $k \in \mathbb{N}_0$，以下条件成立：

$$\eta(s,q,l) \geq 0 \qquad \forall s \in S, q \in Q, l \in \mathbb{N}_0 \qquad (2)$$
$$\eta(s,q_0,0) \leq \gamma \qquad \forall s \in S_0 \qquad (3)$$
$$\eta(s,q,k+1) \geq 1 \qquad \forall s \in S, q \in U \qquad (4)$$
$$\mathbb{E}_{\mathbf{r}\sim\mathcal{D}}[\eta(g(s,\mathbf{r}),q',l')] \leq \eta(s,q,\ell) \qquad \forall s \in S, q \in Q, l \in [0,k] \qquad (5)$$

其中 $l' = l+1$ 若 $q' \in U$，否则为 l。那么，对于任意初始乘积状态 $(s_0,\ q_0,\ 0)$，其中 $s_0 \in S_0$，我们有 $\mathbb{P}_{s_0}[U$ 是一个 k-时间 FOV 集$] \geq 1 - \eta(s_0,\ q_0,\ 0) =: l_i^{fin}$。

证明。令 Ω 为由 FOV 乘积 $\Pi \otimes \mathcal{A}_\varphi^U$ 诱导的所有轨迹的集合。构造一个定义在 Ω 上的随机过程 $\{X_t\}_{t\geq 0}$，使得对于任意 $\omega \in \Omega$，都有 $X_t(\omega) = \eta(\omega_t) = \eta(s_t,\ q_t,\ \ell_t)$。令 κ 为 U 首次被访问 $k+1$ 次的时刻，即 $\kappa(\omega) := \inf\{t \in \mathbb{N} \mid \ell_t = k+1\}$。然后，我们构造如下停止过程 $\tilde{}\{X_t\}_{t\geq 0}$

$$\tilde{X}_t = \begin{cases} X_t, & \text{if } t < \kappa, \\ X_\kappa, & \text{if } t \geq \kappa. \end{cases}$$

$\tilde{}$接下来，我们将证明 $\{X_t\}_{t\geq 0}$ 是一个非负上鞅。当 $t < \kappa$ 时，我们有

$$\mathbb{E}[\tilde{X}_{t+1} \mid \tilde{\mathcal{F}}_t] = \mathbb{E}[X_{t+1} \mid \mathcal{F}_t] \leq X_t = \tilde{X}_t,$$

其中，该不等式由条件 (5) 得出。当 $t \geq \kappa$ 时，我们有

$$\mathbb{E}[\tilde{X}_{t+1} \mid \tilde{\mathcal{F}}_t] = X_\kappa = \tilde{X}_\kappa.$$

$\tilde{}$根据条件 (2)，我们可以得出 $\{X_t\}_{t\geq 0}$ 是一个非负超鞅。根据条件 (4)，当 $q_t \in U$ 且 $\ell_t = k+1$ 时，我们有 $X_t(\omega) = \eta(s_t,\ q_t,\ \ell_t) \geq 1$。因此，对于每个初始状态 $(s_0,\ q_0,\ \ell_0)$，我们有

$$\begin{aligned} & 1 - \mathbb{P}_{s_0}[U \text{ is visited at most } k \text{ times}] \\ &= \mathbb{P}_{s_0}[U \text{ is visited more than } k \text{ times}] \\ &= \mathbb{P}_{s_0}[\{(s_t,q_t,\ell_t)\}_{t=0}^{\infty} \text{ where } \exists t \in \mathbb{N}.\ q_t \in E_i \text{ and } \ell_t = k+1] \\ &\leq \mathbb{P}_{s_0}\left[\sup_{t\in\mathbb{N}} X_t(\omega) \geq 1\right] = \mathbb{P}_{s_0}\left[\sup_{t\in\mathbb{N}} \tilde{X}_t(\omega) \geq 1\right] \\ &\leq \tilde{X}_0(\omega) = X_0(\omega) \end{aligned}$$

其中，最后一个不等式由 Ville 不等式（见定理 8）得出。 □

定理 2（关于 k-时间 FOV 集的上界）。假设存在一个屏障证书 $\eta\colon$ $S \times Q \times \mathbb{N} \to \mathbb{R}$，属于 FOV 乘积 $\Pi \otimes \mathcal{A}_\varphi^U$，使得

