arXiv:2302.06082v1 [cs.LO] 13 Feb 2023

下界　可能发散的概率程序

SHENGHUA FENG,SKLCS，软件研究所，中国科学院大学，中国MINGSHUAI CHEN†，浙江大学，中国HAN SU，SKLCS，软件研究所，中国科学院大学，中国BENJAMIN LUCIEN KAMINSKI，萨尔兰大学，萨尔兰信息学园区，德国及伦敦大学学院，英国JOOST-PIETER KATOEN，亚琛工业大学，德国NAIJUN ZHAN，SKLCS，软件研究所，中国科学院大学，中国

我们提出了一种新的证明规则，用于验证概率程序中各种量的下界。与现有规则一样，该证明规则并不局限于几乎必然终止程序；它可用于为可能发散的概率循环（例如格点上的著名三维随机游走）的终止概率和期望值等建立非平凡下界。

CCS 概念：　• **计算理论** → **程序推理**；• **计算数学** → **概率** **概率算法**　；**随机过程**。

附加关键词和短语：概率程序、定量验证、最弱前期望、下界、几乎必然终止、一致可积性

1 引言

概率程序 [Gordon 等，2014；Kozen，1981；Saheb-Djahromi，1978；van de Meent 等人 2018] 通过随机行为扩展确定性程序，例如随机采样、概率选择和条件化（通过后验观测）。概率程序已在众多领域得到广泛应用：它们为自主机器人和自动驾驶汽车提供控制 [Evans 等，2017；Shamsi 等人 2020]，是描述安全 [Barthe 等人 2013] 和量子 [Ying 2011]机制的关键，能够将随机化算法直接编码其中，用于解决 NP 难问题，甚至是确定性方法无法解决的问题（例如分布式计算中的问题 [Aspnes 和 Herlihy，1990；Schneider1993]），并且是现代机器学习和近似计算的核心 [Carbin 等人2016]。关于概率编程的最新进展，参见 [Barthe 等人 2020] 。

概率程序虽然通常规模较小，却很难理解：概率编程的核心，是将看起来寻常的程序视为概率分布 [Hicks 2014；Saheb-Djahromi 1978]。这种从确定性程序状态到（定义在状态上的）可能具有无限支撑的分布的提升，使概率程序的验证问题出了名地困难 [Kaminski 等人 2019]。具体而言，给定一个随机变量 f（将程序状态映射为数值），一项关键的验证任务是推理程序 C 在输入 σ上终止后 f的期望值。如果 f是事件 A的示性函数，那么该期望值就是 C终止时 A 发生的概率。对于可能不终止的循环程序 C，f的期望值通常刻画为某个单调算子的最小不动点，该算子用于表达 C 关于 f的语义。因此，计算 f 的精确期望值，就相当于推断其最小不动点，而这通常极难处理。

†通讯作者

作者地址：Shenghua Feng，SKLCS，软件研究所，中国科学院大学，中国北京，fengsh@ios.ac.cn；Mingshuai Chen，浙江大学，中国杭州，m.chen@zju.edu.cn；Han Su，SKLCS，软件研究所，中国科学院大学，中国北京，suhan@ios.ac.cn；Benjamin Lucien Kaminski，b. kaminski@ucl.ac.uk，萨尔兰大学，萨尔信息学园区，德国萨尔布吕肯，伦敦大学学院，英国伦敦；Joost-Pieter Katoen，亚琛工业大学，德国亚琛，katoen@cs.rwth-aachen.de；Naijun Zhan，SKLCS，软件研究所，中国科学院大学，中国北京，znj@ios.ac.cn。

因此，现有针对概率循环的验证技术大多致力于证明期望值（即最小不动点）的上界和/或下界。证明下界对于确立概率程序的完全正确性尤为重要 [Katoen 等人 2015; McIver 和 Morgan 2001]，也有助于评估上界的质量和紧确性。要验证一个候选上界 u，众所周知的*Park* 归纳 [Kozen 1985; Park 1969], 或更一般的 κ-归纳 [Batz 等人 2021a], , 只需“将其 u 通过循环语义传递”一次即可。而对于最小不动点的下界，Park 归纳的“对偶”版本则不可靠（参见第 4.3 节）。

现有的（可靠）概率程序下界归纳规则仅适用于以下两种情况：(i) 有界随机变量，且已知程序的终止概率的先验知识 [McIver 和 Morgan 2005]；或 (ii)（对所有输入均）几乎必然终止（AST）的程序（即在所有输入下都以概率 1 终止），以及一致可积的随机变量——这是随机过程中的一个概念，需要对循环时间和/或随机变量的界进行推理 [Hark 等人 2020]。与用于上界的Park归纳不同，应用这些下界归纳规则需要付出大量证明工作，例如寻找超鞅 [Chatterjee 等人2020]，以证明几乎必然终止、检验一致可积性并推断终止概率。尤其是，这些规则都无法推断严格小于 *1* 的终止概率下界，即针对非几乎必然终止（又称发散）程序的下界。举例来说，考虑以下概率循环 C_{3dsrw}，它对著名的三维（*3-D*）随机游走进行了建模，该随机游走定义在 $\mathbb{Z}^3$上的格点上。[1]

$$C_{\text{3dsrw}}\text{: while } (\ x \neq 0 \vee y \neq 0 \vee z \neq 0\ )\ \{\quad x \coloneqq x-1 \ \oplus\ x \coloneqq x+1 \ \oplus\ y \coloneqq y-1 \ \oplus\ y \coloneqq y+1 \ \oplus\ z \coloneqq z-1 \ \oplus\ z \coloneqq z+1 \}\ .$$

其内在的随机性 C_{3dsrw} 本质上不同于一维和二维情形：波利亚 [1921] 证明了，这种随机游走返回原点$\mathcal{P}$ 的概率(0,0,0)严格小于 1，这表明 C_{3dsrw} 不会几乎必然终止。更准确地说，从原点的任意一个相邻位置出发，C_{3dsrw} 的终止概率为

$$\mathcal{P} \;=\; 1 - \left(\frac{3}{(2\pi)^3} \int_{-\pi}^{\pi}\int_{-\pi}^{\pi}\int_{-\pi}^{\pi} \frac{\mathrm{d}x\,\mathrm{d}y\,\mathrm{d}z}{3-\cos x-\cos y-\cos z} \right)^{-1} \;=\; 0.3405373296\ldots \qquad (\dagger)$$

现有验证技术无法处理 C_{3dsrw}，因为其发散的性质十分复杂。

本文提出了一条新的证明规则，称为守卫强化规则，用于验证可能无界随机变量 f 在可能发散的概率循环 $C_{\text{loop}} = \text{while } (\ \varphi\ )\ \{C\}$ 终止后的期望值下界。该证明规则采用归约方法：假设我们要证明 l 是 f 在 C_{loop}终止后的期望值下界。我们首先通过强化循环守卫条件 φ，将其改为 φ'，从而由 C_{loop} 构造出一个新的循环 $C'_{\text{loop}} = \text{while } (\ \varphi'\ )\ \{\ C\}$，将问题归约为一个更容易处理的问题，其中 (i) 修改后的循环 C'_{loop} 具有更强的终止性质（例如，可证明几乎必然终止），且 (ii) 更容易验证 l 的一致可积性和有界性条件。接着，我们的证明规则利用最弱前期望演算 [Kozen 1985; McIver 和 Morgan 2005]，通过考察 C'_{loop} 与 C_{loop} 相对于f的“差异”，断言：若 l 是 C'_{loop} 的下界（相对于受限形式的 f），则它也足以作为 C_{loop} 的下界（相对于 f）。由于守卫强化，前者可凭借 (i) 和 (ii)，通常通过应用前述下界归纳规则来证明；若 C'_{loop} 具有有限状态空间，则也可通过概率模型检测来证明 [Baier 和 Katoen 2008; Katoen 2016; Kwiatkowska 2003]。在这种情况下，我们的证明规则可以（部分）自动化，从而推导出越来越紧的下界；例如，对于 (†) 中三维随机游走的终止概率 P，可以随着 φ' “趋近” φ 而不断改进下界，详见例 24。

本文的主要结果如下：

[1]迭代符号 $\oplus$ 是离散均匀选择的简写（在此情况下，每种选择的概率均为 1/6）。

(a) 我们通过守卫强化提出了一条新的证明规则，用于验证概率程序期望值的下界。据我们所知，这是首条允许发散的概率循环具有无界期望值的下界规则。(b) 我们表明，经过守卫强化的修改后的循环具有易于证明的几乎必然终止性和一致可积性。这使现有的下界证明规则更易于应用，适用范围也更广；此外，我们提出了一条新颖的充分判据，用于证明一致可积性，并能识别出基于可选停止定理的现有充分条件无法涵盖的情形 [Hark 等人 2020]。(c) 我们证明，守卫强化技术引入的近似误差可以任意小，从而得到紧确的下界。(d) 我们指出了一些情形，在这些情形中，我们的证明规则可通过对无限状态概率程序进行模型检验，推断其定量性质；所用模型为有限状态概率模型。

我们通过一系列示例展示该证明规则的有效性，其中包括三维随机游走和一个真实世界中的随机化网络协议。

论文结构。第 2 节通过一个简单示例概述我们的方法。第 3 节回顾最弱前期望（最弱前置条件）演算，将其作为我们的语义基础。我们在第 4 节中形式化我们的问题，并将其置于现有证明规则的背景下。在第 5 节中，我们利用最弱前置条件循环之间的差异，由此得出第6 节中的下界规则。我们在第 7 节中通过案例研究展示证明规则的有效性。我们在第 8 节中讨论守卫强化原理的局限性，在第 9 节中讨论相关工作，并在第 10 节中总结全文。测度论中的基本概念，例如（次）概率测度、随机变量、（停止）随机过程和停时，介绍于附录A。补充背景资料、详细证明以及示例细节见附录 B至D，依次对应。

2 我们的方法概述

简而言之，我们的想法是将给定的潜在非几乎必然终止循环 C_{loop} 转换为一个可证明几乎必然终止的循环 C'_{loop}，然后为 C'_{loop}证明下界。我们的转换方式保证了 C'_{loop} 的期望结果是 C_{loop}期望结果的一个下界。因此，正如我们的证明规则所编码的那样， C'_{loop} 的一个下界足以作为 C_{loop}的下界。

下面通过分析概率循环中最基本的期望结果之一——终止，来演示我们的方法。考虑一维随机游走 C_{1dbrw}，其位于 $\mathbb{Z}$（如下方左侧所示），以有偏的概率 $1/3$ 向左移动，并以概率 $2/3$ 向右移动。由于其具有偏向性，该循环不会几乎必然终止，并且现有的证明规则中没有任何一条[2]足以为其终止概率建立非平凡下界；详情请参见例16。

C_{1dbrw}： while循环 $(0 < n)\{C^{M}_{\text{1dbrw}}$： while循环 $(0 < n < M)\{n := n - 1\ [1/3]\ n := n + 1$ $n := n - 1\ [1/3]\ n := n + 1\}$
$\}$

右上方展示了该循环的修改版本 C^{M}_{1dbrw}，它是从 C_{1dbrw} 中得到的：通过在循环守卫中引入 $M \in \mathbb{N}$ 人为上界 n 。该修改后的循环会几乎必然终止，而且最多只能访问有限多个不同的状态。

C^{M}_{1dbrw} 通过“到达”而终止 $n \leq 0$ 或 $n \geq M$。关键观察是，在 C^{M}_{1dbrw}处终止的 $n \leq 0$ 概率小于 C_{1dbrw}的终止概率，因为 C_{1dbrw} 中有些终止程序轨迹（它们对其终止概率有贡献）在 C^{M}_{1dbrw} 中因人为设置的“屏障” M而不再可能；示意见图 1 。与此同时，对

[2]参阅 基于期望的程序逻辑中的句法证明规则 [Kozen1985；McIver 和 Morgan 2005]。

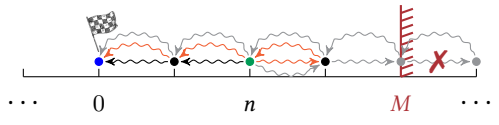

图 1. 守卫强化的效果：在$C_{1\text{dbrw}}$中，所有三条从 • 终止于 • 的程序轨迹（以颜色区分）都会启动。在C_1^M中，然而，穿过“屏障” M 的灰色轨迹不再可能。

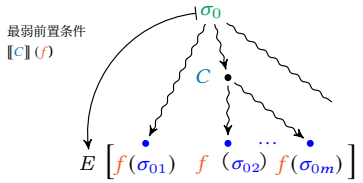

图 2. wp 的示意图：$\text{wp}[\![C]\!]\,(f)\,(\sigma_0)$ 确定在 f 最终状态 • 中求得的期望值，这些状态是在输入 C 时，程序 σ_0 终止后到达的；表示程序 C 的非终止（即发散）路径。

在 $C^M_{1\text{dbrw}}$ 处终止的 $n \le 0$ 概率——从而为 $C_{1\text{dbrw}}$ 的终止概率提供一个下界——可以通过现有的下界归纳规则来处理。事实上，由于 $C^M_{1\text{dbrw}}$ 对于任意固定的 $M \in \mathbb{N}$ 都具有有限状态空间，其精确的在 $n \le 0$ 处的终止概率可以通过概率模型检测得到。此外，如果通过增大M将“屏障”进一步向右推移，就能得到越来越紧的下界。详细分析请参见例16 。

3 最弱前期望推理

3.1 概率守卫命令语言

我们考虑由一种简单但图灵完备的命令式语言描述的概率程序：概率守卫命令语言(pGCL) [McIver 和 Morgan 2005] 该语言扩展了 Dijkstra 的 GCL [Dijkstra 1976]，加入了概率选择和随机赋值。

语法。 pGCL 程序 C 的语法遵循以下文法

$$\begin{aligned} C \quad ::= \quad & \texttt{skip} \mid x \coloneqq e \mid x :\approx \mu \mid C\,;C \mid \{C\}\,[\,p\,]\,\{C\} \mid \\ & \texttt{if}\,(\varphi)\,\{C\}\,\texttt{else}\,\{C\} \mid \texttt{while}\,(\varphi)\,\{C\} \end{aligned}$$

其中， x 是取自可数集合 Vars 的程序变量， e 是关于程序变量的算术表达式， φ 是关于程序变量的无量词一阶谓词， μ 表示离散或连续分布。我们不规定表达式 e 和谓词φ 的语法——只要相应的求值函数可测，它们就可以是任意形式，正如 Szymczak 和 Katoen 2019]所述。大多数程序结构的语义——包括 skip、（确定性）赋值、顺序组合、条件语句和（嵌套）循环——都是标准的。概率选择 $\{\,C_1\,\}\,[\,p\,]\,\{C_2\}$ 以偏置为 $p \in [0,1]$ 的硬币进行随机试验；若结果为正面，则执行 C_1，否则执行 C_2。随机赋值 $x :\approx \mu$ 从分布 μ——离散或连续分布——中抽取一个样本，并将其赋给程序变量 x。

程序状态。A 程序状态 σ 将 Vars 中的每个变量映射到其值，即$\mathbb{R}$中的一个实数。我们用以下符号表示程序状态（可能不可数）的集合：

$$\Sigma \triangleq \{\,\sigma \mid \sigma\colon \texttt{Vars} \to \mathbb{R}\,\}\,.$$

在状态 σ下对表达式 e和守卫条件 φ求值，分别记作 $e(\sigma)$ 和 $\varphi(\sigma)$，其定义是标准的。例如，算术加法的求值为

$$(e_1 + e_2)(\sigma) \triangleq e_1(\sigma) + e_2(\sigma) = e_1\,[x/\sigma(x)] + e_2\,[x/\sigma(x)] \quad \text{for all } x \in \texttt{Vars}$$

其中， $e\,[x/\sigma(x)]$ 表示在 e中用变量 x的值 $\sigma(x)$替换该变量。

谓词。我们将 pGCL 程序中的守卫条件解释为谓词。谓词 φ 表示程序状态 Σ的一个子集。我们用 $\sigma \vDash \varphi$，读作“σ满足 φ”，表示状态 σ属于谓词 φ所表示的集合，即 $\varphi(\sigma)$ = 为真；否则则不成立。我们用 $\varphi_1 \Longrightarrow \varphi_2$，读作“$\varphi_1$强化 φ_2”，表示对于任意状态 $\sigma \in \Sigma$，若 $\varphi_1(\sigma)$ = 为真，则 $\varphi_2(\sigma)$ = 也为真。

3.2 最弱前期望演算

为了推理概率程序的定量性质，特别是对某些概率量的期望值给出下界，我们将pGCL 程序视为期望变换器 [Kaminski 2019；Kozen 1985；McIver 和 Morgan 2005] ——这是对 Dijkstra [1975, 1976]的非概率程序谓词变换器演算的定量扩展。

期望变换器作用于称为期望的实值函数，这些函数将程序状态映射到非负实数（通过无穷大扩展）[3]。请注意期望与期望值之间的区别：与其将其视为期望值，不如将期望看作一个随机变量。

定义1（期望 [Kaminski 2019]）。期望的集合，记作 $\mathbb{E}$，定义为

$$\mathbb{E} \triangleq \{ f \mid f \colon \Sigma \to \mathbb{R}^{\infty}_{\geq 0} \} .$$

期望 $f \in \mathbb{E}$ 是有限的，记作 $f \ll \infty$，当且仅当 f（σ） $< \infty$ 对所有 $\sigma \in \Sigma$均成立； $f \in \mathbb{E}$ 是有界的，当存在 $b \in \mathbb{R}_{\geq 0}$ 使得 f（σ） $\leq b$ 对所有 $\sigma \in \Sigma$均成立时。
为简单起见，将对每个状态求值结果均为 $r \in \mathbb{R}^{\infty}_{\geq 0}$ 的常期望 $\lambda\sigma.\ r$ 记作 r。类似地，给定一个算术表达式 e，我们将期望 $\lambda\sigma.\ e(\sigma)$ 记作 e。
偏序 $\mathrm{l\,order} \leq \mathrm{on}\ \mathbb{E}$ 由对 $\mathbb{R}^{\infty}_{\geq 0}$ 上的规范序 $\leq$ 逐点提升得到，即 .,

$$f_1 \leq f_2 \quad \text{iff} \quad \forall \sigma \in \Sigma \colon\ f_1(\sigma) \leq f_2(\sigma) .$$

$(\mathbb{E}, \leq)$ 构成一个完备格，其最小元为 0，最大元为 ∞。

一个 pGCL 程序 C 被解释为一个期望变换器，它将一个后期望$f \in \mathbb{E}$（在最终状态中求值）沿着 C向后传播，并给出一个前期望 $g \in \mathbb{E}$（在初始状态中求值）。具体而言，如图2所示，关于 C 的最弱前期望 f是一个函数 $g\colon\ \Sigma \to \mathbb{R}^{\infty}_{\geq 0}$，它将的每个初始状态 σ_0 映射 C 到 f在 C 以输入 σ_0:时终止后所到达的最终状态中求得的相应期望值

定义 2（最弱前期望 [Kaminski 2019；Kozen 1985；McIver 和 Morgan 2005]）。给定概率程序 C和初始状态 $\sigma_0 \in \Sigma$。令 ${}^{\sigma_0}\mu_C$ 为[4]在输入 σ_0时，程序 C 终止后到达的最终状态上的（次）概率测度 $f \in \mathbb{E}$。给定关于 ${}^{\sigma_0}\mu_C$可测的后期望 C，程序 f关于 σ_0 的最弱前期望 f将任意初始状态映射为在程序 C 于 σ_0上终止后到达的最终状态中计算所得的期望值，即：[5]

$$\mathrm{wp}[\![C]\!]\,(f)\,(\sigma_0) \triangleq \int_{\Sigma} f \,\mathrm{d}\,({}^{\sigma_0}\mu_C) .$$