对于某些常数 $\alpha \in (0,1)$、 $0 \le \lambda < \gamma \le 1$ 和 $k \in \mathbb{N}$，以下条件成立：

$$0 \le \eta(s,q,l) \le 1 \qquad \forall s \in S, q \in Q, l \in \mathbb{N}_0 \tag{6}$$

$$\eta(s,q_0,0) \ge \gamma \qquad \forall s \in S_0 \tag{7}$$

$$\eta(s,q,k+1) \le \lambda \qquad \forall s \in S, q \in U \tag{8}$$

$$\alpha \cdot \mathbb{E}_{\mathbf{r}\sim\mathcal{D}}[\eta(g(s,\ \mathbf{r})\ q',\ l')] \ge \eta(s,\ q,\ \ell) \qquad \forall s \in S, q \in Q, l \in [0,k] \tag{9}$$

其中 $l' = l+1$ 若 $q' \in U$ 且 l 否则。因此，对于任意满足 $s_0 \in S_0$ 的初始乘积状态 $(s_0,\ q_0,\ 0)$，我们有 $\mathbb{P}_{s_0}[U$ 是一个 k 次 FOV 集$] \le 1-\eta(s_0,\ q_0,\ 0) =: u_i^{fin}$。

证明。令 Ω 为 FOV 乘积 $M_\mu \otimes \mathcal{A}_\varphi^U$ 所诱导的所有轨迹的集合。构造定义在 Ω 上的随机过程 $\{X_t\}_{t\ge 0}$，使得对于任意 $\omega \in \Omega$，$X_t(\omega) = \eta(\omega_t) = \eta(s_t,\ q_t,\ \ell_t)$。令 κ 为 U 被访问 $k+1$ 次的首次时刻，即 $\kappa(\omega) := \inf\{t \in \mathbb{N} \mid \ell_t = k+1\}$。然后构造一个新的随机过程$\{Y_t\}_{t\ge 0}$，使得 $Y_t := \alpha^t X_t$。将其停止过程 $\{\tilde{Y}_t\}_{t\ge 0}$ 定义为

$$\tilde{Y}_t = \begin{cases} Y_t, & \text{if } t < \kappa, \\ Y_\kappa, & \text{if } t \ge \kappa. \end{cases}$$

˜接下来，我们将证明 $\{Y_t\}_{t\ge 0}$ 是一个下鞅。当 $t < \kappa$时，我们有

$$\begin{aligned} \mathbb{E}[\tilde{Y}_{t+1} \mid \tilde{\mathcal{F}}_t] &= \mathbb{E}[Y_{t+1} \mid \mathcal{F}_t] \\ &= \mathbb{E}[\alpha^{t+1} X_{t+1} \mid \mathcal{F}_t] = \alpha^{t+1}\mathbb{E}[X_{t+1} \mid \mathcal{F}_t] \\ &= \alpha^t \cdot \alpha \mathbb{E}[X_{t+1} \mid \mathcal{F}_t] \ge \alpha^t X_t = \tilde{Y}_t \end{aligned}$$

其中，不等式由条件 (9) 得出。当 $t \ge \kappa$时，我们有

$$\mathbb{E}[\tilde{Y}_{t+1} \mid \tilde{\mathcal{F}}_t] = Y_\kappa = \tilde{Y}_t$$

˜根据条件 (6)，对于任意 $t \in \mathbb{N}$，我们有 $Y_t \in [0,1]$。因此，我们可以得出˜$\{Y_t\}_{t\ge 0}$ 是一个下鞅。于是，对于每个初始状态 (s_0, q_0, ℓ_0)，我们有

$$\begin{aligned} & 1 - \mathbb{P}_{s_0}[U \text{ is visited at most } k \text{ times}] \\ &= \mathbb{P}_{s_0}[U \text{ is visited more than } k \text{ times}] \\ &= \mathbb{P}_{s_0}[\{(s_t,q_t,\ell_t)\}_{t=0}^\infty \text{ where } \exists t \in \mathbb{N}.\ q_t \in E_i \text{ and } \ell_t = k+1] \\ &= \mathbb{P}_{s_0}[\kappa < \infty] \\ &\ge \mathbb{E}[\alpha^\kappa \cdot X_\kappa \mid \kappa < \infty] \cdot \mathbb{P}_{s_0}[\kappa < \infty] \\ &= \mathbb{E}[\alpha^\kappa \cdot X_\kappa \mid \kappa < \infty] \cdot \mathbb{P}_{s_0}[\kappa < \infty] + \mathbb{E}[\alpha^\kappa \cdot X_\kappa \mid \kappa = \infty] \cdot \mathbb{P}_{s_0}[\kappa = \infty] \\ &= \mathbb{E}[\alpha^\kappa \cdot X_\kappa] = \mathbb{E}[Y_\kappa] = \mathbb{E}[\tilde{Y}_\kappa] \ge \mathbb{E}[\tilde{Y}_0] = X_0 \end{aligned}$$

其中，第一个不等式是根据以下事实推导得出的：$\alpha^\kappa \cdot X_\kappa \in (0,\ 1)$，且 $\alpha \in (0,\ 1)$，并且 $X_\kappa \in [0,1]$ 由条件 (6) 可知；第四个等式是根据以下事实得出的：当 $\kappa = \infty$ 且 $\alpha \in (0,\ 1)$时，$\alpha^\kappa \cdot X_\kappa = 0$；最后一个不等式则是应用可选停止定理定理 7 得出的。□

定理 3（ k-时间 IOV 集的下界）。假设存在 IOV 乘积 $\Pi \otimes \mathcal{A}_{\varphi}^{U}$ 的屏障证书 h: $S \times Q \times \mathbb{N} \to \mathbb{R}$，使得对于两个常数 $\gamma \in (0,\ 1)$ 和 $k \in \mathbb{N}$，以下条件成立:

$$h(s,q,l) \geq 0 \qquad \forall s \in S, q \in Q, l \in \mathbb{N}_0 \qquad (10)$$

$$h(s,q_0,0) \leq \gamma \qquad \forall s \in S_0 \qquad (11)$$

$$h(s,\ q,\ k+1) \geq 1 \qquad \forall s \in S, q \in Q \setminus U \qquad (12)$$

$$\mathbb{E}_{\mathbf{r}\sim\mathcal{D}}[h(g(s,\mathbf{r}),q',l')] \leq h(s,q,l) \qquad \forall s \in S, q \in Q, l \in [0,k] \qquad (13)$$

其中 $l' = 0$ 若 $q' \in U$ 且 $l' = l+1$ 否则。于是，对于任意满足 $s_0 \in S_0$ 的初始乘积状态 $(s_0,\ q_0,\ 0)$，有 $\mathbb{P}_{s_0}[U$ 是一个 k 次 IOV 集$] \geq 1 - h(s_0,\ q_0,\ 0) =: l_i^{inf}$。

证明。令 Ω 为由 IOV 乘积 $M_\mu \otimes \mathcal{A}_{\varphi}^{U}$ 所诱导的所有轨迹的集合。构造定义在 Ω 上的随机过程 $\{X_t\}_{t\geq 0}$，使得对于任意 $\omega \in \Omega$，$X_t(\omega) = h(\omega_t) = h(s_t,\ q_t,\ \ell_t)$。令 κ 为 $Q \setminus U$ 连续被访问 $k+1$ 次的首次时刻，即 $\kappa(\omega) := \inf\{t \in \mathbb{N} \mid \ell_t = k+1\}$。然后定义停止的˜过程 $\{X_t\}_{t\geq 0}$ 如下

$$\tilde{X}_t = \begin{cases} X_t, & \text{if } t < \kappa, \\ X_\kappa, & \text{if } t \geq \kappa. \end{cases}$$

˜接下来，我们将证明 $\{X_t\}_{t\geq 0}$ 是一个非负上鞅。当 $t < \kappa$ 时，我们有

$$\mathbb{E}[\tilde{X}_{t+1} \mid \tilde{\mathcal{F}}_t] = \mathbb{E}[X_{t+1} \mid \mathcal{F}_t] \leq X_t = \tilde{X}_t,$$

其中，不等式是由条件 (13) 得出的。当 $t \geq \kappa$ 时，我们有

$$\mathbb{E}[\tilde{X}_{t+1} \mid \tilde{\mathcal{F}}_t] = X_\kappa = \tilde{X}_\kappa.$$