已知：(i) 对每个可测的 $f \in \mathbb{E}$，最弱前置条件$[\![C]\!]\,(f)$ 都是可测的（参见 [SzymczakandKatoen2019，引理 3。2]）；(ii) 可测期望的集合在偏序 $\leq$ 下也构成一个完备格（参见 [Szymczak 和 Katoen 2019，引理 2]）。因此，为简便起见，在本文余下部分中，我们滥用记号 $\mathbb{E}$ 来表示可测期望的集合。

[3]为简单起见，我们考虑非负期望这一标准情形。因此，当且仅当算术表达式在所有可达程序状态上取非负值时，它才是定义良好的期望。关于将混合符号期望映射到完整扩展实数范围的更复杂技术，请参见 [Kaminski 和 Katoen 2017]。[4] ${}^{\sigma_0}\mu_C(\sigma) \in [0,1]$ 是程序在输入 σ_0时终止于最终状态 σ的概率。请注意，${}^{\sigma_0}\mu_C(\Sigma) \leq 1$，其中“缺失”的概率质量就是程序 C在输入 σ_0时不终止的概率。${}^{\sigma_0}\mu_C$的形式化定义需要 pGCL 的（操作性）语义模型，这超出了本文的范围；感兴趣的读者可参阅 [Dahlqvist 等人 2020]。[5]若状态空间 Σ可数，则积分可以写成可数和 $\sum_{\sigma \in \Sigma} {}^{\sigma_0}\mu_C(\sigma) \cdot f(\sigma)$。

表 1. wp 变换器的规则。 $[\varphi]$ 表示 φ的伊弗森括号，即当$\sigma \models \varphi$时， $[\varphi]\,(\sigma)$ 的值为 1，否则为 0。对于任意变量 $x \in$ Vars及任意表达式 e， $f\,[x/e]$ 表示满足以下条件的期望：对于任意 $\sigma \in \Sigma$， $f\,[x/e]\,(\sigma) = f(\sigma\,[x/e])$，其中 $\sigma\,[x/e]\,(x) = e(\sigma)$，且对于所有$y \in \text{Vars} \setminus \{x\}$， $\sigma\,[x/e]\,(y) = \sigma(y)$。

C	**最弱前置条件** $[\![C]\!]\,(f)$
skip	f
$x \coloneqq e$	$f\,[x/e]$
$x :\approx \mu$	$\int_{\mathbb{R}} f\,[x/v]\,\mathrm{d}\,\mu(v)$
$C_1 \,;\, C_2$	最弱前置条件$[\![C_1]\!]\,$(最弱前置条件$[\![C_2]\!]\,(f)$)
$\{\,C_1\,\}\ [\,p\,]\ \{C_2\}$	$p \cdot$ 最弱前置条件$[\![C_1]\!]\,(f) + (1-p) \cdot$ 最弱前置条件$[\![C_2]\!]\,(f)$
如果 $(\,\varphi)\,\{\,C_1\}$ 否则 $\{C_2\}$	$[\varphi] \cdot$ 最弱前置条件$[\![C_1]\!]\,(f) + [\neg\varphi] \cdot$ 最弱前置条件$[\![C_2]\!]\,(f)$
while循环 $(\,\varphi)\,\{C'\}$	最小不动点 $^{\text{wp}}\Phi_{\varphi,\,C'\,f}$
$^{\text{wp}}\Phi_{\langle\varphi,C'\rangle\,f}$: $\mathbb{E} \to \mathbb{E}$, $h \mapsto [\neg\varphi] \cdot f + [\varphi] \cdot$ 最弱前置条件$[\![C']\!](h)$	特征函数

最弱前期望可以通过反向、组合式的方式求得；参见附录 B。事实上，所有最弱前置条件-变换器均可通过结构归纳法对所有pGCL 构造进行形式化描述：

定理 3（最弱前置条件变换器 [McIver 和 Morgan 2005]）。设 pGCL 为概率守卫命令语言中程序的集合。其 最弱前期望变换器

$$\text{wp}\colon \text{pGCL} \to \mathbb{E} \to \mathbb{E}$$

遵循 表 1 中的规则是良定义的；事实上，表 1与 定义 2一致。

定理 3 的证明见 [Szymczak 和 Katoen 2019，第 5], 节，其中将离散概率程序的良定义性扩展到了 [Kaminski 2019，定理 4.11]。表 1 中的函数 $^{\text{wp}}\Phi_{\varphi,C\ f}$称为 while（$\varphi$）$\{C\}$ 相对于 f 的特征函数。为简便起见，凡是可从上下文明确得知的情况，我们都省略 wp、φ、 C 或 f中的 Φ。事实上， Φ 是一个（Scott）连续算子，因此也是单调算子，即 $\Phi(\sup\{g_1 \preceq g_2 \preceq \ldots\}) = \sup \Phi(\{g_1 \preceq g_2 \preceq \ldots\})$；参见 [Szymczak 和 Katoen 2019，引理 3.1]。因此，根据 Kleene 不动点定理 [Lassez 等人 1982], , 在 $\mathbb{E}$ 上的偏序 $\preceq$ 中，最小不动点 $\text{lfp}\ \Phi = \sup_{n\in\mathbb{N}} \Phi^n(0) = \lim_{n\to\omega} \Phi^n(0)$ 和最大不动点 $\text{gfp}\ \Phi = \inf_{n\in\mathbb{N}} \Phi^n(\infty) = \lim_{n\to\omega} \Phi^n(\infty)$ 均存在。

表 1 中 wp 变换器的规则具有组合性，而且大多纯粹是句法层面的，因此为自动化最弱前期望演算提供了工具；示例见附录 B。然而，有一个例外：while 循环的变换规则需要确定定量最小不动点，而这通常难以计算，甚至可能无法计算 [Kaminski 等人 2019]；因此，最好能为其求得上界和/或下界。原则上有两个挑战（参见 [Hark 等人 2020]）：(i) 找到一个候选界；(ii) 验证该候选界确实是上界或下界。本文旨在验证 $\text{wp}[\![C]\!]\,(f)$ 的候选下界，其中 C是一个可能嵌套的 while 循环，它可能无法几乎必然终止。 C的终止概率由 $\text{wp}[\![C]\!]\,(1)\,(\sigma_0)$ 表示：

定义 4（几乎必然终止与发散）。设 C 是一个 pGCL 程序，$\sigma_0 \in \Sigma$ 是一个初始程序状态。那么，C在输入 σ_0 上几乎必然终止，当且仅当

$$\text{wp}[\![C]\!]\,(1)\,(\sigma_0) = 1\,.$$

C 几乎必然终止（几乎必然终止）当且仅当 C 对所有输入都几乎必然终止，即，

$$\mathrm{wp}[\![C]\!]\,(1) \;=\; 1\,.$$

C 在输入 σ_0 上发散，当且仅当 最弱前置条件$[\![C]\!]\,(1)\,(\sigma_0) \;<\; 1$。$C$ 发散 当且仅当 C 在某个输入上发散 σ_0。

4 下界推理

本节将形式化表述我们关于证明最小不动点 ${}^{\mathrm{wp}}\Phi_{\langle\varphi,C\rangle}\;\; f$下界的问题，也就是可能发散的 while 循环 $C_{\text{loop}} = \text{while}\,(\;\varphi)\,\{C\}$ 相对于后期望 f 的最弱前置条件的下界。随后，我们将结合现有的归纳法证明规则，从高层次介绍我们的方法。

4.1 问题陈述

本文所关注的问题可表述如下。

> 给定一个可能发散的概率循环 $C_{\text{loop}} = \text{while}\,(\;\varphi)\,\{C\}$、一个可能无界的后期望 $f \in \mathbb{E}$，以及一个可能无界的候选下界 $l \in \mathbb{E}$，验证
>
> $$l \;\preceq\; \mathrm{wp}[\![C_{\text{loop}}]\!]\,(f)\;. \tag{1}$$

我们提出一条新的证明规则来解决这一问题：该规则不使用归纳法，而是将对(1)（含可能发散的） C_{loop} 和可能无界的 f 的验证 $l \in \mathbb{E}$ 转化为

$$l \;\preceq\; \mathrm{wp}[\![\texttt{while}\,(\varphi')\,\{C\}]\!]\,([\neg\varphi]\cdot f) \quad \text{with} \quad \varphi' \implies \varphi\,. \tag{2}$$

具体而言，我们通过强化循环守卫条件φ，将 C_{loop} 构造为一个新的循环 $C'_{\text{loop}} = \text{while}\,(\;\varphi')\,\{\;C\}$，使其守卫条件变为 φ'。这种守卫强化缩小了（可达）状态空间，因此，(i) 修改后的循环 C'_{loop} 具有更强的终止性质（例如，达到几乎必然终止），且 (ii) l 的一致可积性和期望有界性更容易验证。

我们的证明规则利用$\mathrm{wp}[\![C'_{\text{loop}}]\!]\,(f)$ 与$\mathrm{wp}[\![C_{\text{loop}}]\!]\,(f)$ 之间的差异，断言：满足(2) 的相对于 C'_{loop} 而言的下界 l也足以作为满足(1)的相对于 C_{loop} 而言的下界。前者由于守卫强化，通常可以通过应用现有的下界归纳规则（见下文第 4.3 节）得到；或者，在 C'_{loop} 具有有限状态空间的情况下，通过概率模型检测得到。

4.2 用于上界的归纳规则

Park 归纳原理 [Park 1969] 用于最小不动点，为验证最弱前期望的上界提供了一种优雅的方法：

定理 5（用于上界的Park归纳 [Kaminski 2019；Kozen 1985]）。设 Φ_f 是 $C_{\text{loop}} = \text{while}$循环$(\;\varphi)\,\{C\}$ 关于后期望 $f \in \mathbb{E}$ 的特征函数，且 $u \in \mathbb{E}$。则

$$\Phi_f(u) \;\preceq\; u \quad \text{implies} \quad \mathrm{wp}[\![C_{\text{loop}}]\!]\,(f) \;\preceq\; u\,. \tag{3}$$

我们称 $u \in \mathbb{E}$ 满足 $\Phi_f(u) \;\preceq\; u$ 为超不变式。正如Hark 等人 [2020], 所指出的，Park 归纳的显著威力在于其简洁性：一旦找到合适的候选 u（不过这通常并非易事），我们要做的就是将 u 代入 Φ_f一次，并检查它是否在 $\preceq$意义下变小。如果是这样，我们就验证了 u 确实是最小不动点 Φ_f 以及最弱前期望的上界。

Park 归纳法的可靠性由图中左侧（递减）链说明。图 图 3。我们请读者参阅 [Hark 等人 2020]，其中利用 Tarski-Kantorovitch原理给出了形式化的可靠性论证（另见 [Jachymski 等人 2000]）。另请参阅 [Batz 等人 2021a]，其中通过（格点） k归纳法给出了更一般的证明规则，用于确立最小不动点的上界。

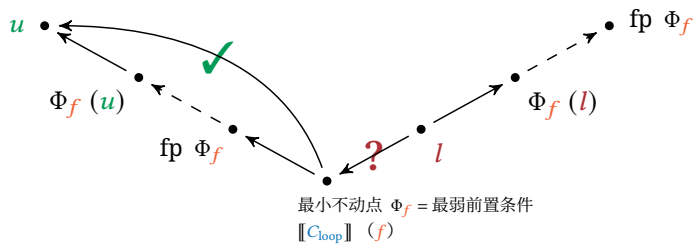

图 3. Park 归纳的可靠性直观示意（左支）以及简单下界归纳的不健全性（右支）。从 $g_1 \in \mathbb{E}$ 指向 $g_2 \in \mathbb{E}$ 的箭头表示 $g_1 \preceq g_2$。对于 Park 归纳，Φ_f 在 u 上的迭代向下收敛到 Φ_f 的一个不动点；根据 Knaster–Tarski 定理 [Knaster 1928；Lassez 等，1982；Tarski 1955]，该不动点必然大于等于最小不动点 Φ_f，从而证明 $\mathrm{wp}[\![C\text{循环}]\!](f) \preceq u$。然而，对于简单下界归纳，升链 $l \preceq \Phi_f(l) \preceq \ldots$ 收敛到 Φ_f 的一个不动点，该不动点必然小于等于最大不动点 $\mathrm{gfp}\ \Phi_f$，但我们不知道 l 与最小不动点 Φ_f 的大小关系。

4.3 下界归纳规则

Park 归纳法的“对偶”版本——将 $\preceq$ 中(3) 翻转——可用于验证最大不动点最大不动点 Φ_f的下界，但不能用于验证最小不动点 Φ_f的下界。更准确地说，对于 $l \in \mathbb{E}$，规则为

$$l \preceq \Phi_f(l) \quad \text{implies} \quad l \preceq \mathrm{wp}[\![C_{\mathrm{loop}}]\!](f)\,, \qquad \lightning$$

在一般情况下并不可靠。我们称 $l \in \mathbb{E}$ 满足 $l \preceq \Phi_f(l)$ 的一个次不变式，并将上述不可靠规则称为简单下界归纳。图 3中右侧（递增）链展示了简单下界归纳的不健全性，下方的一个反例也说明了这一点。形式化论证可参阅 [Hark 等人 2020] 的工作，其中再次使用了 Tarski-Kantorovitch原理。

例6（简单下界归纳的不健全性）。重新考虑第 2 节中带有后期望 $f = 1$ 的循环 $C_{1\mathrm{dbrw}}$；其特征函数为 $\Phi_f(h) = [n \le 0] + [n > 0] \cdot (1/3 \cdot h(n-1) + 2/3 \cdot h(n+1))$。注意，常期望 $g = 1$ 是一个超不变式，因为 $\Phi_f(g) = 1 \preceq g$。这表明 $C_{1\mathrm{dbrw}}$ 的终止概率（显然）不超过 1（参见定理5）。与此同时，g 也是一个次不变式，因为 $g \preceq 1 = \Phi_f(g)$，但这不足以证明 1 是终止概率的下界（回想一下，$C_{1\mathrm{dbrw}}$ 是非几乎必然终止的；参见第 2 节）。◁

为了恢复下界归纳的可靠性，Hark 等人 [2020] 提出了依赖于几乎必然终止（即 $\mathrm{wp}[\![C_{\mathrm{loop}}]\!](1) = 1$，参见定义4）和随机过程领域中的一致可积性等概念的侧条件。为表述后者，我们用 X_n 表示循环体 C执行 n次迭代后的程序状态所对应的随机变量，用 $T^{\neg\varphi} \triangleq \inf\{n \in \mathbb{N} \mid X_n \models \neg\varphi\}$ 表示停时（又称循环时间），它指示 X_n 首次达到 $\neg\varphi$的时刻；[6]并用 $\{X_n^{T^{\neg\varphi}}\}_{n\in\mathbb{N}}$表示相应的停时随机过程，即当 $n \le T^{\neg\varphi}$时为 $X_n^{T^{\neg\varphi}} = X_n$，否则为$X_n^{T^{\neg\varphi}} = X_{T^{\neg\varphi}}$；停时和停时过程的形式化定义见附录A。

定义 7（一致可积性）。概率空间 $(\Omega, \mathcal{F}, P)$上的随机过程 $\{X_n\}_{n\in\mathbb{N}}$称为一致可积（简称u.i.），如果

$$\lim_{R\to\infty} \sup_{n\in\mathbb{N}} E\left[|X_n| \cdot \mathbb{1}_{|X_n|\ge R}\right] = 0 \tag{4}$$

其中 $\mathbb{1}_{|X_n|\ge R}$是示性函数，即 $\mathbb{1}_{|X_n|\ge R}(\omega) = 1$当 $\omega \in \{\omega \in \Omega \mid |X_n(\omega)| \ge R\}$，否则为 0。给定 $C_{\mathrm{loop}} = \text{while循环}\,(\varphi)\{C\}$，期望 $h \in \mathbb{E}$对于 C_{loop}是一致可积的，$\{h(X_n^{T^{\neg\varphi}})\}_{n\in\mathbb{N}}$当 C_{loop}在由 C_{loop}诱导的概率空间上一致可积时（参见 第 5 节）。

[6]循环时间 $T^{\neg\varphi}$不考虑循环体 C的运行时间。

直观地说，(4) 断言 X_n 的尾部期望值在 L^1-范数意义下是一致地（由上确界表示）较小的。一个一致可积过程 X_n 因此满足 $E(\lim_{n\to\infty} X_n) = \lim_{n\to\infty} E(X_n)$，条件是 $\lim_{n\to\infty} X_n$ 几乎必然存在。现在，针对下界的可靠归纳规则如下所述。

定理 8（Hark等人的下界归纳 [Hark 等人 2020]）。令 Φ_f 为 $C_{\text{loop}} = \texttt{while}(\varphi)\{C\}$ 关于后期望 $f \in \mathbb{E}$，并令 $l \in \mathbb{E}$。则

$$\underbrace{l \leq \Phi_f(l)}_{\text{次不变性}} \quad \text{and} \quad \underbrace{\text{最弱前置条件}[\![C_{\text{loop}}]\!](1) = 1 \text{ 并且 } l \text{ 对 } C_{\text{loop}} \text{一致可积}}_{\text{侧条件}} \quad \text{意味着} \quad l \leq \text{wp}[\![C_{\text{loop}}]\!](f)。 \tag{5}$$

与用于上界的Park归纳不同，为了建立下界，(5) 中的侧条件需要额外证明几乎必然终止和一致可积性，而这两项在计算上通常都难以处理，例如参见 [Kaminski 等人 2019]。文献中已提出多种技术和工具，例如 [Chatterjee等，2020；McIver 等人，2018；Moosbrugger 等人 2021]，，用于证明（若干子类）概率程序几乎必然终止。为证明一致可积性，Hark 等人 [2020] 基于著名的可选停止时间定理提出了充分条件 [Williams1991，第 10]:

定理 9（一致可积性的充分判据 [Hark 等人 2020]）。给定 C_{loop} =while循环 $(\varphi)\{C\}$，令 $^{\sigma_0}\mathbb{P}$ 为由 C_{loop} 在初始状态 $\sigma_0 \in \Sigma$上诱导的（次）概率测度。[7]那么，当以下条件之一成立时，期望 $h \ll \infty$ 对于 C_{loop} 是一致可积的：

(a) 循环时间 $T^{\neg\varphi}$ 几乎必然有界，即对于任意初始状态 $\sigma_0 \in \Sigma$，都存在$N \in \mathbb{N}$ 使得 $^{\sigma_0}\mathbb{P}(T^{\neg\varphi} \leq N) = 1$，且对于任意 $n \in \mathbb{N}$，$wp[\![C]\!]^n(h) \ll \infty$。*(b)* 期望循环时间有限，且 h条件差有界，即对于任意 $\sigma_0 \in \Sigma$，$E\,[T^{\neg\varphi}] < \infty\ ^{\sigma_0}$，并且存在 $c \in \mathbb{R}_{\geq 0}$，使得对于任意 $\sigma \vDash \varphi$，$wp[\![C]\!](|h - h(\sigma)|) \leq c$。*(c)* h 有界，即存在 $c \in \mathbb{R}_{\geq 0}$，使得对于任意 $\sigma \in \Sigma$，$h(\sigma) \leq c$。

总之，Hark 等人的可靠下界归纳规则定理 8 不适用于发散的程序；即便对于几乎必然终止的程序，该规则也需要额外的证明工作，例如，寻找能够 [Chat- terjee 等人 2020] 证明程序几乎必然终止的超鞅，并推理循环时间（(a) 和(b) 见定理 9），或建立期望的界（(b) 和(c) 见定理 9），以实现一致可积。

McIver 和 Morgan 提出了一个正交的归纳规则，适用于McIver 和 Morgan [2005] 有界期望的：

定理 10（McIver 和 Morgan 的下界归纳 [McIver 和 Morgan 2005]）。设 Φ_f是 C_{loop} = while循环$(\varphi)\{C\}$ 关于有界后期望的特征函数 $f \in \mathbb{E}$，$l \in \mathbb{E}$ 是~~一个有界~~期望，满足 $l \leq \Phi_f(l)$ 且 $[\neg\varphi] \cdot l = [\neg\varphi] \cdot f$，并且 $p = \text{wp}[\![C_{\text{loop}}]\!](1)$是 C_{loop}的终止概率。则

(a) 若 $l = [G]$ 对于某个谓词 G成立，则 $p \cdot l \leq \text{wp}[\![C_{\text{loop}}]\!](f)$。(b) 若 $[G] \leq p$ 对于某个谓词 G成立，则 $[G] \cdot l \leq \text{wp}[\![C_{\text{loop}}]\!](f)$。(c) 若 $\varepsilon \cdot l \leq p$ 对于某个 $\varepsilon \in \mathbb{R}_{>0}$成立，则 $l \leq \text{wp}[\![C_{\text{loop}}]\!](f)$。

McIver 和 Morgan 的下界归纳规则适用于发散程序（其终止概率为 < 1）；然而，该规则仅适用于有界期望，且要求预先知道一个 p while循环的终止概率，而一般而言这很难推断（这反过来可能需要求出 p的下界）。事实上，当 C_{loop} 几乎必然终止时，Hark 等人的归纳规则是 McIver 和 Morgan 的归纳规则的推广 [（Hark 等人，2020，定理 41]）。据我们所知，这两条证明规则是现有的仅有的用于验证最弱前期望下界的（归纳）规则。

[7]The 测度 $^{\sigma_0}\mathbb{P}$ 将在 第 5 节中正式定义。注意，$^{\sigma_0}\mathbb{P}(T^{\neg\varphi} < \infty) = 1$ 当且仅当 最弱前置条件$[\![C_{\text{loop}}]\!](1)(\sigma_0) = 1$.

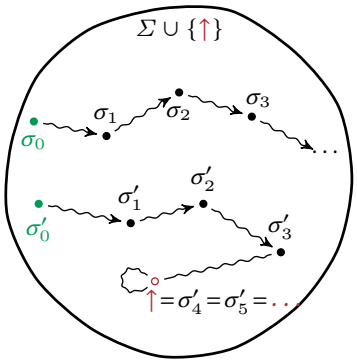

图 4. $\mathbb{S}$ 中的无限轨迹。

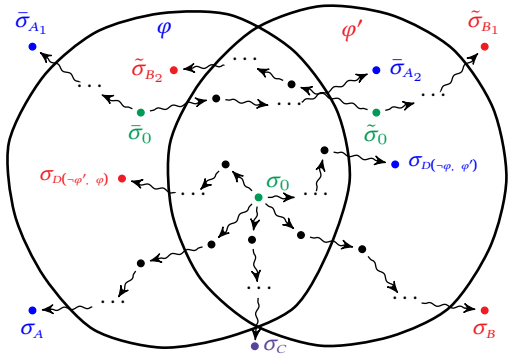

图 5. 图示 定理 11 (参见 (10))。

5 最弱前期望的差异

我们的下界证明规则将概率循环的验证归约为其强化版本的验证。为了证明这种归约合理，我们需要从最弱前期望的角度对两个概率循环进行定量关联。本节将说明，如何量化两个 while 循环的最弱前期望之间的差异。这两个循环仅在循环守卫上有所不同，并且对应相同的后期望 $f \in \mathbb{E}$，即

$$\mathrm{wp}[\![\underbrace{\texttt{while}\,(\varphi)\,\{C\}}_{C_{\text{loop}}}]\!]\,(f) \;-\; \mathrm{wp}[\![\underbrace{\texttt{while}\,(\varphi')\,\{C\}}_{C'_{\text{loop}}}]\!]\,(f) \tag{6}$$

其中 φ和 φ'是表示 Σ的子集的任意谓词（此处，φ,不一定比 φ更强）[8]，且共享的循环体 C 本身也可以包含更深层的嵌套while循环。对最弱前置条件差值作这样的量化，构成了我们新证明规则的基础（参见第 6 节）。

回顾一下，循环相对于 $f \in \mathbb{E}$ 的最弱前期望定义为（参见 定义 2）f 关于循环终止后到达的最终状态上的（次）概率测度的积分，其中终止行为由循环守卫和循环体决定。因此，为了联系(6)中的两个最弱前期望，我们首先抽象掉循环守卫 φ 和 φ'，从而得到一个必然发散的循环 $C^{\uparrow}\,\mathsf{loop} = \mathsf{while}\,(\,\mathsf{true}\,)\,\{C\}$。接着，我们在 $C^{\uparrow}\,\mathsf{loop}$ 的 $\mathbb{S}$ 集合上构造一个概率空间，该集合由无限轨迹（即程序状态序列）组成，形式化地，

$$\mathbb{S} \;\triangleq\; \{\,\sigma_0\sigma_1\cdots\sigma_i\cdots \mid \sigma_0 \in \Sigma,\ \forall i \geq 1\colon \sigma_i \in \Sigma \cup \{\uparrow\} \wedge (\sigma_i = \uparrow \implies \sigma_{i+1} = \uparrow)\,\}$$

其中，$\sigma_i \neq \uparrow$ 表示循环体 C 在第 i次迭代后终止时所处的状态，$\uparrow$表示 C 发散时所处的汇状态。图 4 展示了两种无限轨迹（有汇状态和无汇状态）的示例。给定无限轨迹的一个有限前缀 π，其柱集为 $\pi\,cyl(\pi) \triangleq \{s \in \mathbb{S} \mid \exists t \in (\Sigma \cup \{\uparrow\})^{\omega}\colon\ s = \pi t\}$，即所有以 π为前缀的无限轨迹的集合。

循环的操作语义 [Dahlqvist 等人 2020] 诱导出一族（次）概率测度——对任意 $\sigma \in \Sigma$，记为 ${}^{\sigma}\mathbb{P}$ ——定义在 $\mathbb{S}$ 上，其最小的包含所有柱集的 σ-代数

[8]假设 $\varphi' \implies \varphi$足以证明我们的证明规则。然而，我们关注的是关于最弱前置条件差异的一个更一般的结果，其中无关 φ 和 φ'，原因包括：(i) φ 和 φ'的对称性；以及 (ii) 这一一般性结果有望解决验证下界之外的问题，例如概率程序的敏感性分析 [Aguirre 等人，2021；Barthe 等人，2018；Wang 等人 2020] 以及模型修复 [Bartocci 等人 2011]，这也是一个值得探讨的未来方向。

柱集。也就是说，对于任意有限前缀 $\pi = \sigma_0\sigma_1\cdots\sigma_n$,

$$ {}^{\sigma}\mathbb{P}\left(cyl(\pi)\right) = \begin{cases} [\sigma = \sigma_0]\cdot {}^{\sigma_0}\mu_C(\sigma_1)\cdot\ldots\cdot {}^{\sigma_{i-1}}\mu_C(\sigma_i)\cdot\ldots\cdot {}^{\sigma_{n-1}}\mu_C(\sigma_n) & \text{if } \forall i \le n\colon \sigma_i \neq \uparrow, \\ [\sigma = \sigma_0]\cdot {}^{\sigma_0}\mu_C(\sigma_1)\cdot\ldots\cdot {}^{\sigma_{i-1}}\mu_C(\sigma_i)\cdot(1 - {}^{\sigma_i}\mu_C(\Sigma)) & \text{if } \exists i < n\colon \sigma_i \neq \uparrow \wedge \sigma_{i+1} = \uparrow, \end{cases} $$

其中， ${}^{\sigma}\mu_C$ 表示循环体 C 在输入 σ 上终止后所到达最终状态上的（次）概率测度。随机变量 $X_n\colon\ \mathbb{S} \to \Sigma$ 表示循环体 n 第 C 次迭代后程序状态的 $X_n(\sigma_0\sigma_1\cdots) = \sigma_n$。给定 $C_{\text{loop}} = \text{while}\ (\varphi)\ \{\ C\}$， $T^{\neg\varphi}$ 的循环时间 $\mathbb{S} \to \mathbb{N}$ 定义为 C_{loop} 的 $T^{\neg\varphi}(s)\ = \inf\{n \mid X_n(s)\ \models \neg\varphi\}$。对于任意关于 $\mathbb{S}$ 的随机变量 X 以及关于 X 的谓词 ϕ，我们将 ${}^{\sigma}\mathbb{P}(\{s \in \mathbb{S} \mid \phi(X(s))\})$ 简写为 ${}^{\sigma}\mathbb{P}(\phi(X))$; 例如，${}^{\sigma}\mathbb{P}(T^{\neg\varphi} \ge n)$ 是 ${}^{\sigma}\mathbb{P}(\{s \in \mathbb{S} \mid T^{\neg\varphi}(s)\ \ge n\})$ 的简写。基于上述定义的测度 ${}^{\sigma}\mathbb{P}$，(6)中 $\text{wp}[\![C_{\text{loop}}]\!](f)$ 与 $\text{wp}[\![C'_{\text{loop}}]\!](f)$ 之间的差异可量化如下。

定理 11（最弱前置条件差异）。给定循环 $C_{\text{loop}} = \texttt{while}\ (\varphi)\ \{\ C\}$ 和 $C'_{\text{loop}} = \texttt{while}\ (\varphi')\ \{\ C\}$，则对于任意后期望 $f \in \mathbb{E}$、[9]

$$ \begin{aligned} &\text{wp}[\![C_{\text{loop}}]\!](f) - \text{wp}[\![C'_{\text{loop}}]\!](f)\ = \\ &\qquad \text{wp}[\![\texttt{while}\,(\varphi \wedge \varphi')\,\{C\}]\!]\left([\neg\varphi \wedge \varphi']\cdot f\right) + \lambda\sigma.\ \int_A f_{C_{\text{loop}}}\,\mathrm{d}\left({}^{\sigma}\mathbb{P}\right) - \\ &\qquad \text{wp}[\![\texttt{while}\,(\varphi \wedge \varphi')\,\{C\}]\!]\left([\varphi \wedge \neg\varphi']\cdot f\right) - \lambda\sigma.\ \int_B f_{C'_{\text{loop}}}\,\mathrm{d}\left({}^{\sigma}\mathbb{P}\right), \end{aligned} \tag{7} $$

其中， $A \subseteq \mathbb{S}$ 是这样一组无限轨迹：它们在命中 $\neg\varphi$ 之前先命中 $\neg\varphi'$； $f_{C_{\text{loop}}}$ 是一个偏函数，将轨迹 $s \in \mathbb{S}$ 映射为 $f\ (\sigma_n)$，条件是 s 在 σ_n 处首次命中 $\neg\varphi$，即：

$$ \begin{aligned} A\ &\triangleq\ \{\,\sigma_0\sigma_1\cdots\sigma_i\cdots \in \mathbb{S} \mid \exists n \in \mathbb{N}\colon\ (\sigma_n \models \neg\varphi) \wedge (\forall i < n\colon \sigma_i \models \varphi) \wedge (\exists k < n\colon \sigma_k \models \neg\varphi')\,\}, \\ f_{C_{\text{loop}}}&\colon \mathbb{S} \rightharpoonup \mathbb{R}^{\infty}_{\ge 0} \qquad \sigma_0\sigma_1\cdots\sigma_i\cdots \mapsto f(\sigma_n) \quad \text{if } (\sigma_n \models \neg\varphi) \wedge (\forall i < n\colon \sigma_i \models \varphi)\ ; \end{aligned} \tag{8} $$

对偶地， $B \subseteq \mathbb{S}$ 是这样一组无限轨迹：它们在命中 $\neg\varphi$ 之前先命中 $\neg\varphi'$；而 $f_{C'_{\text{loop}}}$ 将轨迹 $s \in \mathbb{S}$ 映射 f 为 (σ_n)，条件是 s 在 $\neg\varphi'$ 处首次命中 σ_n （ B 和 $f_{C'_{\text{loop}}}$ 的定义类似于（8））。

证明。我们通过考察 $\mathbb{S}$ 中的不同类型轨迹来证明该定理，如图 5 所示。给定一个谓词， ϕ 令 $\Diamond\phi$ 为所有最终命中 ϕ 的轨迹集合，即：

$$ \Diamond\phi\ \triangleq\ \{\,\sigma_0\sigma_1\cdots\sigma_i\cdots \in \mathbb{S} \mid \exists n \in \mathbb{N}\colon \sigma_n \models \phi\,\}. $$

根据（次）概率测度 ${}^{\sigma}\mathbb{P}$ 的定义，我们有

$$ \begin{aligned} \text{wp}[\![C_{\text{loop}}]\!](f)\ &=\ \lambda\sigma.\ \int_{\Sigma} f\ \mathrm{d}\left({}^{\sigma}\mu_{C_{\text{loop}}}\right)\ =\ \lambda\sigma.\ \int_{\Diamond(\neg\varphi)} f_{C_{\text{loop}}}\,\mathrm{d}\left({}^{\sigma}\mathbb{P}\right), \\ \text{wp}[\![C'_{\text{loop}}]\!](f)\ &=\ \lambda\sigma.\ \int_{\Sigma} f\ \mathrm{d}\left({}^{\sigma}\mu_{C'_{\text{loop}}}\right)\ =\ \lambda\sigma.\ \int_{\Diamond(\neg\varphi')} f_{C'_{\text{loop}}}\,\mathrm{d}\left({}^{\sigma}\mathbb{P}\right). \end{aligned} \tag{9} $$

为了量化 wp 差，我们首先分别将 $\Diamond(\neg\varphi)$ 和 $\Diamond(\neg\varphi')$ 中的轨迹集合分解为互不相交的部分。为此，令

$$ C\ \triangleq\ \{\,\sigma_0\sigma_1\cdots\sigma_i\cdots \in \mathbb{S} \mid \exists n \in \mathbb{N}\colon\ (\sigma_n \models \neg\varphi \wedge \neg\varphi') \wedge (\forall i < n\colon \sigma_i \models \varphi \wedge \varphi')\,\}, $$

对于任意谓词 ϕ_1， ϕ_2，令

$$ D\left(\phi_1, \phi_2\right)\ \triangleq\ \{\,\sigma_0\sigma_1\cdots\sigma_i\cdots \in \mathbb{S} \mid \exists n \in \mathbb{N}\colon\ (\sigma_n \models \phi_1) \wedge (\forall i \le n\colon \sigma_i \models \phi_2)\,\}. $$

[9]为便于理解， （7）被表述为最弱期望之差的形式。这种表述可能会引发“$\infty - \infty$”的问题，不过，可以将（7）中的所有负项移到等式另一边来避免这个问题。同样的改写方法也适用于定理 11 的证明。

由此可得

$$\begin{aligned}
\Diamond\,(\neg\varphi) \;&=\; \overbrace{A}^{\substack{\text{在到达 } \neg\varphi \text{ 之前到达 } \neg\varphi'\\ \text{例如，} \sigma_0\cdots\sigma_A\cdots\ \bar{\sigma}_0\cdots \text{ 见图 5}}} \;\uplus\; \overbrace{C}^{\substack{\text{同时到达 } \neg\varphi',\ \neg\varphi\\ \text{例如，} \sigma_0\cdots\sigma_C\cdots \text{ 见图 5}}} \;\uplus\; \overbrace{D(\neg\varphi,\ \varphi')}^{\substack{\text{达到 } \neg\varphi \text{ while循环，同时满足 } \varphi'\\ \text{例如，} \sigma_0\cdots\sigma_{D(\neg\varphi,\varphi')}\cdots \text{ 见图 5}}}\,,\\
\Diamond\,(\neg\varphi') \;&=\; \overbrace{B}^{\substack{\text{在达到 } \neg\varphi' \text{之前达到 } \neg\varphi\\ \text{例如，} \sigma_0\cdots\sigma_B\cdots\ \bar{\sigma}_0\cdots \text{ 见图 5}}} \;\uplus\; \overbrace{C}^{\substack{\text{同时命中 } \neg\varphi,\ \neg\varphi'\\ \text{例如，} \sigma_0\cdots\sigma_C\cdots \text{ 在图 5}}} \;\uplus\; \overbrace{D(\neg\varphi',\ \varphi)}^{\substack{\text{命中 } \neg\varphi',\ \text{同时满足 } \varphi\\ \text{例如，} \sigma_0\cdots\sigma_{D(\neg\varphi',\varphi)}\cdots \text{ 在图 5}}}\,.
\end{aligned} \tag{10}$$

显然，根据定义，$f_{C_{\text{loop}}}$和$f_{C'_{\text{loop}}}$在$C \subseteq \mathbb{S}$上重合，即，

$$\forall s \in C\colon\ f_{C_{\text{loop}}}(s) \;=\; f_{C'_{\text{loop}}}(s)\ . \tag{11}$$

对于 $D(\cdot,\ \cdot)$，我们有（关于引理 32，见附录 C.1，其中给出了下面(12)的更详细证明 ）

$$\begin{aligned}
\lambda\sigma.\ \int_{D(\neg\varphi,\varphi')} f_{C_{\text{loop}}}\ \mathrm{d}\left({}^{\sigma}\mathbb{P}\right) \;&=\; \underbrace{\mathsf{wp}[\![\texttt{while}\,(\,\varphi\wedge\varphi'\,)\,\{\,C\,\}]\!]\,([\neg\varphi\wedge\varphi']\cdot f)}_{\text{evaluating } f \text{ over, e.g., } \sigma_{D(\neg\varphi,\varphi')} \text{ in Fig. 5}}\,,\\
\lambda\sigma.\ \int_{D(\neg\varphi',\varphi)} f_{C'_{\text{loop}}}\ \mathrm{d}\left({}^{\sigma}\mathbb{P}\right) \;&=\; \underbrace{\mathsf{wp}[\![\texttt{while}\,(\,\varphi\wedge\varphi'\,)\,\{\,C\,\}]\!]\,([\varphi\wedge\neg\varphi']\cdot f)}_{\text{evaluating } f \text{ over, e.g., } \sigma_{D(\neg\varphi',\varphi)} \text{ in Fig. 5}}\,.
\end{aligned} \tag{12}$$