˜根据条件 (10)，我们可以得出 $\{X_t\}_{t\geq 0}$ 是一个非负上鞅。根据条件 (12)，当 $q_t \in Q \setminus F_i$ 且 $\ell_t = k+1$ 时，我们有 $X_t(\omega) = h(s_t,\ q_t,\ \ell_t) \geq 1$。因此，对于每个初始状态 $(s_0,\ q_0,\ \ell_0)$，我们有

$$\begin{aligned} & 1 - \mathbb{P}_{s_0}[Q \setminus U \text{ is visited consecutively at most } k \text{ times}] \\ &= \mathbb{P}_{s_0}[Q \setminus U \text{ is visited consecutively more than } k \text{ times}] \\ &= \mathbb{P}_{s_0}[\{(s_t,q_t,\ell_t)\}_{t=0}^{\infty} \text{ where } \exists t \in \mathbb{N}.\ q_t \in Q \setminus F_i \text{ and } \ell_t = k+1] \\ &\leq \mathbb{P}_{s_0}\left[\sup_{t\in\mathbb{N}} X_t(\omega) \geq 1\right] = \mathbb{P}_{s_0}\left[\sup_{t\in\mathbb{N}} \tilde{X}_t(\omega) \geq 1\right] \\ &\leq \tilde{X}_0(\omega) = X_0(\omega) \end{aligned}$$

其中，最后一个不等式由 Ville 不等式定理 8 得出。 □

定理 4（ k时间 IOV 集的上界）。假设存在一个屏障证书 h： $S \times Q \times \mathbb{N} \to \mathbb{R}$，它对应于 IOV 乘积 $\Pi \otimes \mathcal{A}_{\varphi}^{U}$，满足

对于某些常数 $\gamma \in (0,\ 1)$、$0 \le \lambda < \gamma \le 1$ 和 $k \in \mathbb{N}$，以下条件成立：

$$
\begin{aligned}
&0 \le h(s,q,l) \le 1 && \forall s \in S, q \in Q, l \in \mathbb{N}_0 && (14)\\
&h(s,q_0,0) \ge \gamma && \forall s \in S_0 && (15)\\
&h(s,q,k+1) \le \lambda && \forall s \in S, q \in Q \setminus U && (16)\\
&\alpha \cdot \mathbb{E}_{\mathbf{r}\sim\mathcal{D}}[h(g(s,\mathbf{r}),q',l')] \ge h(s,q,l) && \forall s \in S, q \in Q, l \in [0,k] && (17)
\end{aligned}
$$

其中 $l' = 0$ 若 $q' \in U$ 且 $l' = l+1$ 否则。因此，对于任意满足 $s_0 \in S_0$ 的初始乘积状态 $(s_0, q_0, 0)$，我们有 $\mathbb{P}_{s_0}[U$ 是一个 k-时间 IOV 集$] \le 1 - h(s_0, q_0, 0) =: u_i^{inf}$。

证明。令 Ω 为由 IOV 乘积 $M_\mu \otimes \mathcal{A}_\varphi^U$ 诱导的所有轨迹所构成的集合。构造一个定义在 Ω 上的随机过程 $\{X_t\}_{t\ge 0}$，使得对于任意 $\omega \in \Omega$，$X_t(\omega) = h(\omega_t) = h(s_t, q_t, \ell_t)$。令 κ 为 $Q \setminus U$ 连续被访问 $k+1$ 次的首次时刻，即 $\kappa(\omega) := \inf\{t \in \mathbb{N} \mid \ell_t = k+1\}$。然后构造一个新的随机过程 $\{Y_t\}_{t\ge 0}$，使得 $Y_t := \alpha^t X_t$。将其停止过程定义为 $\{Y_t\}_{t\ge 0}$：

$$\tilde{Y}_t = \begin{cases} Y_t, & \text{if } t < \kappa, \\ Y_\kappa, & \text{if } t \ge \kappa. \end{cases}$$