结合以上事实，我们得到

$$\begin{aligned}
&\mathsf{wp}[\![C_{\text{loop}}]\!]\,(f) - \mathsf{wp}[\![C'_{\text{loop}}]\!]\,(f) = \lambda\sigma.\ \int_{\Diamond(\neg\varphi)} f_{C_{\text{loop}}}\ \mathrm{d}\left({}^{\sigma}\mathbb{P}\right) - \lambda\sigma.\ \int_{\Diamond(\neg\varphi')} f_{C'_{\text{loop}}}\ \mathrm{d}\left({}^{\sigma}\mathbb{P}\right) \quad \text{[by (9)]}\\
=\ &\lambda\sigma.\ \int_{A} f_{C_{\text{loop}}}\ \mathrm{d}\left({}^{\sigma}\mathbb{P}\right) + \lambda\sigma.\ \int_{C} f_{C_{\text{loop}}}\ \mathrm{d}\left({}^{\sigma}\mathbb{P}\right) + \lambda\sigma.\ \int_{D(\neg\varphi,\varphi')} f_{C_{\text{loop}}}\ \mathrm{d}\left({}^{\sigma}\mathbb{P}\right) -\\
&\lambda\sigma.\ \int_{B} f_{C'_{\text{loop}}}\ \mathrm{d}\left({}^{\sigma}\mathbb{P}\right) - \lambda\sigma.\ \int_{C} f_{C'_{\text{loop}}}\ \mathrm{d}\left({}^{\sigma}\mathbb{P}\right) - \lambda\sigma.\ \int_{D(\neg\varphi',\varphi)} f_{C'_{\text{loop}}}\ \mathrm{d}\left({}^{\sigma}\mathbb{P}\right) \quad \text{[by linearity of } \textstyle\int\text{, (10)]}\\
=\ &\mathsf{wp}[\![\texttt{while}\,(\,\varphi\wedge\varphi'\,)\,\{\,C\,\}]\!]\,([\neg\varphi\wedge\varphi']\cdot f) + \lambda\sigma.\ \int_{A} f_{C_{\text{loop}}}\ \mathrm{d}\left({}^{\sigma}\mathbb{P}\right) -\\
&\mathsf{wp}[\![\texttt{while}\,(\,\varphi\wedge\varphi'\,)\,\{\,C\,\}]\!]\,([\varphi\wedge\neg\varphi']\cdot f) - \lambda\sigma.\ \int_{B} f_{C'_{\text{loop}}}\ \mathrm{d}\left({}^{\sigma}\mathbb{P}\right)\ . \quad \text{[by (11) and (12)]}
\end{aligned}$$

证明至此完成。 □

例子 12（最弱前置条件-差异）。考虑两个以后期望 $f = [0 \le n \le 11]$ 为后期望的循环：

$$\begin{aligned}
C_{\text{loop}}\colon&\quad \texttt{while}\,(\,0 < n < 10\,)\,\{\,n \coloneqq n-1\ [1/2]\ n \coloneqq n+1\,\}\ ,\\
C'_{\text{loop}}\colon&\quad \texttt{while}\,(\,1 < n < 11\,)\,\{\,n \coloneqq n-1\ [1/2]\ n \coloneqq n+1\,\}\ .
\end{aligned}$$

令 $C_{\wedge}$为 循环 while循环$(1 < n < 10)\{n \coloneqq n-1\ [1/2]\ n \coloneqq n+1\}$。为说明 定理 11，我们展示

最弱前置条件$[\![C_{\text{loop}}]\!]([0 \le n \le 11])$ − 最弱前置条件$[\![C'_{\text{loop}}]\!]([0 \le n \le 11])$ =

$$\begin{aligned}
&\mathsf{wp}[\![C_{\wedge}]\!]\,([n=10]) + \lambda\sigma.\ \int_{A} f_{C_{\text{loop}}}\ \mathrm{d}\left({}^{\sigma}\mathbb{P}\right) -\\
&\mathsf{wp}[\![C_{\wedge}]\!]\,([n=1]) - \lambda\sigma.\ \int_{B} f_{C'_{\text{loop}}}\ \mathrm{d}\left({}^{\sigma}\mathbb{P}\right)\ .
\end{aligned} \tag{13}$$

注意，

$$\mathsf{wp}[\![C_{\text{loop}}]\!]\,([0 \le n \le 11]) \;=\; \mathsf{wp}[\![C'_{\text{loop}}]\!]\,([0 \le n \le 11]) \;=\; [0 \le n \le 11]\,,$$

由于一个关键事实：C_{loop} 和 C'_{loop} 都以概率1终止。因此，(13) 的左侧等于0。对于(13)的右侧，应用Hark等人的下界归纳和用于上界的Park归纳（省略细节）可得

$$\mathsf{wp}[\![C_{\wedge}]\!]\,([n=10]) \;=\; [1\le n\le 10]\cdot\frac{n-1}{9}\,,\qquad \mathsf{wp}[\![C_{\wedge}]\!]\,([n=1]) \;=\; [1\le n\le 10]\cdot\frac{10-n}{9}\,.$$

此外，注意到 $f_{C_{\text{loop}}}=1$ over A 和 $f_{C'_{\text{loop}}}=1$ over B，我们有

$$\int_A f_{C_{\text{loop}}}\,\mathrm{d}\left({}^{\sigma}\mathbb{P}\right) \;=\; [1\le n<10]\cdot\frac{10-n}{9}\,,\qquad \int_B f_{C'_{\text{loop}}}\,\mathrm{d}\left({}^{\sigma}\mathbb{P}\right) \;=\; [1<n\le 10]\cdot\frac{n-1}{9}\,.$$

由此可知，(13)的右侧也等于 0。 ◁

定理 11 背后的直觉是，将最弱前期望分解为互不相交的部分，这些部分覆盖 $\mathbb{S}$ 中不同类型的轨迹——轨迹类型由其命中 $\neg\varphi$ 和/或命中 $\neg\varphi'$ 的时间行为决定，见 (10) 和图 5——从而通过消去共有部分，得到 $\mathsf{wp}[\![C_{\text{loop}}]\!]\,(f)$ 与 $\mathsf{wp}[\![C'_{\text{loop}}]\!]\,(f)$ 之间的精确差值，参见 (11)。然而，其互异部分在 (7) 中的积分仍难以求解；不过，只需在 φ' 加强 φ 时，为 $\mathsf{wp}[\![C_{\text{loop}}]\!]\,(f)$ 求得一个下界即可（该下界的紧确性见第 6.3 节）：

推论 13. 给定循环 $C_{\text{loop}}=\texttt{while}(\varphi)\{C\}$ 和 $C'_{\text{loop}}=\texttt{while}(\varphi')\{C\}$，假设 $\varphi'\not\Longrightarrow\varphi$，那么，对于任意后期望 $f\in\mathbb{E}$，

$$\mathsf{wp}[\![C_{\text{loop}}]\!]\,(f) \;\ge\; \mathsf{wp}[\![C'_{\text{loop}}]\!]\,([\neg\varphi]\cdot f)\,.$$

推论 13 的直观解释如下：回顾一下，$\mathsf{wp}[\![C_{\text{loop}}]\!]\,(f)$ 将任意初始状态 σ_0 映射为 f 在 C_{loop} 于 σ_0 上终止后到达的最终状态中求得的期望值，即循环守卫条件 φ被违反时的期望值。为了通过修改后的循环 C'_{loop}，为 $\mathsf{wp}[\![C_{\text{loop}}]\!]\,(f)$ 得到一个可靠的下界，我们必须将后期望 f限制为 $[\neg\varphi]\cdot f$，使得 f仅在违反原始守卫条件 φ（因而也违反强化后的守卫条件 φ'）的状态中求值。推论 13 的证明利用了这样一个事实：由于 $\varphi'\Longrightarrow\varphi$，我们有 $\varphi\wedge\varphi'=\varphi'$, $[\neg\varphi\wedge\varphi']=0$，且$B=\emptyset$（即，在命中 $\neg\varphi'$之前，任何轨迹都不可能命中 $\neg\varphi$，参见（10））；详见附录 C.2 中的详细证明。

6 下界证明规则

本节将介绍一种用于验证最弱前期望下界的新证明规则，称为守卫强化规则。该规则基于最弱前置条件差以及第 5 节中的守卫强化技术第 5 节。随后，我们将从多个方面展示该证明规则的实用性，尤其是它在推理可能发散的概率程序方面的用途。

定理 14（下界的守卫强化）。给定循环 $C_{\text{loop}}=\texttt{while}(\varphi)\{C\}$、$C'_{\text{loop}}=\texttt{while}(\varphi')\{C\}$以及后期望 $f\in\mathbb{E}$，令 $l\in\mathbb{E}$，则以下推理规则成立：

$$\frac{\varphi'\Longrightarrow\varphi \qquad l\;\le\;\mathsf{wp}[\![C'_{\text{loop}}]\!]\,([\neg\varphi]\cdot f)}{l\;\le\;\mathsf{wp}[\![C_{\text{loop}}]\!]\,(f)}\;\textsc{Guard-Strengthening}\,. \tag{14}$$

证明。（可靠性）证明规则(14) 可由推论 13直接推出。我们在附录 C.3 给出另一种证明，该证明与轨迹无关，因而更简单，但无法为我们在第 6.3 节中关于该证明规则紧确性的论证作出贡献。□

我们的守卫强化规则断言，只要满足 $\varphi'\Longrightarrow\varphi$，那么 $\mathsf{wp}[\![C_{\text{loop}}]\!]\,(f)$ 的下界也可由 $\mathsf{wp}[\![C'_{\text{loop}}]\!]\,([\neg\varphi]\cdot f)$ 的下界 l 充当。此类守卫强化会限制（可达）状态空间，因此，(i) 修改后的循环 C'_{loop} 具有更强的终止

性质（例如，变为几乎必然终止），并且 (ii) 一致可积性 l 和期望有界性也更容易验证。我们将说明，由于这些效果，我们的证明规则

(a) 通用性（第6.1节和 6.2）：适用于发散的 C_{loop} 和无界的 $f, l \in \mathbb{E}$，现有规则（如定理 8 和 10）无法处理这类情况；即使 C_{loop} 几乎必然终止，它也能证明一个对于 C_{loop} 而言并非一致可积的下界 l（因此超出了 Hark 等人的下界归纳规则 [Hark 等人 2020] 的适用范围）；此外，它还提供了一个用于证明一致可积性的正交充分判据。(b) 紧致性（第 6.3 节）：当 φ' 以适当方式趋近 φ 时，用 $\mathrm{wp}[\![C'_{\text{loop}}]\!]([\neg\varphi]\cdot f)$ 近似 $\mathrm{wp}[\![C_{\text{loop}}]\!](f)$ 所产生的误差趋于零；(c) 可自动化（第 6.4 节）：当 C'_{loop} 具有有限状态空间时，通过概率模型检测可以实现自动化——前提是进行适当的强化。

注。式 (14) 中守卫强化规则的完备性显而易见：如果 l 是 $\mathrm{wp}[\![C_{\text{loop}}]\!](f)$ 的一个下界，那么总存在某个 φ' 强化 φ，使得 l 是 $\mathrm{wp}[\![C'_{\text{loop}}]\!]([\neg\varphi]\cdot f)$ 的一个下界，因为我们总可以选择 $\varphi' = \varphi$，从而得到 $\mathrm{wp}[\![C'_{\text{loop}}]\!]([\neg\varphi]\cdot f) = \mathrm{wp}[\![C_{\text{loop}}]\!](f)$。然而，不应将这一完备性论证视为对我们的证明规则绝对普适性的刻画，因为选择 $\varphi' = \varphi$ 并不能使非几乎必然终止循环变为几乎必然终止。我们指出，要刻画证明规则的绝对普适性并非易事，因为这在很大程度上取决于守卫强化的“质量”，而守卫强化又可能依赖专家知识。尽管如此，我们仍在第 6.4 节提供了实用的启发式方法，以便找到一个“良好”的强化。◁

注。 我们的守卫强化规则 (14) 也适用于 非概率 循环 C_{loop}。在这种情况下，最弱前期望变换器退化为 Dijkstra [1975, 1976] 的最弱前置条件变换器，l 且 f变为按 ═══部分排序的谓词，而 $\cdot$ 则变为 $\wedge$。因此，我们的证明规则能够验证一个下近似 l，即满足以下条件的 初始状态集合：程序C_{loop} 必定终止于满足 f 的状态。

6.1 对可能不终止程序的应用

我们的守卫强化规则将验证 $l \preceq$ 最弱前置条件$[\![C_{\text{loop}}]\!](f)$ ——其中 C_{loop} 可能不有界 f，也可能发散——$l \in \mathbb{E}$ 归约为验证 $l \preceq$ 最弱前置条件$[\![C'_{\text{loop}}]\!]([\neg\varphi]\cdot f)$。若要对后者应用现有的下界归纳规则，就必须证明修改后的循环几乎必然终止 C'_{loop}，和/或证明期望有界性。要证明几乎必然终止，可以采用基于超鞅的成熟技术，例如 [Chatterjee 等人，2020；McIver 等人，2018；Moosbrugger 等人 2021]。然而，得益于我们的守卫强化技术，往往只需采用一种新颖而简单的论证，无须寻找精细调优的超鞅，即可证明 C'_{loop}几乎必然终止：

引理 15（几乎必然终止见证）。 给定 $C'_{\text{loop}} =$while循环 $(\varphi')\{C\}$，设 $T^{\neg\varphi'}$ 为 C'_{loop}的循环时间。若存在 $N \in \mathbb{N}$ 和 $p \in (0,\ 1)$，使得对于任意初始状态 $\sigma \in \Sigma$，

$$ {}^{\sigma}\mathbb{P}\left(T^{\neg\varphi'} > N\right) \ \leq\ p\,, \tag{15}$$

那么 C'_{loop} 几乎必然终止。

证明（概要）。只需证明尾概率 ${}^{\sigma}\mathbb{P}(T^{\neg\varphi'} > n)$（例如，参见 [Sankara-narayanan 2020]），即 C'_{loop} 在 $n \in \mathbb{N}$ 步内未终止的概率会随 n指数级下降。接着，将 n无限次地向前推，我们得到 ${}^{\sigma}\mathbb{P}(T^{\neg\varphi'} < \infty) = 1 - \lim_{n\to\infty} {}^{\sigma}\mathbb{P}(T^{\neg\varphi'} > n) \geq 1 - 0 = 1$。因此，$C'_{\text{loop}}$ 几乎必然终止。详尽证明见附录 C.4。□

注。如何刻画循环 C_{loop} 这一类循环，使其存在满足C'_{loop} 引理 15 中几乎必然终止判据的强化对应形式引理 15，仍是一个有趣的开放问题。这也可能有助于刻画我们上述证明规则的绝对一般性。◁

存在半自动化方法，例如 [Chatterjee 等人 2016a], ，可通过 排序超鞅 来证明非终止概率呈指数级下降。然而，在我们的设定中，引理 15 或许更容易验证，因为在加强守卫条件（例如，对变量设定上界；参见 第 6.4 节）之后，通常可以直接从含有（某些）有界变量的修改后程序中读出式 (15) 中的常数 N 和 p。事实上，对于本文给出的(15) 所有示例，引理 15 都足以证明修改后的循环几乎必然终止；此外，它还提供了一个建立一致可积性的额外充分条件，这与定理 9 相互独立（参见 第6.2节）。

例 16 **（一维偏置随机游走，基于 $\mathbb{Z}$ [McIver 等人 2018]）**。回顾第 2 节中的示例：

$$C_{1\text{dbrw}}: \quad \texttt{while}\,(n>0)\,\{\,n \coloneqq n-1\ [1/3]\ n \coloneqq n+1\,\}\ .$$

该循环一旦到达满足以下条件的状态，就会终止： σ满足 $\sigma(n)$。 ≤ 0我们希望为 $C_{1\text{dbrw}}$ 的终止概率建立非平凡下界，也就是说，为 最弱前置条件$[\![C_{1\text{dbrw}}]\!]\,(f)$ 满足$f=1$时建立下界。然而，现有证明规则均不适用：(i) $C_{1\text{dbrw}}$ 由于其存在偏向性，它并非几乎必然终止（例如参见 [McIver 等人 2018]），因此 Hark 等人的下界归纳法 [Hark 等人 2020] 不适用；此外，(ii) 应用 McIver 和 Morgan 的下界归纳法 [McIver 和 Morgan 2005] 也毫无意义，因为拥有（终止概率的下界）——也就是我们试图推导的量——本身就是应用该规则的前提条件之一（参见定理10）。

现在，我们将展示如何使用守卫强化规则来验证 $\text{wp}[\![C_{1\text{dbrw}}]\!]\,(1)$ 的非平凡下界。为此，对于任意固定的 $M\in\mathbb{N}$，我们将 $C_{1\text{dbrw}}$ 的守卫条件（$n>0$）强化为 $\varphi^M=$（$0<n<M$），从而得到一个修改后的循环，它与 $C_{1\text{dbrw}}$ 的区别仅在于守卫条件：

$$C^M_{1\text{dbrw}}: \quad \texttt{while}\,(0<n<M)\,\{\,n \coloneqq n-1\ [1/3]\ n \coloneqq n+1\,\}\ .$$

我们的证明规则断言，对于任意固定的 $M\in\mathbb{N}$，$\text{wp}[\![C^M_{1\text{dbrw}}]\!]([n\leq 0]\cdot 1)$ 的一个下界足以作为 $\text{wp}[\![C_{1\text{dbrw}}]\!]\,(1)$ 的下界。由于 $C^M_{1\text{dbrw}}$ 以概率 $(2/3)^{M-1}$ 在连续向右移动至多 $M-1$ 步后终止，因此对于任意初始状态 $\sigma(n)\in\mathbb{Z}$，都有 ${}^{\sigma}\mathbb{P}\big(T^{\neg\varphi^M}>M\big)<1-(2/3)^{M-1}$。因此，根据引理 15，$C^M_{1\text{dbrw}}$ 几乎必然终止。由此，我们可以尝试应用 Hark 等人的下界归纳法，为 $\text{wp}[\![C^M_{1\text{dbrw}}]\!]([n\leq 0]\cdot 1)$ 求一个下界。令

$$l_M \;=\; [n<0]+[0\leq n\leq M]\cdot\Big((1/2)^n-(1/2)^M\Big)\ .$$

这很直 观易于验证（见附录 D.1），对于任意固定的 $M\in\mathbb{N}$， l_M 是一个次不变式，即 .,

$$l_M \;\leq\; \Phi^M_g\,(l_M)$$

其中 $g=[n\leq 0]\cdot 1$ 是受限后期望，而 Φ^M_g是 $C^M_{1\text{dbrw}}$ 关于 g的特征函数。此外， l_M 有上界 1，因此根据 $C^M_{1\text{dbrw}}$ 满足定理（c）这一条件，定理 9中的

$$\begin{aligned} l_M \;&\leq\; \text{wp}[\![C^M_{1\text{dbrw}}]\!]\,([n\leq 0]\cdot 1) && \text{[根据 Hark 等人的归纳法，参见定理 8]}\\ &\leq\; \text{wp}[\![C_{1\text{dbrw}}]\!]\,(1)\ . && \text{[根据守卫强化规则，参见定理 14]}\end{aligned}$$

因此我们得出结论：对于任意固定的 $M\in\mathbb{N}$， l_M 是 $\text{wp}[\![C_{1\text{dbrw}}]\!](1)$ 的下界。特别地，通过将 M 无限推进——从而得到可能的最紧界；不过，要建立一个有效的下界，这一步并非必要——我们得到

$$\text{wp}[\![C_{1\text{dbrw}}]\!]\,(1) \;\geq\; \lim_{M\to\infty} l_M \;=\; [n<0]+[n\geq 0]\cdot(1/2)^n\ ,$$

也就是说，$l_\infty = [n<0] + [n\geq 0]\cdot(1/2)^n$ 是 $\mathsf{wp}[\![C_{\mathrm{1dbrw}}]\!]\,(1)$ 的下界。事实上，对于这个特定示例，可以验证（见附录 D.1），l_∞ 是一个超不变式，即 $\Phi_f(l_\infty)\preceq l_\infty$，其中 Φ_f 是相对于后期望 $f=1$ 的 C_{1dbrw} 的特征函数。因此，根据 Park 归纳法（参见定理5），l_∞ 也是 $\mathsf{wp}[\![C_{\mathrm{1dbrw}}]\!]\,(1)$ 的上界。由此我们可以断言，Φ_f 的精确最小不动点，即从初始位置 n 开始时 C_{1dbrw} 的精确终止概率，是

$$\mathsf{wp}[\![C_{\mathrm{1dbrw}}]\!]\,(1) \;=\; l_\infty \;=\; [n<0] + [n\geq 0]\cdot(1/2)^n\ .$$

最后，我们指出，本例中的推理过程适用于更一般形式的一维随机游走，其偏置概率为参数化的 $p\in[0,1/2)$，其精确终止概率可以证明为 $[n<0]+[n\geq 0]\cdot(p/1-p)^n$。◁

接下来，我们通过以下示例说明，即使目标循环 C_{loop} 几乎必然终止，$\mathsf{wp}[\![C_{\mathrm{loop}}]\!]\,(f)$ 的一个真实下界也未必对 C_{loop}一致可积，因此无法通过 Hark 等人的下界归纳规则来获得；然而，我们的守卫强化规则能够证明这样的下界。

示例 17（伯努利的圣彼得堡悖论 [伯努利 1954]）。考虑以下循环C_{pd}，它通过公平抛硬币来模拟一场彩票游戏：赌注 $b\in\mathbb{Z}_{>0}$ 每当出现正面时便翻倍；首次出现反面时，游戏结束，玩家赢得池中全部赌注：

$$C_{\mathrm{pd}}\colon\quad \texttt{while}\,(\,a=1\,)\,\{\,a\coloneqq 0\ [1/2]\ b\coloneqq 2\cdot b\,\}\ .$$

我们旨在为该彩票的期望收益建立非平凡下界，即在 $f=b$ 条件下，为 $\mathsf{wp}[\![C_{\mathrm{pd}}]\!]\,(f)$ 建立下界。由于 C_{pd} 以概率 $1/2$, 将 a 设为 0 后终止，因此对于任意初始状态 σ，我们都有 ${}^{\sigma}\mathbb{P}(T^{a\neq 1}>1)\ <1/2$。因此，根据引理 15，$C_{\mathrm{pd}}$ 几乎必然终止。然而，真正的下界 $l_\infty=([a\neq 1]\cdot b+[a=1]\cdot\infty)\not<\infty$——这正是我们最终希望验证的下界——对于 C_{pd}并非一致可积，因此无法通过 Hark 等人的下界归纳规则处理（详细论证见 [Hark 等人 2019，附录A]）。

为了应用我们的新证明规则，我们将 C_{pd} 的守卫条件（$a=1$）强化为：对于任意固定的 $M\in\mathbb{Z}_{>0}$，均满足 $\varphi^M=(a=1\wedge b<M)$，从而得到修改后的循环：

$$C_{\mathrm{pd}}^M\colon\quad \texttt{while}\,(\,a=1\wedge b<M\,)\,\{\,a\coloneqq 0\ [1/2]\ b\coloneqq 2\cdot b\,\}\ .$$

我们的证明规则断言，对于任意固定的 $M\in\mathbb{Z}_{>0}$，$\mathsf{wp}[\![C_{\mathrm{pd}}^M]\!]\,([a\neq 1]\cdot b)$ 的下界足以作为 $\mathsf{wp}[\![C_{\mathrm{pd}}]\!]\,(b)$ 的下界。程序 C_{pd}^M 显然是几乎必然终止的（理由与 C_{pd}相同）；事实上，其循环时间 $T^{\neg\varphi^M}$ 肯定有 $\lceil\log_2 M\rceil$ 作为上界，因此根据定理 9 的条件 (a)，对于 C_{pd}^M，任意期望 $h\ll\infty$ 都是一致可积的（因为对于任意 $n\in\mathbb{N}$，$\mathsf{wp}[\![C]\!]^n(h)\ll\infty$ 都由 $h\ll\infty$ 和无循环体 C 平凡地满足，C_{pd}^M 就是这种情况）。令

$$l_M \;=\; [a\neq 1]\cdot b+\sum_{i=1}^{\lceil\log_2 M\rceil}[a=1\wedge(M/2^i\leq b<M/2^{i-1})]\cdot i\cdot b/2\ .$$

显然 可前往查看（参见 附录 D.2），对于任意固定的 $M\in\mathbb{Z}_{>0}$，l_M是一个次不变式，即，

$$l_M\ \preceq\ \Phi_g^M(l_M)$$

其中 $g=[a\neq 1]\cdot b$是受限后期望，且 Φ_g^M是 C_{pd}^M相对于 g的特征函数。由于 $l_M\ll\infty$对于 C_{pd}^M一致可积，根据 定理 8 和 14，我们有

$$l_M\ \preceq\ \mathsf{wp}[\![C_{\mathrm{pd}}^M]\!]\,([a\neq 1]\cdot b)\ \preceq\ \mathsf{wp}[\![C_{\mathrm{pd}}]\!]\,(b)$$

对任意固定的 $M\in\mathbb{Z}_{>0}$均成立。因此，当 M趋于无穷时，

$$\mathsf{wp}[\![C_{\mathrm{pd}}]\!]\,(b)\ \geq\ \lim_{M\to\infty} l_M\ =\ [a\neq 1]\cdot b+[a=1]\cdot\infty\ =\ l_\infty\ .$$

类比例16，可以进一步证明 l_∞ 足以作为一个超不变式，并最终得出最弱前置条件$[\![C_{\mathrm{pd}}]\!](b) = l_\infty$，也就是说，在终止时 b 的精确期望值。◁

6.2 一致可积性的正交充分条件

例16 和 17 展示了如何利用现有的一致可积性充分判据（参见 最弱前置条件$[\![C_{\mathrm{loop}}]\!](f)$，为修改后的循环建立下界 C'_{loop}。事实上， C'_{loop} 通常具有强且易于检验的终止性质（参见引理 15），因此可以采用另一种充分条件来证明一致可积性（证明见 附录C.5）：

定理 18（一致可积性的正交充分判据）。假设 C'_{loop} =while循环 $(\varphi')\{C\}$满足 引理 15中的几乎必然终止条件。则，当 $h \lll \infty$满足 C'_{loop} 时，期望 C'_{loop} 具有有界更新性质[10],，即存在 $c \in \mathbb{R}_{\geq 0}$ 使得对于任意 $\sigma \in \Sigma$， ${}^{\sigma}\mathbb{P}(\forall n \in \mathbb{N}\colon |X_{n+1} - X_n| \leq c) = 1$；并且 h有一个多项式期望上界[11]时，该期望一致可积。

定理 18 中关于一致可积性的充分判据定理 18与定理 9中的条件正交，尤其是与其中的条件(b) 正交：我们的新充分条件利用了这样一个事实： C'_{loop}采用强化守卫条件的程序往往具有强大且易于检验的终止性质（参见引理 15）；它仅适用于具有有界更新性质的循环，但将 h 的条件差有界性放宽为 h的多项式有界性。我们的新充分判据通常比更容易检验(b) 中的条件定理 9，具体而言：(i) 若 C'_{loop} 具有无循环体，则可以直接从 C'_{loop}的语法中看出其有界更新性质；(ii) 任意（分段）多项式期望 h 都满足多项式有界条件。下面的例子展示了一种情形：虽然定理 9中的条件定理 9 都不足以证明一致可积性，但我们在定理 18中的（正交）充分条件可以做到。

例19（有界更新的一维对称随机游走）。考虑以下循环 C_{bu}，其模拟了 $\mathbb{Z}$上的对称化一维随机游走；此外，以概率 $1/2$，每次向左（分别向右）移动时，我们将 $b \in \mathbb{R}_{\geq 0}$ 的值增加（分别减少）2：

$$C_{\mathrm{bu}}\colon \quad \texttt{while}\,(n > 0)\,\{\,\{n := n-1 \mathbin{;} b := b+2\}\ [1/2]\ \{n := n+1 \mathbin{;} b := b-2\}\,\}\ .$$

我们希望证明终止时 b 的期望值的非平凡下界，即证明 $\mathrm{wp}[\![C_{\mathrm{bu}}]\!]\ (f)$ 的下界，其中 $f = b$。注意， C_{bu} 与标准一维对称随机游走表现出完全相同的终止行为， [McIver 等人 2018], 指出， C_{bu} 该随机游走几乎必然终止，但其期望循环时间 是无穷的。此外，候选下界$l_\infty = [n < 0] \cdot b + [n \geq 0] \cdot (b + 2 \cdot n)$ ——这正是我们最终希望验证的下界——是无界的，因此无法通过 Hark 等人的下界归纳法得到（因为 定理 9 不足以证明 l_∞的一致可积性）。

为应用我们的新证明规则，对于任意固定的 $M \in \mathbb{Z}_{>0}$，我们将 C_{bu} 的守卫条件（$n > 0$）加强为 $\varphi^M = (0 < n < M)$，从而得到修改后的循环：

$$C^M_{\mathrm{bu}}\colon \quad \texttt{while}\,(0 < n < M)\,\{\,\{n := n-1 \mathbin{;} b := b+2\}\ [1/2]\ \{n := n+1 \mathbin{;} b := b-2\}\,\}\ .$$

我们的证明规则断言，对于任意固定的 $M \in \mathbb{Z}_{>0}$，只要 $\mathrm{wp}[\![C^M_{\mathrm{bu}}]\!]\,([n \leq 0] \cdot b)$ 有下界，该下界就足以作为 $\mathrm{wp}[\![C_{\mathrm{bu}}]\!](b)$ 的下界。令

$$l_M \ = \ [n < 0] \cdot b + [0 \leq n \leq M] \cdot (b + 2 \cdot n) \cdot (1 - n/M)\ .$$

容易验证，对于任意固定的 $M \in \mathbb{Z}_{>0}$， l_M是一个次不变式（见 附录 D.3）。由于 C^M_{bu}至多在 $M-1$ 步连续递增 n 后以概率 $(1/2)^{M-1}$终止，因此我们

[10]有界更新性质已用于分析非确定性概率程序的期望成本 [Wang 等人 2019]；它包含常概率程序这一类 [Giesl 等人 2019]。[11]可以用 (ii')(ii) 替换 (ii') h 有一个有界的分段多项式期望，且定理仍然成立。

有 ${}^{\sigma}\mathbb{P}(T^{\neg\varphi^M} > M) < 1-(1/2)^{M-1}$，对于任意初始状态 $\sigma(n) \in \mathbb{Z}$。因此，根据 引理 15， C_{bu}^M 几乎必然终止。尽管如此，定理 9 中的条件仍然都不足以证明 l_M 对 C_{bu}^M一致可积：循环时间 $T^{\neg\varphi^M}$并非几乎必然有界， l_M由于其无界变量而无界， b且 l_M并非条件差有界（见 附录 D.3 ）。

然而，显然定理 18中的（正交）充分判据得到满足，从而证明了 l_M 对于 C_{bu}^M的一致可积性： C_{bu}^M 具有有界更新性质，因为它具有一个仅含有界更新的无循环体；此外， l_M 满足多项式有界条件，因为对于任意固定的 $M \in \mathbb{Z}_{>0}$， l_M 是关于 n 和 b的分段多项式。因此，根据定理 8 和14，对于任意固定的 $M \in \mathbb{Z}_{>0}$，我们有

$$l_M \;\le\; \mathrm{wp}[\![C_{\mathrm{bu}}^M]\!]\,([n \le 0]\cdot b) \;\le\; \mathrm{wp}[\![C_{\mathrm{bu}}]\!]\,(b)\ .$$

通过将 M 无限推进，我们最终可以证实下界 l_∞：

$$\mathrm{wp}[\![C_{\mathrm{bu}}]\!]\,(b) \;\ge\; \lim_{M\to\infty} l_M \;=\; [n<0]\cdot b + [n\ge 0]\cdot(b+2\cdot n) \;=\; l_\infty\ . \qquad \triangleleft$$

6.3 守卫强化规则的紧确性

接下来，我们讨论守卫强化规则所引入的误差，即最弱前置条件$[\![C_{\mathrm{loop}}]\!]\,(f)$ 与根据 l 定理 14所建立的下界之间的差异。为此，请注意

$$\mathrm{wp}[\![C_{\mathrm{loop}}]\!]\,(f) - l \;=\; \underbrace{\left(\mathrm{wp}[\![C_{\mathrm{loop}}]\!]\,(f) - \mathrm{wp}[\![C'_{\mathrm{loop}}]\!]\,([\neg\varphi]\cdot f)\right)}_{\text{error incurred by guard strengthening, } \ge 0} + \underbrace{\left(\mathrm{wp}[\![C'_{\mathrm{loop}}]\!]\,([\neg\varphi]\cdot f) - l\right)}_{\text{error incurred in the reduced problem, } \ge 0} \tag{16}$$

其中，右侧的第一项表示守卫强化技术本身固有的误差，而第二项则表示将最弱前置条件 $[\![C'_{\mathrm{loop}}]\!]\,([\neg\varphi]\cdot f)$ 低估为 l 时产生的误差，这与证明规则本身无关。下文将量化第一项，即强化守卫条件所产生的误差。

引理 20。 给定循环 $C_{\mathrm{loop}} = \texttt{while}(\varphi)\{C\}$和 $C'_{\mathrm{loop}} = \texttt{while}(\varphi')\{C\}$，假设 $\varphi' \Longrightarrow \varphi$，那么对于任意后期望 $f \in \mathbb{E}$，

$$\mathrm{wp}[\![C_{\mathrm{loop}}]\!]\,(f) - \mathrm{wp}[\![C'_{\mathrm{loop}}]\!]\,([\neg\varphi]\cdot f) \;\le\; \mathrm{wp}[\![C'_{\mathrm{loop}}]\!]\,([\varphi]) \cdot \sup_{\sigma\models\neg\varphi'\wedge\varphi} \mathrm{wp}[\![C_{\mathrm{loop}}]\!]\,(f)\,(\sigma)\ .$$

证明（概要）。 如推论 13的附录 C.2证明中所示，我们有

$$\mathrm{wp}[\![C_{\mathrm{loop}}]\!]\,(f) - \mathrm{wp}[\![C'_{\mathrm{loop}}]\!]\,([\neg\varphi]\cdot f) \;=\; \lambda\sigma.\ \int_A f_{C_{\mathrm{loop}}}\ \mathrm{d}\left({}^{\sigma}\mathbb{P}\right)\ .$$

因此，只需对右侧的积分进行界定，这可以通过考察 A中的轨迹片段（由守卫违反所见）来实现。详情参见附录 C.6。 □

由 引理 20 可直接得出我们守卫强化规则的 紧确性，也就是说，通过低估 最弱前置条件$[\![C_{\mathrm{loop}}]\!]\,(f)$ 得到 最弱前置条件$[\![C'_{\mathrm{loop}}]\!]\,([\neg\varphi]\cdot f)$ 所产生的误差，在 φ' 以适当方式趋近于 φ时趋近于零：

定理 21（守卫强化的紧致性）。 给定 $C_{\mathrm{loop}} = \text{while循环}(\varphi)\{C\}$，假设存在一个守卫条件序列 $\{\varphi^m\}_{m\in\mathbb{N}}$，使得 $\forall m \in \mathbb{N}$： $\varphi^m \Longrightarrow \varphi$。令 $C_{\mathrm{loop}}^m = \text{while循环}(\varphi^m)\{C\}$。若以下两个条件之一成立：

(a) $\lim_{m\to\infty} \sup_{\sigma\models\neg\varphi^m\wedge\varphi} \mathrm{wp}[\![C_{\mathrm{loop}}]\!]\,(f)\,(\sigma) < \infty$ and $\lim_{m\to\infty} \mathrm{wp}[\![C_{\mathrm{loop}}^m]\!]\,([\varphi]) = 0$,
(b) $\lim_{m\to\infty} \sup_{\sigma\models\neg\varphi^m\wedge\varphi} \mathrm{wp}[\![C_{\mathrm{loop}}]\!]\,(f)\,(\sigma) = 0$,[12]

[12]N注意，$\mathrm{wp}[\![C_{\mathrm{loop}}^m]\!]\,([\varphi])$ 将状态映射为一个概率，因此 $\lim_{m\to\infty} \mathrm{wp}[\![C_{\mathrm{loop}}^m]\!]\,([\varphi]) \le 1 \ll \infty$。

th此外，通过使用 φ^m 强化 φ 所产生的误差会随着 m 趋近于 ∞ 而收敛至零，即 .,

$$\mathrm{wp}[\![C_{\mathrm{loop}}]\!]\,(f) \;=\; \lim_{m\to\infty} \mathrm{wp}[\![C_{\mathrm{loop}}^m]\!]\,([\neg\varphi]\cdot f)\ .$$

注。在某些情况下，定理 21 中的条件 (a) 和 (b) 均不成立：回顾第 2 节给出的一维随机游走，并考虑例如如下的守卫条件序列 $\{\varphi^m\}_{m\in\mathbb{N}}$ 其中$\varphi^m = (0 < n < 9 + (2^m{-}1)/2^m)$。我们有 $\lim_{m\to\infty}\varphi^m = (0 < n < 10)$ 和 $\forall m \in \mathbb{N}\colon\ \varphi^m \implies \varphi$。然而，可以验证 (a) 和 (b) 均不成立（因为 $\{\varphi^m\}_{m\in\mathbb{N}}$ 根本没有趋近于 φ）。◁

条件 (a) 和 (b) 在 定理 21 中，可以通过对其中最弱前期望的上界进行证明来检验，例如使用 Park 归纳法，正如下例所示。

例 22。 重新考虑概率循环 $C_{1\mathrm{dbrw}}$和 $C_{1\mathrm{dbrw}}^M$，其后期望为 $f = 1$，在例16中。借助 Park 归纳法，我们已经证明 $l_\infty = [n < 0] + [n \geq 0]\cdot(1/2)^n$与以下程序的精确终止概率 $C_{1\mathrm{dbrw}}$ 从初始位置 n开始时相一致最弱前置条件$[\![C_{1\mathrm{dbrw}}]\!](1) = l_\infty \ll \infty$。因此，根据 (16)，我们已经可以得出其紧确性，即

$$\mathrm{wp}[\![C_{1\mathrm{dbrw}}]\!]\,(1) \;=\; \lim_{M\to\infty} \mathrm{wp}[\![C_{1\mathrm{dbrw}}^M]\!]\,([n \leq 0]\cdot 1)\ .$$

我们现在说明可以通过 （b）条件引理 21得出相同的结论。注意 t

$$\begin{aligned}
\lim_{M\to\infty}\ \sup_{\sigma\models\neg\varphi^M\wedge\varphi} \mathrm{wp}[\![C_{1\mathrm{dbrw}}]\!]\,(1)\,(\sigma) \;&=\; \lim_{M\to\infty}\ \sup_{\sigma\models n\geq M} \mathrm{wp}[\![C_{1\mathrm{dbrw}}]\!]\,(1)\,(\sigma)\\
&\leq\; \lim_{M\to\infty}\ \sup_{\sigma\models n\geq M} ([n<0] + [n\geq 0]\cdot(1/2)^n)\,(\sigma)\\
&\qquad\qquad [\text{by } \mathrm{wp}[\![C_{1\mathrm{dbrw}}]\!]\,(1) \leq l_\infty]\\
&=\; \lim_{M\to\infty}\ \sup_{\sigma\models n\geq M} ((1/2)^n)\,(\sigma)\\
&=\; \lim_{M\to\infty} (1/2)^M \;=\; 0\ .
\end{aligned}$$

因此，根据（b）条件引理 21，强化 φ 为 φ^M 所产生的误差会随着 M 趋近于 ∞而趋于零。◁

6.4 守卫强化规则的自动化

我们简要讨论自动化守卫强化规则的可能性，以便寻找（而不仅仅是验证）最弱前期望的下界。这种自动化需要解决两个问题：（i）如何找到一个“良好”的守卫强化，即 $\varphi' \implies \varphi$? （ii）如何为修改后的循环$C'_{\mathrm{loop}}$生成一个非平凡的下界?