接下来，我们将证明 $\{Y_t\}_{t\ge 0}$ 是一个下鞅。当 $t < \kappa$ 时，我们有

$$
\begin{aligned}
\mathbb{E}[\tilde{Y}_{t+1} \mid \tilde{\mathcal{F}}_t] &= \mathbb{E}[Y_{t+1} \mid \mathcal{F}_t] \\
&= \mathbb{E}[\alpha^{t+1} X_{t+1} \mid \mathcal{F}_t] = \alpha^{t+1}\mathbb{E}[X_{t+1} \mid \mathcal{F}_t] \\
&= \alpha^t \cdot \alpha \mathbb{E}[X_{t+1} \mid \mathcal{F}_t] \ge \alpha^t X_t = \tilde{Y}_t
\end{aligned}
$$

其中，不等式是由条件 (17) 得出的。当 $t \ge \kappa$ 时，我们有

$$\mathbb{E}[\tilde{Y}_{t+1} \mid \tilde{\mathcal{F}}_t] = Y_\kappa = \tilde{Y}_t$$

根据条件 (14)，对于任意 $t \in \mathbb{N}$，我们有 $Y_t \in [0,1]$。因此，可以得出 $\{Y_t\}_{t\ge 0}$ 是一个下鞅。于是，对于每个初始状态（s_0，q_0，ℓ_0），我们有

$$
\begin{aligned}
&1 - \mathbb{P}_{s_0}[Q \setminus U \text{ is visited consecutively at most } k \text{ times}] \\
&= \mathbb{P}_{s_0}[Q \setminus U \text{ is visited consecutively more than } k \text{ times}] \\
&= \mathbb{P}_{s_0}[\{(s_t,q_t,\ell_t)\}_{t=0}^{\infty} \text{ where } \exists t \in \mathbb{N}.\ q_t \in Q \setminus F_i \text{ and } \ell_t = k+1] \\
&= \mathbb{P}_{s_0}[\kappa < \infty] \\
&\ge \mathbb{E}[\alpha^\kappa \cdot X_\kappa \mid \kappa < \infty] \cdot \mathbb{P}_{s_0}[\kappa < \infty] \\
&= \mathbb{E}[\alpha^\kappa \cdot X_\kappa \mid \kappa < \infty] \cdot \mathbb{P}_{s_0}[\kappa < \infty] + \mathbb{E}[\alpha^\kappa \cdot X_\kappa \mid \kappa = \infty] \cdot \mathbb{P}_{s_0}[\kappa = \infty] \\
&= \mathbb{E}[\alpha^\kappa \cdot X_\kappa] = \mathbb{E}[Y_\kappa] = \mathbb{E}[\tilde{Y}_\kappa] \ge \mathbb{E}[\tilde{Y}_0] = X_0
\end{aligned}
$$

其中，第一个不等式是由以下事实推得：$\alpha^\kappa \cdot X_\kappa \in (0,\ 1)$，且当 $\alpha \in (0,\ 1)$ 时，以及由条件 (14) 可得 $X_\kappa \in [0,1]$；第四个等式则是根据以下事实得出的

即当 $\kappa = \infty$ 且 $\alpha \in (0, 1)$ 时， $\alpha^{\kappa} \cdot X_{\kappa} = 0$ ；最后一个不等式是通过应用可选停止定理定理 7 得出的。□

定理 5（收敛性）。对于任意初始状态 $s_0 \in S_0$，当 $k \to m^*$ 属于定理 1 和定理 2 时，我们有 $\mathbb{P}_{s_0}[E_i$ 是一个 FOV 集$] \in [l_i^{fin}, u_i^{fin}]$；当 $k \to n^*$ 属于定理 3 和定理 4 时，我们有 $\mathbb{P}_{s_0}[F_i$ 是一个 IOV 集$] \in [l_i^{inf}, u_i^{inf}]$。因此，
$\mathbb{P}_{s_0}[\Pi \models \varphi] \in [l_i^{fin} \cdot l_i^{inf}, u_i^{fin} \cdot u_i^{inf}]$。

证明。证明很直接。当 k 足够大时，我们将统计所有有效轨迹的贡献。

C 第 5 节补充材料

$x \sim$ 伯努利分布(0.3)； $y := 0$;
当翻转(0.5)时执行
  如果翻转(0.6)，则
    $x := 1 - x$;
  如果 $x = 1$ ，则
    $y := y + 1$;
od

(a) RE 1

$x := 0$； $y := 0$;
当 $x = 0$ 时
  $n := n + 1$;
  如果 flip(0.5) 则
    $x := 1 - x$;
od

(b) RE 2

图 2：新颖示例