如何找到“良好”的强化？从逻辑强度来看，良好的修改后守卫条件 φ'不能过强，否则只能推导出平凡的下界（可以考虑 $\varphi' = \mathtt{false}$）；也不能过弱，否则所得循环 C'_{loop} 可能无法满足关于终止（参见引理 15）和一致可积性（参见定理 9和18）的条件。一般而言，很难找到——甚至难以刻画——“最佳”强化 $\varphi' \implies \varphi$。不过，一种简单的强化模式，即仅对程序变量的一个子集进行界定，事实证明相当有效，也就是说，$\mathcal{V} \subseteq \mathtt{Vars}$:

$$\varphi' \;=\; \varphi \wedge \bigwedge\nolimits_{x\in\mathcal{V}} x \diamond c\ ,$$

其中 c是一个常数，且 $\diamond \in \{<、\ >、\ \leq、\ \geq、\ =\}$。子集 $\mathcal{V} \subseteq \mathtt{Vars}$ 的选取方式应使得 C'_{loop} 满足我们对终止和一致可积性的条件。这种强化模式确实是一种启发式方法，但足以为 φ' 本文介绍的所有示例生成良好的强化守卫（含义如上文所述）——以下情况除外：第 8 节 中我们

讨论朴素强化模式的局限性。研究一种可能更先进、更巧妙的守卫强化策略，将留待未来工作。

如何为 C'_{loop} 生成非平凡下界？由于 C'_{loop} 具有良好的性质，例如终止性，因此可以借助各种（半）自动化技术来合成最小不动点的下界，从而发现所需的 $\text{wp}[\![C'_{\text{loop}}]\!]([\neg\varphi]\cdot f)$ 下界。在概率情形下，这些技术包括：基于约束求解的方法 [Chen 等人 2015；Feng 等人 2017；Katoen 等 2010]，以及不变式学习方法 [Bao 等人 2022]，用于生成概率程序最弱前期望的下界；递推求解方法 [Bartocci 等人2019]，用于合成（可解）概率循环的基于矩的不变式；以及各种形式的值迭代 [Baier 等，2017；Hartmanns 和 Kaminski, 2020；Quatmann 和 Katoen 2018]，用于确定马尔可夫模型中的可达概率。特别是，我们指出了一种特殊情形，在这种情形下，可以通过概率模型检测计算出精确的最小不动点：

定理 23（归约为概率模型检验 [Baier 和 Katoen, 2008，第 10]**章）**。给定 $C'_{\text{loop}} =$ while循环 $(\varphi')\{C\}$ 以及后期望 $g \in \mathbb{E}$，如果 C'_{loop} 具有有限可达状态集，那么 最弱前置条件 $[\![C'_{\text{loop}}]\!](g)$ 可以通过求解线性方程组精确计算。

定理23 成立，因为有限状态循环 C'_{loop} 可以展开为有限状态马尔可夫链 $\mathcal{M}$，而最弱前置条件 $[\![C'_{\text{loop}}]\!](g)$ 与由 $\mathcal{M}$ 导出的线性方程组的唯一解一致，其中的奖励用于对 g [Baier 和 Katoen, 2008，第 10]，章进行建模；概率模型检查器（例如 Storm [Dehnert 等人 2017],PRISM [Kwiatkowska 等人 2002]）可以对其进行符号计算。

将我们的守卫强化规则与 定理23 结合起来，可通过对有限状态概率模型进行模型检验，推断无限状态概率程序的定量性质：

例 24（$\mathbb{Z}^3$ [McCrea 和 Whipple, 1940；Montroll 1956]）。考虑循环 C_{3dsrw}，它刻画了在 $\mathbb{Z}^3$ 上的三维格点对称随机游走：

$$C_{\text{3dsrw}}\text{: while } (\ x \neq 0 \vee y \neq 0 \vee z \neq 0\ )\ \{\ x \coloneqq x-1 \ \oplus\ x \coloneqq x+1 \ \oplus\ y \coloneqq y-1 \ \oplus\ y \coloneqq y+1 \ \oplus\ z \coloneqq z-1 \ \oplus\ z \coloneqq z+1 \}$$

其中，迭代的 $\oplus$ 是离散均匀选择的简写（此处每种选择的概率为 $1/6$）。其背后的随机性 C_{3dsrw} 本质上不同于 一维和二维情形：波利亚 [1921] 证明，随机游走在 $\mathcal{P}$ 时返回原点 (0,0,0)的概率严格小于 1，这表明 C_{3dsrw} 并非几乎必然终止。更准确地说， C_{3dsrw} 从原点任一相邻位置出发的终止概率为

$$\mathcal{P} \;=\; 1 - \left(\frac{3}{(2\pi)^3} \int_{-\pi}^{\pi}\int_{-\pi}^{\pi}\int_{-\pi}^{\pi} \frac{\mathrm{d}x\ \mathrm{d}y\ \mathrm{d}z}{3-\cos x-\cos y-\cos z} \right)^{-1} \;=\; 0.3405373296\ldots$$

这被称为波利亚随机游走常数之一。据我们所知，现有技术无法对 C_{3dsrw} 进行验证，因为其发散性质十分复杂。

现在我们展示如何利用概率模型检测，使用我们的守卫强化规则自动推导出 C_{3dsrw} 终止概率 P 的下界（即后期望为 $f=1$）。为此，我们首先用边长为 $2\cdot M$、 $M \in \mathbb{Z}_{>0}$ 固定的立方体界定可能的位置（x， y， z），从而得到修改后的循环：

$$C^{M}_{\text{3dsrw}}\text{:}\quad \texttt{while}\,(\,(x \neq 0 \vee y \neq 0 \vee z \neq 0) \wedge |x| < M \wedge |y| < M \wedge |z| < M\,)\,\{\ x \coloneqq x-1 \ \oplus\ x \coloneqq x+1 \ \oplus\ y \coloneqq y-1 \ \oplus\ y \coloneqq y+1 \ \oplus\ z \coloneqq z-1 \ \oplus\ z \coloneqq z+1 \}\ .$$

注意，从格点上的任意初始位置出发，修改后的随机游走 $C^M_{3\mathrm{dsrw}}$ 只能到达有限个位置，即它要么 (i) 逃出立方体或返回原点而终止，要么 (ii) 继续在立方体内游走。因此，根据定理23中的联系，简化后的最弱前置期望最弱前置条件$[\![C^M_{3\mathrm{dsrw}}]\!]([x=0\wedge y=0\wedge z=0]\cdot 1)$——它是终止概率 P 的下近似$C_{3\mathrm{dsrw}}$——可以通过现成的概率模型检查器进行符号计算。例如，图 6展示了PRISM[Kwiatkowska 等人 2002] 在不同的 M取值下生成的这类下近似（参见 X-轴）。特别是，图 6证实了我们先前关于紧确性的论断（参见定理 21）[13]：随着 M 增大，强化程度减弱，因此得到的实际终止概率$\mathcal{P}$下界会更加紧确。

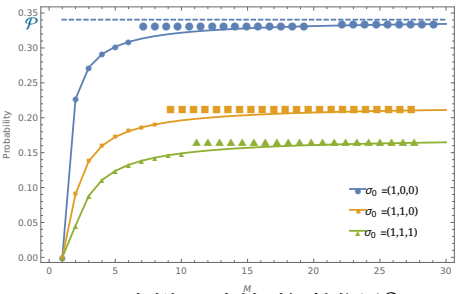

图 6. PRISM 在例 24 中针对初始位置C_3处的 dsrw 的终止概率 σ_0所计算出的下界。$\mathcal{P}\approx 0.34$ 表示从原点邻近位置（例如 $\sigma_0=(1,0,0)$）出发时的真实终止概率；其他初始位置的真实终止概率未知。

图 6 也印证了我们的直觉：行走者离原点越远，返回原点的概率就越低。◁

注。 在前文提到的特殊情形中，我们的问题可以归约为有限状态离散时间马尔可夫链的模型检验，此时我们的守卫强化规则在效果上类似于概率模型检测中所谓的部分探索技术 [Brázdil 等人 2014] 提出的方法。后者通过（部分）探索状态空间中逐步扩大的子集，构造一系列精度不断提高的近似（可达概率的下界和上界）。随着我们逐渐减弱强化程度以获得越来越紧的下界，这一过程会产生类似的效果。由于我们始终推导出安全的下近似，因此，我们的技术可用于生成关键子系统 [Ábrahám 等人2014]，以此作为概率验证中定量性质的反例。

7 案例研究

在本节中，我们介绍几个非平凡示例，以展示我们的守卫条件强化规则在建立最弱前期望的下界方面的有效性。这些示例包括具有连续分布、嵌套循环和状态依赖概率的概率程序，以及一个现实世界中的随机化网络协议。这些都是无限状态程序；对于其中一些程序，我们的证明规则可以通过证明 1 是终止概率的下界，来证明其几乎必然终止。

示例 25（连续采样）。考虑以下循环 C_{cs}，它模拟一个一维随机游走，其中分支概率取自区间 (0，1) 上的连续均匀分布。

C_{cs}：while（$n>0$）$\{p:\approx$ uniform（0，1）$;\{n:=n-1;b:=b+$uniform（0，1）$\}\ [p]\{n:=n+1;b:=b-$uniform（0，1）$\}\}$。

我们旨在验证 $l_\infty=[n<0]\cdot b+[n\geq 0]\cdot(b+1/2\cdot n)$ 是 b终止时的期望值下界，即 $l_\infty\preceq \mathrm{wp}[\![C_{\mathrm{cs}}]\!](b)$。注意，$l_\infty$无界；此外，$C_{\mathrm{cs}}$的行为——

[13]要严格证明这个例子的紧确性，需要找到一个合适的超不变式——就像我们在示例 22中所做的那样，但现在针对的是三维随机游走——这极其困难，超出了本文的讨论范围。

期望——与标准一维对称随机游走相同 [McIver 等人 2018] 因此几乎必然终止，但其期望循环时间却是无限的。因此，现有的证明规则不适用。

现在，我们将$(n > 0)$的C_{cs}守卫条件加强为$\varphi^M = (0 < n < M)$，其中$M \in \mathbb{Z}_{>0}$为任意固定值，并将如此得到的循环记为C_{cs}^M。可以证明（参见附录 D.4）：

$$l_M \;=\; [n < 0] \cdot b + [0 \le n \le M] \cdot (b + 1/2 \cdot n) \cdot (1 - n/M)$$

是一个次不变式，即$l_M \le \Phi_g^M(l_M)$，其中$g = [n \le 0] \cdot b$是受限后期望，而Φ_g^M是相对于g的C_{cs}^M的特征函数。此外，C_{cs}^M在连续递增n至多$M-1$步后终止的概率至少为$(1/2 \cdot 1/2)^{M-1}$（即先抽取$p \in (1/2, 1)$，再选择正确的分支），因此，对于任意初始状态$\sigma(n) \in \mathbb{Z}$，我们有${}^{\sigma}\mathbb{P}\big(T^{\neg\varphi^M} > M\big) < 1 - (1/4)^{M-1}$。于是，根据引理 15，$C_{\text{cs}}^M$几乎必然终止。此外，根据定理 18 中新的充分条件，C_{cs}^M关于C_{cs}^M一致可积。因此，对于任意固定的$M \in \mathbb{Z}_{>0}$，可得$l_M \le \mathsf{wp}[\![C_{\text{cs}}^M]\!]([n \le 0] \cdot b) \le \mathsf{wp}[\![C_{\text{cs}}]\!](b)$。最终，我们可以通过将$M$不断向前推，认证下界$l_\infty$：

$$\mathsf{wp}[\![C_{\text{cs}}]\!](b) \;\ge\; \lim_{M\to\infty} l_M \;=\; [n < 0] \cdot b + [n \ge 0] \cdot (b + 1/2 \cdot n) \;=\; l_\infty\,. \qquad \lhd$$

例 26（嵌套循环）。考虑程序C_{nl}，其中包含两个嵌套循环（外层循环根据内层循环的结果修改$n \in \mathbb{Z}$；$a,\ b \in \mathbb{Z}_{>0}$是满足条件$a > b$[14]的参数）：

$$\begin{aligned} C_{\text{nl}}\colon\quad & \texttt{while}\,(n > 0)\,\{ \\ & \quad k \coloneqq n\,; \\ & \quad \texttt{while}\,(-a < k - n < b)\,\{k \coloneqq k-1\ [1/2]\ k \coloneqq k+1\}\,; \\ & \quad \texttt{if}\,(k < n)\,\{n \coloneqq n-1\}\,\texttt{else}\,\{n \coloneqq n+1\}\}\,. \end{aligned}$$

假设我们想要证明终止概率存在一个非平凡下界最弱前置条件$\mathsf{wp}[\![C_{\text{nl}}]\!](1)$。现有证明规则无法解决这个问题，因为$C_{\text{nl}}$并非几乎必然终止。为了应用我们的证明规则，我们将外层循环的守卫条件加强为$\varphi^M = (0 < n < M)$，其中$M \in \mathbb{Z}_{>0}$为任意固定值。修改后的程序C_{nl}^M几乎必然终止，理由与引理 15类似。令

$$l_M \;=\; [n < 0] + [0 \le n \le M] \cdot \left((b/a)^n - (b/a)^M\right)\,.$$

由于l_M有界，根据定理 8 和 14，我们知道l_M是C_{nl}的终止概率的下近似，如果l_M是C_{nl}^M的次不变式。在这种情况下，我们证明了下界l_∞:

$$\mathsf{wp}[\![C_{\text{nl}}]\!](1) \;\ge\; \lim_{M\to\infty} l_M \;=\; [n < 0] + [n \ge 0] \cdot (b/a)^n \;\triangleq\; l_\infty\,.$$

现在我们证明，l_M确实是C_{nl}^M的一个次不变式，即$l_M \le \Phi_g^M(l_M)$，其中$g = [n \le 0] \cdot 1$是受限后期望，而Φ_g^M是关于g的C_{nl}^M的特征函数。由于C_{nl}^M具有嵌套特征，在这种情况下验证次不变性更加复杂：还必须针对一个依赖于l_M的特定后期望，推理内层循环的下界。更准确地说，令C_{body}^M和C_{inner}^M分别表示C_{nl}^M的循环体和内层循环。我们有

$$\begin{aligned} \Phi_g^M(l_M) \;&=\; [n \le 0 \vee n \ge M] \cdot [n \le 0] + [0 < n < M] \cdot \mathsf{wp}[\![C_{\text{body}}^M]\!](l_M) \\ &=\; [n \le 0] + [0 < n < M] \cdot \\ &\qquad \mathsf{wp}[\![k \coloneqq n]\!]\left(\mathsf{wp}[\![C_{\text{inner}}^M]\!]([k < n] \cdot l_M\,[n/n-1] + [k \ge n] \cdot l_M\,[n/n+1])\right)\,. \end{aligned}$$

[14]该限制$a > b$使其成为C_{nl}一个非几乎必然终止的程序。

通过组合　利用这一事实（参见附录 D.5，其中给出了详细证明）：对于任意有界后期望 h，

$$\text{最弱前置条件}[\![C^M_{\text{inner}}]\!](h) \;\geq\; [(k-n<-a)\ \vee (k-n>b)]\cdot\ h + [-a\leq k-n\leq b]\cdot\left(\frac{b-(k-n)}{b+a}\cdot h\,[k/n-a]+\frac{(k-n)+a}{b+a}\cdot h\,[k/n+b]\right),$$

我们可以得出 l_M 的次不变性，即 $l_M \leq \Phi^M_g(l_M)$(详见 附录 D.5)。至此，我们完成了对下界的验证 l_{∞}。
◁

示例 27（渐近公平随机游走 [McIver 等人 2018]）。考虑以下循环 C_{flrw}，它刻画了 $\mathbb{Z}$ 上的偏置随机游走，其中下一步移动的概率尤其取决于行走者的当前位置：[15]

$$C_{\text{flrw}}:\quad \texttt{while}\,(n>0)\,\{\,n \coloneqq n-1\ [^{n+1}/_{2n+1}]\ n \coloneqq n+1\,\}\ .$$

行走者越向右移动，随机游走就越公平，因为 $^{n+1}/_{2\cdot n+1}$渐近趋近于 $1/2$。我们将展示如何使用守卫强化规则，通过证明 1 是 $\text{wp}[\![C_{\text{flrw}}]\!](1)$ 的下界，来验证 C_{flrw} 几乎必然终止。类似地，对于任意固定的 $M\in\mathbb{Z}_{>0}$，我们将守卫条件 $(n>0)$ 强化为 $\varphi^M=(0<n<M)$，并将由此得到的循环记为 C^M_{flrw}。由于 C^M_{flrw} 连续向左移动至多 $M-1$ 步后便会终止，且该事件的概率至少为 $(1/2)^{M-1}$，根据引理 15，C^M_{flrw} 几乎必然终止。令

$$l_M \;=\; [n<0]+[0\leq n\leq M]\cdot(1-{}^{n}/_{M})\ .$$

l_M 上界为 1，因此对于 C^M_{flrw} 根据条件 (c) 在 定理 9中。此外，l_M 是一个次不变式，因为

$$\begin{aligned}\Phi_g(l_M) &= [n\leq 0\vee n\geq M]\cdot[n\leq 0]+[0<n<M]\cdot\left(\frac{n+1}{2n+1}\cdot l_M\,[n/n-1]+\frac{n}{2n+1}\cdot l_M\,[n/n+1]\right)\\ &= [n\leq 0\vee n\geq M]\cdot[n\leq 0]+[0<n<M]\cdot\left(\frac{n+1}{2n+1}\cdot\frac{M-n+1}{M}+\frac{n}{2n+1}\cdot\frac{M-n-1}{M}\right)\\ &= [n\leq 0]+[0<n<M]\cdot\left(1-\frac{n}{M}+\frac{1}{(2n+1)\cdot M}\right)\ \geq\ l_M\,,\end{aligned}$$

其中，$g=[n\leq 0]\cdot 1$ 是受限后期望，而 Φ^M_g是 C^M_{flrw}关于 g的特征函数。这意味着 $l_M\leq \text{wp}[\![C_{\text{flrw}}]\!](1)$，即对于任意固定的 $M\in\mathbb{Z}_{>0}$，l_M 是 C_{flrw} 的终止概率下界。特别地，当 M 趋于无穷时，我们有

$$\text{wp}[\![C_{\text{flrw}}]\!](1)\ \geq\ \lim_{M\to\infty} l_M\ =\ 1\,.$$

因此我们可以得出结论：C_{flrw} 几乎必然终止。 ◁

示例 28（Zeroconf 协议 [Bohnenkamp 等人 2003]）。考虑以下循环 C_{zc}，它对随机化 IPv4 零配置协议进行编码（以 N为参数），用于自配置 IP 网络接口：

$$\begin{aligned}C_{\text{zc}}:\quad & \mathit{start}=1\,;\,\mathit{established}=0\,;\,\mathit{probe}=0\,;\\ & \texttt{while}\,(\mathit{start}\leq 1\wedge\mathit{established}\leq 0\wedge\mathit{probe}<N\wedge N\geq 4)\,\{\\ & \quad\texttt{if}\,(\mathit{start}=1)\,\{\\ & \quad\quad\{\,\mathit{start}\coloneqq 0\,\}\ [0.5]\ \{\,\mathit{start}\coloneqq 0\,;\,\mathit{established}\coloneqq 1\,\}\,\}\\ & \quad\texttt{else}\,\{\,\{\,\mathit{probe}\coloneqq\mathit{probe}+1\,\}\ [0.001]\ \{\,\mathit{start}\coloneqq 1\,;\,\mathit{probe}\coloneqq 0\,\}\,\}\,\}\,.\end{aligned}$$

[15]如果将偏置概率 $^{n+1}/_{2n+1}$ 替换为 $^{n}/_{2n+1}$，循环仍然几乎必然终止。然而，在这种情况下，需要使用更高级的次不变式来证明循环几乎必然终止。例如，参见 [McIver 等人 2018]中使用调和数的证明。

该程序旨在提供一种便捷的方法，用于分析将一个未使用的 IP 地址成功分配给新接入由 m 个现有设备组成的网络的主机的概率：接入后，主机首先从包含 n个可用地址的地址池中随机选择一个 IP 地址。该地址已被占用的概率为 m/n（取值为 0.5）；所选地址未被占用的概率为 $1 - m/n$，因此可以建立 IP 连接（以程序终止并返回 established $= 1$ 表示）。对于前一种情况，主机会向网络中的其他设备广播一条“探测”消息，询问所选 IP 地址是否已被占用；如果某个已使用该地址的设备收到探测消息，就会回复一条消息说明这一情况。收到该消息后，待配置的主机便会重新开始。[16] else 语句中的 0.001 表示消息丢失（探测消息或回复消息）的概率。为提高可靠性，要求主机发送多条探测消息（上限为 N）。事实上，C_{zc} 通过将 N设为参数，编码了一个无限的马尔可夫链族（参见 [Baier 和 Katoen，2008，例 10.5]），因此无法通过概率模型检测进行处理。

我们希望验证一个非平凡的下界 0.99999999999 关于概率 $\mathcal{P}$：从满足循环守卫条件的状态开始，C_{zc} 最终终止于一个 已建立 $= 1$ 的状态。为此，我们尝试使用近期开发的工具 *cegispro2* [Batz 等人 2023] 将 Hark 等人的可靠下界归纳规则自动化[Hark 等人 2020]。遗憾的是，cegispro2 在此案例中失败了（运行 20 分钟后超时）。不过，通过用 N 的上界强化循环守卫条件，例如 $N \leq 10$，并应用我们的证明规则，cegispro2 找到了一个分段线性次不变式（不到一秒；因篇幅有限而省略），足以证明 0.99999999999 是 $\mathcal{P}$ 的下界。总的来说，这表明我们的证明规则有望借助自动化技术，为实用的随机化算法验证下界，而这类算法原本难以企及。◁

我们的证明规则还适用于定量验证基准集中的另外几个案例研究 [Hartmanns 等人 2019]，包括有界重传协议（这一无限族协议）、Rabin 互斥算法（参数化版本）以及优惠券收集问题。这些案例研究未被纳入，是因为它们要么无法为 Zeroconf 协议提供额外见解，要么已有现成技术可以解决。要研究范围更广的真实随机化算法，主要挑战是：（i）找到合适的守卫强化（参见第 8 节下文）；在某些情况下，（ii）找到能够证明给定下界的次不变式。我们计划通过挖掘自动化 证明规则的潜力来应对这些挑战，详见第 6.4 节。

8 守卫强化规则的局限性

有一些有趣的发散程序，所提出的守卫强化原理对它们并不充分或不适用。我们通过两个例子来说明这些局限性。

以下示例展示了这样一种情况：朴素的强化启发式不足以完成证明，但更高级的强化策略足以确立非平凡下界。

例29（二维离散螺旋）。考虑以下概率程序

$$
\begin{aligned}
&x \coloneqq 0 \,;\, y \coloneqq 0 \,;\, \mathit{flag} \coloneqq 0 \,;\\
&\texttt{while}\left((x-1)^2 + (y-1)^2 < 4\right)\{\\
&\quad \{\, x \coloneqq -1 \,;\, y \coloneqq -1 \,\}\ [\,|x-1|/4\,]\ \{\\
&\qquad \texttt{if}\ (\mathit{flag})\ \{\, y \coloneqq (3-y)/2 \,\}\ \texttt{else}\ \{\, x \coloneqq (3-x)/2 \,\} \,;\, \mathit{flag} \coloneqq 1 - \mathit{flag} \,\}\,\}\,.
\end{aligned}
$$

[16]该程序 C_{zc} 是实际协议的抽象模型，因为 C_{zc} 抽象掉了在执行 if 语句的右分支时广播探测消息的必要性（在这种情况下，反正也不会发送回复消息）。这种抽象不会影响对以 已确立 $= 1$ 终止的概率进行分析。

该程序只有在访问概率选择的左分支时才会终止；否则，它会发散，且 $(x,\ y)$ 会沿着二维离散螺旋的轨迹趋近于 $(1,\ 1)$。注意，该程序是非几乎必然终止的，我们旨在验证其终止概率的下界。可以看到，在这种情况下，朴素的强化启发式方法 $\varphi' = \varphi \wedge x < c \wedge y < c$（通过为程序变量 c添加常数界）不足以 适用于任何 $c > 3/2$，因为得到的程序仍然是非几乎必然终止的；而对于任何 $c \leq 3/2$,，得到的程序至多经过一次循环迭代便会终止，因此只能得到平凡的 下界。相比之下，采用更高级（但直观）的强化方法$\varphi' = \varphi \wedge (x-1)^2 + (y-1)^2 > \epsilon$并设置一个较小的常数 $\epsilon > 0$（即排除螺旋中心 $(1,\ 1)$），可以将程序化简为有限状态空间的情况，随后便可通过概率模型检测来建立非平凡的 下界。◁

正如第 6.4 节所述，探讨比本文所用启发式方法更先进且（半）自动化的守卫强化策略，是一个值得研究的未来方向。

以　下例展示了一个不存在有用强化的边界情况。

例 30（虚拟交换器）。考虑以下概率程序

$$\texttt{while}\,(x \neq y)\,\{\,x \coloneqq y \;\oplus\; \{temp \coloneqq x \fatsemi x \coloneqq y \fatsemi y \coloneqq temp\} \;\oplus\; \texttt{diverge}\,\}$$

其中，迭代的 $\oplus$ 是离散均匀选择的简写（在此例中，每种选择的概率均为 $1/3$）；diverge 是 while(true){skip} 的语法糖。该程序是非几乎必然终止的，只有通过均匀选择中最左侧的分支才会终止；否则，它会因持续交换 x 和 y 的值（即在两点间往返）而发散，或者因选择最右侧的分支而立即发散。可以证明，任何 能使该程序几乎必然终止的强化都必然导致 $\varphi' = \text{false}$——否则，至少会执行一次循环迭代，且程序以至少 $1/3$ 的概率发散——因此只能得出平凡的下界。◁

9 相关工作

最弱前期望推理。作为 Dijkstra 的谓词变换器演算的概率类比， [Dijkstra 1975, 1976], 期望变换器已被广泛用于推理概率程序的定量性质。wp 风格推理可追溯至 Kozen [1983, 1985] 关于概率命题动态逻辑的开创性工作。Jones [1990],Morgan 等人 [1996], McIver 和 Morgan [2005], 以及 Hehner [2011] 等人进一步推进了这一研究方向，例如探讨非确定性，以及在存在循环时界定前期望的证明规则。经典的最弱前期望演算在多个方向上得到了显著拓展，以推理诸如（递归）概率程序的期望运行时间 [Kaminski 等人 2016、2018；Olmedo 等人 2016], 带条件化的概率程序 [Olmedo 等人 2018；Szymczak 和 Katoen 2019], 混合符号后期望 [Kaminski 和 Katoen 2017], 概率程序的敏感性 [Aguirre 等人 2021], 概率时序逻辑 [Morgan 和 McIver1999], 以及定量分离逻辑 [Batz 等人 2019]。Batz 等人 [2021b] 最近为最弱前期望推理建立了一个相对完备性结果。

最弱前期望与不动点的下界。 针对由（最小）不动点刻画的循环语义，已有大量研究结果用于确立其上界和／或下界。这些研究包括基于 计量函数 [Frohn 等人 2020, 2016]，用于对非概率程序的运行时间进行下近似；基于 约束求解 [Chen 等人 2015；Feng 等人 2017；Katoen 等人 2010]；以及基于 不变式学习 [Bao 等人 2022]，用于生成概率程序最弱前期望的下界；基于 递推求解 [Bartocci 等人 2019]，用于合成所谓概率可解循环的基于矩的不变式；以及 有界模型检测 [Jansen 等人 2016]，用于验证带有非确定性的概率程序，以及

条件化，以及各种形式的 值迭代 [Baier 等人 2017； Hartmanns 和 Kaminski，2020; Quatmann 和 Katoen 2018]，用于确定马尔可夫模型中的可达概率。

除了本文详细阐述的证明规则外，Baldan 等人 [2021] 最近还提出了格论证明规则，用于验证有限状态随机系统最小不动点的下界。Batz 等人 [2021a] 发明了格点 k-归纳法，以确定可能具有无限状态的概率程序的最小不动点上界。与我们的守卫强化规则密切相关的概念是 ω-次不变式 [Audebaud and Paulin-Mohring 2009; Jones 1990; Kaminski et al. 2016, 2018]，，它是一个单调递增的期望序列 $\{I_n\}_{n\in\mathbb{N}}$，其中各项彼此互为次不变式，即 $I_0 = 0$ 和 $I_{n+1} \preceq \Phi(I_n)$。已知 $\sup_{n\in\mathbb{N}} I_n$ 足以作为 Φ最小不动点的下界；然而，寻找这样的下界需要 (i) 通过检查不动点迭代中的“模式”，推导出 I_n 在 n 中的闭式；以及 (ii) 求出该闭式的上确界。与直接推断序列 $\sup_{n\in\mathbb{N}} \Phi^n(0)$ 的上确界（极限）以得到精确的最小不动点相比，这两个步骤几乎省不了多少功夫。在一些示例中，我们还会讨论 l_M 相对于 M（用于强化守卫条件的常数）的极限，以获得紧确的下界。不过，这一步并非必要，因为对于任意固定的 M，$l_M \preceq \Phi(l_M)$已经足以作为下界；也就是说，我们只需将 l_M “通过循环语义推送”一次。此外，对于具有复杂闭式解的离散状态程序，例如例 24 中的三维随机游走，我们的规则能够推导出紧确的下界（通过概率模型检测），而无需取极限。

分析随机游走中的空间限制。我们的守卫强化技术与分析无限离散格上随机游走时采用的空间限制策略之间存在着思想上的联系：按照Feller [1950, 第十四章]和McCrea 和 Whipple [1940] 的方法，通过设置“屏障”来限制无限空间中的随机游走，然后取极限，这与我们的方法类似。尽管如此，他们在施加限制后，都会通过求解递推方程（又称差分方程）来获得受限随机游走的闭式解，以便取极限。虽然类似的方法也可以融入我们的方法——因为求解递推方程是求得次不变式的一种（代价高昂的）方式——但这并非必要：我们的证明规则将问题转化为概率模型检测问题。因此，该规则能够处理现有验证技术无法企及的例子，例如三维随机游走，而无需求解递推方程或取极限。此外，我们的证明规则将概率论中的特设证明方法编码为程序逻辑中的一条句法规则，并使现有证明规则能够用于原本超出适用范围的验证问题。

基于鞅的推理。Chakarov 和 Sankaranarayanan 开创了通过鞅进行概率程序分析的方法，用于求得期望运行时间的上界并合成期望不变式。Chatterjee 等人进一步扩展了基于鞅的方法，以处理非确定性。Barthe 等人专注于合成精确的鞅表达式。Fioriti 和 Hermanns 开发了一种用于一致可积性的类型系统，以证明概率程序几乎必然终止，并给出期望运行时间的上界。与此相反，Fu 和 Chatterjee 给出了期望运行时间的下界；Chatterjee 等人证明了终止概率的下界。Kobayashi 等人提供了一种半判定过程，用于求得概率高阶递归程序终止概率的上界。Chatterjee 等人；Wang 等人专注于求得断言违反概率的上界和下界。Ngo 等人进行自动化的模板驱动资源分析，但只推断上界。Wang 等人给出了求得期望成本上界和下界的充分条件。Wang 等人提出了推导期望累积成本高阶矩上界和下界的条件。与我们的证明规则不同，这些基于鞅、用于推断下界的方法大多只适用于几乎必然终止的概率程序。

概率双模拟与等价。我们关于 wp 差的结果属于量化两个程序之间“距离”的一般研究范畴。这引出了概率双模拟（Hong 等人，2019；Larsen 和 Skou）以及概率等价的概念（参见有限数据类型方面的 Murawski 和 Ouaknine，以及直线程序方面的 Barthe 等人）。Chen 等人最近证明了一项可判定性结果：在假设程序几乎必然终止的前提下，可以判定一个无限状态离散循环概率程序是否等价于一个无循环规约程序。Barthe 等人为概率程序开发了关系霍尔逻辑，该逻辑已被广泛用于证明程序等价，并应用于可证明安全性和侧信道分析。我们的证明规则专门用于推理可能发散的概率程序的期望值下界；尽管如此，仍值得探索将其推广到证明可能具有无限状态且非几乎必然终止的概率程序之间的等价、双模拟及 ε-接近关系，例如将我们的证明规则嵌入概率关系霍尔逻辑。

10 结论

我们提出了一条新的证明规则——基于 wp 差和守卫强化技术——用于验证概率程序最弱前期望的下界。这是首条允许期望可能无界的发散概率循环的下界规则。具体而言，我们使现有的下界归纳规则能够普遍适用于可能发散的程序：这些程序经过强化后，其对应程序具有易于证明的几乎必然终止性和一致可积性。此外，我们证明了守卫强化技术引入的误差可以任意小，从而得到紧下界；若修改后的循环具有有限状态空间，则可以通过概率模型检测自动化应用我们的证明规则，生成下界。我们通过若干示例展示了该证明规则的有效性。具体而言，我们成功推导出了格点上著名的三维随机游走的紧终止概率下界；此前，验证领域尚未对此问题进行研究。

未来的研究方向包括：(i) 将我们的证明规则扩展到期望运行时间演算，以求得期望运行时间的下界 [Kaminski 等人 2016, 2018]，用于带有天使式/恶魔式非确定性的概率程序 [McIver 和 Morgan 2001, 2005]，和/或带有软/硬条件的程序 [Olmedo 等人，2018；Szymczak 和 Katoen 2019]；(ii) 探索我们的最弱前置条件差异结果在敏感性分析 [Aguirre 等人，2021；Barthe 等人，2018；Wang 等人 2020] 和概率程序模型修复 [Bartocci 等人 2011] 中的适用性；以及 (iii) 研究用于我们证明规则的（候选）定量（次）不变式的（半）自动化综合。

致谢

本研究部分获得中国国家重点研发计划（项目编号：2022YFA1005101）、国家自然科学基金委员会（项目编号：62192732 和 62032024）、中国科学院青年科学家基础研究项目（项目编号：YSBR-040）、浙江大学教育基金会求是人才计划、欧洲研究委员会高级项目 FRAPPANT（项目编号：787914），以及欧盟地平线2020研究与创新计划玛丽·斯克沃多夫斯卡-居里资助协议（编号：101008233）的资助。作者感谢 Kevin Batz、Tim Quatmann 及匿名审稿人，就与 ω最弱前期望推理中的不变式、马尔可夫模型中的部分探索，以及分析随机游走时的空间限制策略的相关联系进行了富有见地的讨论。

参考文献

Erika Ábrahám、Bernd Becker、Christian Dehnert、Nils Jansen、Joost-Pieter Katoen 和 Ralf Wimmer。2014。离散时间马尔可夫模型的反例生成：入门综述。载于*SFM*（*LNCS*，第 *8483* 卷）。施普林格，65–121。

Alejandro Aguirre、Gilles Barthe、Justin Hsu、Benjamin Lucien Kaminski、Joost-Pieter Katoen 和 Christoph Matheja。2021。概率敏感性的前期望演算。ACM程序设计语言会议录 5，POPL（2021），1–28。James Aspnes 和 Maurice Herlihy。1990。使用共享内存的快速随机化共识。《算法》杂志 11，3（1990），441–461。Philippe Audebaud 和 Christine Paulin-Mohring。2009。Coq 中随机化算法的证明。《科学计算程序》74，8（2009），568–589。Christel Baier 和 Joost-Pieter Katoen。2008。模型检测原理。麻省理工学院出版社。Christel Baier、Joachim Klein、Linda Leuschner、David Parker 和 Sascha Wunderlich。2017。确保模型检查器的可靠性：马尔可夫决策过程的区间迭代。载于 CAV (II)（LNCS，第 10426 卷）。施普林格，160–180。Paolo Baldan、Richard Eggert、Barbara König 和 Tommaso Padoan。2021。不动点理论——颠倒过来。载于 FoSSaCS（LNCS，第 12650 卷）。施普林格，62–81。Jialu Bao、Nitesh Trivedi、Drashti Pathak、Justin Hsu 和 Subhajit Roy。2022。概率程序的数据驱动不变式学习。载于 CAV (I)（LNCS，第 13371 卷）。施普林格，33–54。Gilles Barthe、Thomas Espitau、Luis María Ferrer Fioriti 和 Justin Hsu。2016。通过杜布分解综合概率不变式。载于 CAV (I)（LNCS，第 9779 卷）。施普林格，43–61。Gilles Barthe、Thomas Espitau、Benjamin Grégoire、Justin Hsu 和 Pierre-Yves Strub。2018。证明概率程序的期望敏感性。ACM程序设计语言会议录 2，POPL（2018），57:1–57:29。Gilles Barthe、Benjamin Grégoire 和 Santiago Zanella Béguelin。2009。基于代码的密码学证明的形式化认证。载于 POPL。美国计算机协会，90–101。Gilles Barthe、Benjamin Grégoire 和 Santiago Zanella Béguelin。2012。用于计算机辅助安全证明的概率关系霍尔逻辑。载于 MPC（LNCS，第 7342 卷）。施普林格，1–6。Gilles Barthe、Joost-Pieter Katoen 和 Alexandra Silva（编）。2020。概率编程基础。剑桥大学出版社。Gilles Barthe、Boris Köpf、Federico Olmedo 和 Santiago Zanella Béguelin。2013。差分隐私的概率关系推理。《ACM程序设计语言与系统汇刊》35，3（2013），9:1–9:49。Ezio Bartocci、Radu Grosu、Panagiotis Katsaros、C. R. Ramakrishnan 和 Scott A. Smolka。2011。概率系统的模型修复。载于 TACAS（LNCS，第 6605 卷）。施普林格，326–340。Ezio Bartocci、Laura Kovács 和 Miroslav Stankovic。2019。自动生成概率可解循环的基于矩的不变式。载于 ATVA（LNCS，第 11781 卷）。施普林格，255–276。Kevin Batz、Mingshuai Chen、Sebastian Junges、Benjamin Lucien Kaminski、Joost-Pieter Katoen 和 Christoph Matheja。2023。通过归纳综合归纳不变式验证概率程序。载于 TACAS。即将出版。Kevin Batz、Mingshuai Chen、Benjamin Lucien Kaminski、Joost-Pieter Katoen、Christoph Matheja 和 Philipp Schröer。2021a。格点上的 k-归纳及其在概率程序中的应用。载于 CAV (I)（LNCS，第 12760 卷）。施普林格，524–549。Kevin Batz、Benjamin Lucien Kaminski、Joost-Pieter Katoen 和 Christoph Matheja。2021b。概率程序的相对完备验证：一种用于基于期望推理的表达性语言。ACM程序设计语言会议录 5，POPL（2021），1–30。Kevin Batz、Benjamin Lucien Kaminski、Joost-Pieter Katoen、Christoph Matheja 和 Thomas Noll。2019。定量分离逻辑：一种用于推理概率指针程序的逻辑。ACM程序设计语言会议录 3，POPL（2019），34:1–34:29。Daniel Bernoulli。1954。关于风险度量新理论的阐述。《计量经济学》22，1（1954），23–36。Henrik C. Bohnenkamp、Peter van der Stok、Holger Hermanns 和 Frits W. Vaandrager。2003。IPv4 零配置协议的成本优化。载于 DSN。IEEE计算机学会，531–540。Tomás Brázdil、Krishnendu Chatterjee、Martin Chmelik、Vojtech Forejt、Jan Kretínský、Marta Z. Kwiatkowska、David Parker 和 Mateusz Ujma。2014。使用学习算法验证马尔可夫决策过程。载于 ATVA（LNCS，第 8837 卷）。施普林格，98–114。Michael Carbin、Sasa Misailovic 和 Martin C. Rinard。2016。验证在不可靠硬件上执行的程序的定量可靠性。ACM 通讯 59，8（2016），83–91。Aleksandar Chakarov 和 Sriram Sankaranarayanan。2013。利用鞅进行概率程序分析。载于 CAV（LNCS，第 8044 卷）。施普林格，511–526。Aleksandar Chakarov 和 Sriram Sankaranarayanan。2014。作为不动点的概率程序循环期望不变式。载于 SAS（LNCS，第 8723 卷）。施普林格，85–100。Krishnendu Chatterjee、Hongfei Fu 和 Amir Kafshdar Goharshady。2016a。通过正定性定理分析概率程序的终止性。载于 CAV (I)（LNCS，第 9779 卷）。施普林格，3–22。Krishnendu Chatterjee、Hongfei Fu 和 Petr Novotný。2020。使用鞅分析概率程序的终止性，221–258。载于 Barthe 等人 [Barthe 等人 2020]。Krishnendu Chatterjee、Hongfei Fu、Petr Novotný 和 Rouzbeh Hasheminezhad。2016b。仿射概率程序定性与定量终止问题的算法分析。载于 POPL。美国计算机协会，327–342。

Krishnendu Chatterjee、Amir Kafshdar Goharshady、Tobias Meggendorfer 和 Djordje Zikelic。2022。《概率程序定量终止分析的可靠且完备证书》。载于 CAV (I)（LNCS，第 13371 卷）。施普林格，55–78。Krishnendu Chatterjee、Petr Novotný 和 Dorde Zikelic。2017。《概率终止的随机不变量》。载于 POPL。ACM，145–160。Mingshuai Chen、Joost-Pieter Katoen、Lutz Klinkenberg 和 Tobias Winkler。2022。《程序能否产生正确的分布？通过生成函数验证概率程序》。载于 CAV (I)（LNCS，第 13371 卷）。施普林格，79–101。Yu-Fang Chen、Chih-Duo Hong、Bow-Yaw Wang 和 Lijun Zhang。2015。《通过拉格朗日插值进行反例引导的多项式循环不变量生成》。载于 CAV (I)（LNCS，第 9206 卷）。施普林格，658–674。Fredrik Dahlqvist、Alexandra Silva 和 Dexter Kozen。2020。《概率编程语义：温和导论》，1–42。载于 Barthe 等人 [Barthe 等人 2020]。Christian Dehnert、Sebastian Junges、Joost-Pieter Katoen 和 Matthias Volk。2017。《风暴将至：现代概率模型检查器》。载于 CAV (II)（LNCS，第 10427 卷）。施普林格，592–600。Edsger Wybe Dijkstra。1975 18, 8 1975 453 457 。《守卫命令、非确定性与程序的形式化推导》。《ACM 通讯》（ ），– 。Edsger Wybe Dijkstra。1976。《程序设计的学科》。Prentice-Hall。Owain Evans、Andreas Stuhlmüller、John Salvatier 和 Daniel Filan。2017。《用概率程序对智能体建模》。http://agentmodels.org。访问日期：2022-7-7。Willliam Feller。1950年。《概率论及其应用导论》。第 I 卷。John Wiley & Sons。Yijun Feng、Lijun Zhang、David N. Jansen、Naijun Zhan 和 Bican Xia。2017。《寻找概率程序的多项式循环不变量》。载于 ATVA（LNCS，第 10482 卷）。施普林格，400–416。Luis María Ferrer Fioriti 和 Holger Hermanns。2015。《概率终止：可靠性、完备性与组合性》。载于 POPL。ACM，489–501。Florian Frohn、Matthias Naaf、Marc Brockschmidt 和 Jürgen Giesl。2020。《推断整数程序的运行时间下界》。《ACM程序设计语言与系统汇刊》42，3（2020），13:1–13:50。Florian Frohn、Matthias Naaf、Jera Hensel、Marc Brockschmidt 和 Jürgen Giesl。2016。《整数程序的运行时间下界》。载于 IJCAR（LNCS，第 9706 卷）。施普林格，550–567。Hongfei Fu 和 Krishnendu Chatterjee。2019。《非确定性概率程序的终止》。载于 VMCAI（LNCS，第 11388 卷）。施普林格，468–490。Jürgen Giesl、Peter Giesl 和 Marcel Hark。2019。《计算常概率程序的期望运行时间》。载于 CADE（LNCS，第 11716 卷）。施普林格，269–286。Andrew D. Gordon、Thomas A. Henzinger、Aditya V. Nori 和 Sriram K. Rajamani。2014。《概率编程》。载于 FOSE。ACM，167–181。Marcel Hark、Benjamin Lucien Kaminski、Jürgen Giesl 和 Joost-Pieter Katoen。2019。《目标较低反而更难——概率程序验证中最弱前期望下界的归纳证明规则》。CoRR abs/1904.01117（2019）。arXiv:1904.01117。Marcel Hark、Benjamin Lucien Kaminski、Jürgen Giesl 和 Joost-Pieter Katoen。2020。《目标较低反而更难：概率程序验证中的下界归纳法》。ACM程序设计语言会议录 4，POPL（2020），37:1–37:28。Arnd Hartmanns 和 Benjamin Lucien Kaminski。2020。《乐观值迭代》。载于 CAV (II)（LNCS，第 12225 卷）。施普林格，488–511。Arnd Hartmanns、Michaela Klauck、David Parker、Tim Quatmann 和 Enno Ruijters。2019。《定量验证基准集》。载于 TACAS (I)（LNCS，第 11427 卷）。施普林格，344–350。Eric Charles Roy Hehner。2011。《概率视角》。《计算机的形式化方面》23，4（2011），391–419。Michael Hicks。2014。《什么是概率编程？》载于：《编程语言爱好者》。http://www.pl- enthusiast.net/2014/09/08。访问日期：2021-12-09。Chih-Duo Hong、Anthony W. Lin、Rupak Majumdar 和 Philipp Rümmer。2019。《参数化系统的概率双模拟——（及其在验证匿名协议中的应用）》。载于 CAV (I)（LNCS，第 11561 卷）。施普林格，455–474。Jacek Jachymski、Leslaw Gajek 和 Piotr Pokarowski。2000。《Tarski-Kantorovitch原理与迭代函数系统理论》。《澳大利亚数学会通报》61，2（2000），247–261。Nils Jansen、Christian Dehnert、Benjamin Lucien Kaminski、Joost-Pieter Katoen 和 Lukas Westhofen。2016。《概率程序的有界模型检测》。载于 ATVA（LNCS，第 9938 卷）。68–85。Claire Jones。1990。《概率非确定性》。博士论文。爱丁堡大学，英国。Benjamin Lucien Kaminski。2019。《概率程序的高级最弱前条件演算》。博士论文。亚琛工业大学，德国。Benjamin Lucien Kaminski 和 Joost-Pieter Katoen。2017。《混合符号期望的最弱前期望语义》。载于 LICS。IEEE计算机学会，1–12。

Benjamin Lucien Kaminski、Joost-Pieter Katoen 和 Christoph Matheja。2019。《概率程序分析的难度》。《Acta Informatica》56，3（2019），255–285。Benjamin Lucien Kaminski、Joost-Pieter Katoen、Christoph Matheja 和 Federico Olmedo。2016。《概率程序期望运行时间的最弱前置条件推理》。载于 ESOP（LNCS，第 9632 卷）。施普林格，364–389。Benjamin Lucien Kaminski、Joost-Pieter Katoen、Christoph Matheja 和 Federico Olmedo。2018。《随机化算法期望运行时间的最弱前置条件推理》。《ACM学报》65，5（2018），30:1–30:68。Joost-Pieter Katoen。2016。《概率模型检测概览》。载于 LICS。ACM，31–45。Joost-Pieter Katoen、Friedrich Gretz、Nils Jansen、Benjamin Lucien Kaminski 和 Federico Olmedo。2015。《理解概率程序》。载于《正确的系统设计》（LNCS，第 9360 卷）。施普林格，15–32。Joost-Pieter Katoen、Annabelle McIver、Larissa Meinicke 和 Carroll C. Morgan。2010。《概率程序的线性不变量生成：基于证明的方法的自动化支持》。载于 SAS（LNCS，第 6337 卷）。施普林格，390–406。Bronisław Knaster。1928。《集合函数上的一个定理》。《波兰数学会年刊》6（1928），133–134。Naoki Kobayashi、Ugo Dal Lago 和 Charles Grellois。2020。《概率高阶递归程序的终止问题》。《逻辑方法与计算机科学》16，4（2020）。Dexter Kozen。1981。《概率程序的语义》。《计算机与系统科学杂志》22，3（1981），328–350。Dexter Kozen。1983。《概率PDL》。载于 STOC。ACM，291–297。Dexter Kozen。1985。《概率PDL》。《计算机与系统科学杂志》30，2（1985），162–178。Marta Kwiatkowska、Gethin Norman 和 David Parker。2002。《PRISM：概率符号模型检查器》。载于 TOOLS。施普林格，200–204。Marta Z. Kwiatkowska。2003。《概率与时间的模型检测：从理论到实践》。载于 LICS。IEEE计算机学会，351。Kim Guldstrand Larsen 和 Arne Skou。1991。《通过概率测试实现双模拟》。《信息与计算》94，1（1991），1–28。Jean-Louis Lassez、V. L. Nguyen 和 E. A. Sonenberg。1982。《不动点定理与语义：一个民间故事》。《信息处理快报》14，3（1982），112–116。William H. McCrea 和 Francis J. W. Whipple。1940。《XXII——二维和三维中的随机路径》。《爱丁堡皇家学会会刊》60，3（1940），281–298。Annabelle McIver 和 Carroll Morgan。2001。《概率恶魔程序的部分正确性》。《理论计算机科学》266，1-2（2001），513–541。Annabelle McIver 和 Carroll Morgan。2005。《概率系统的抽象、精化与证明》。施普林格。Annabelle McIver、Carroll Morgan、Benjamin Lucien Kaminski 和 Joost-Pieter Katoen。2018。《几乎必然终止的新证明规则》。ACM程序设计语言会议录 2，POPL（2018），33:1–33:28。Elliot W Montroll。1956。《多维空间中的随机游走，特别是周期晶格上的随机游走》。《工业与应用数学学会杂志》4，4（1956），241–260。Marcel Moosbrugger、Ezio Bartocci、Joost-Pieter Katoen 和 Laura Kovács。2021。《概率终止工具 Amber》。载于 FM（LNCS，第 13047 卷）。施普林格，667–675。Carroll Morgan 和 Annabelle McIver。1999。《概率时序逻辑的期望变换器模型》。《 IGPL 逻辑杂志》 7，6 （ 1999 ），779–804。Carroll Morgan、Annabelle McIver 和 Karen Seidel。1996。《概率谓词变换器》。《ACM程序设计语言与系统汇刊》18，3（1996），325–353。Andrzej S. Murawski 和 Joël Ouaknine。2005。《概率程序等价与精化》。《CONCUR》（LNCS，第 3653 卷）。施普林格，156–170。Van Chan Ngo、Quentin Carbonneaux 和 Jan Hoffmann。2018。《有界期望：概率程序的资源分析》。载于 PLDI。ACM，496–512。Federico Olmedo、Friedrich Gretz、Nils Jansen、Benjamin Lucien Kaminski、Joost-Pieter Katoen 和 Annabelle McIver。2018。《概率编程中的条件化》。《ACM程序设计语言与系统汇刊》40，1（2018），4:1–4:50。Federico Olmedo、Benjamin Lucien Kaminski、Joost-Pieter Katoen 和 Christoph Matheja。2016。《递归概率程序推理》。载于 LICS。ACM，672–681。David Park。1969。《不动点归纳与程序性质证明》。《机器智能》5（1969）。G. Pólya。1921。《关于概率计算中与道路网络随机游走有关的问题》。《数学年刊》84（1921），149–160。Tim Quatmann 和 Joost-Pieter Katoen。2018。《可靠值迭代》。载于 CAV (I)（LNCS，第 10981 卷）。施普林格，643–661。Nasser Saheb-Djahromi。1978。《概率LCF》。载于 MFCS（LNCS，第 64 卷）。施普林格，442–451。Sriram Sankaranarayanan。2020。《结合概率与测度集中不等式的程序定量分析》，259–294。载于 Barthe 等人 [Barthe 等人 2020]。Marco Schneider。1993。《自稳定》。《ACM计算调查》25，1（1993），45–67。

Seyed Mahdi Shamsi、Gian Pietro Farina、Marco Gaboardi 和 Nils Napp。2020。《用于自主系统建模的概率编程语言》。载于 *MFI*。IEEE，32–39。Marcin Szymczak 和 Joost-Pieter Katoen。2019。《用于贝叶斯推断的最弱前期望语义——条件化、连续分布与发散》。载于 *SETSS (LNCS, Vol. 12154)*。施普林格，44–121。阿尔弗雷德·塔斯基。1955。《格论不动点定理及其应用》。《太平洋数学杂志》5, 2 (1955), 285–309。Jan-Willem van de Meent、Brooks Paige、Hongseok Yang 和 Frank Wood。2018。《概率编程导论》。*CoRR* abs/1809.10756 (2018)。Di Wang、Jan Hoffmann 和 Thomas W. Reps。2021a。《概率程序中成本累加器的中心矩分析》。载于 *PLDI*。美国计算机协会，559–573。Jinyi Wang、Yican Sun、Hongfei Fu、Krishnendu Chatterjee 和 Amir Kafshdar Goharshady。2021b。《概率程序中断言违反的定量分析》。载于 *PLDI*。美国计算机协会，1171–1186。Peixin Wang、Hongfei Fu、Krishnendu Chatterjee、Yuxin Deng 和 Ming Xu。2020。《证明具有随机变量相关终止时间的概率程序的期望敏感性》。*ACM*程序设计语言会议录 4, POPL (2020), 25:1–25:30。Peixin Wang、Hongfei Fu、Amir Kafshdar Goharshady、Krishnendu Chatterjee、Xudong Qin 和 Wenjun Shi。2019。《非确定性概率程序的成本分析》。载于 *PLDI*。美国计算机协会，204–220。David Williams。1991。《鞅与概率》。剑桥大学出版社。Mingsheng Ying。2011。《量子程序的 Floyd-Hoare 逻辑》。*ACM Trans.Program. Lang. Syst.* 33,6(2011),19:1–19:49。

附录
测度论基本概念

我们回顾测度论中的基本概念，这些概念构成了理解概率程序的基础。我们建议感兴趣的读者参阅 [Dahlqvist 等人，2020，第 1 节。2] 以获取面向概率编程的测度论更详细介绍。

可测空间与函数。集合 S 上的一个 σ-代数 B 是由 S 的子集组成的集合，它包含空集 $\emptyset$，并且对 S 中的补集运算和可数并运算封闭。给定同一集合 S 上的两个 σ-代数 B_1 和 B_2，当且仅当 $\mathrm{B}_1 \subseteq \mathrm{B}_2$ 时，B_1 是 B_2 的子-σ-代数。$\mathbb{R}$ 上的博雷尔 σ-代数——由 $\mathbb{R}$ 上的博雷尔集组成——是包含这些区间的 $\mathbb{R}$ 上最小的 σ-代数。若 S 是一个集合，且 B 是 S 上的 σ-代数，则称有序对（S, B）为可测空间。给定两个可测空间（S, B_S）和（T, B_T），若对每个属于 B_T 的可测子集 $B \in$，其原像 $f^{-1}(B) = \{x \in S \mid f(x) \in B\}$ 都是 S 的可测子集，则函数 $f\colon S \to T$ 是可测的。

（次）概率测度。在可测空间 (S, B) 上的符号（有限）测度是一个可数可加映射 $\mu\colon \mathrm{B} \to \mathbb{R}$，满足 $\mu(\emptyset) = 0$。注意，μ 可数可加意味着：若 A 是一个由两两不相交事件组成的可数集合，则 $\mu(\cup\mathrm{A}) = \sum_{A\in\mathrm{A}} \mu(A)$。若 (S, B) 上的符号测度满足对所有 $B \in \mathrm{B}$，$\mu(B) \geq 0$，则称其为正测度。若 (S, B) 上的正测度满足 $\mu(S) = 1$，则称为概率测度；若满足 $\mu(S) \leq 1$，则称为次概率测度。若可测集 B 满足 $\mu(B) = 0$，则称其为 μ-零测集；若上下文明确，也简称零测集。若性质在 S 上不成立的点集包含于某个零测集，则称该性质在 S 上（μ-）几乎必然成立。

概率空间与随机变量。概率空间 (Ω, F, P) 由样本空间 Ω、定义在 Ω 上的 σ-代数 F，以及可测空间 (Ω, F) 上的概率测度 $P\colon \mathrm{F} \to [0,1]$ 构成。定义在概率空间 (Ω, F, P) 上的随机变量 X 是一个 F- 可测函数 $X\colon \Omega \to \mathbb{R}$；其期望值（相对于 P）记作 $\mathbb{E}[X]$。每个随机变量 X 都会诱导一个定义在 $\mathbb{R}$ 上的（次）概率测度 $\mu_X\colon \mathrm{B} \to [0,1]$，其定义为：对于 $\mathbb{R}$ 上的博雷尔 σ-代数 B 中的博雷尔集 B，$\mu_X(B) \triangleq P(X^{-1}(B))$。$\mu_X$ 也称为 X 的分布。如果对于所有满足 $\{s\} \in \mathrm{B}$ 的单点集 $\{s\}$，$\mu(\{s\}) = 0$，则 μ_X 在可测空间 $(\mathbb{R}, \mathrm{B})$ 上是连续的；如果它是狄拉克测度 δ_s 的可数加权和，且 $s \in S$，并且当 $s \in B$ 时 $\delta_s(B) = 1$，否则为 0，则它是离散的。

随机过程与停时。给定一个概率空间（Ω, F, P），一个（离散时间）随机过程是由随机变量组成的参数化集合 $\{X_n\}_{n\in\mathbb{N}}$，这些随机变量定义在（Ω, F, P）上；当上下文清楚时，我们有时会省略 $\{X_n\}$ 中的括号。若由 F 的子σ代数构成的集合 $\{\mathrm{F}_n\}_{n\in\mathbb{N}}$ 满足对所有 $i \leq j$ 均有 $\mathrm{F}_i \subseteq \mathrm{F}_j$，则称其为滤过；直观地说，$\mathrm{F}_n$ 承载着观察者在步骤 n 时已知的信息。若随机变量 $\tau\colon \Omega \to \mathbb{N}$ 满足对所有 $n \in \mathbb{N}$ 均有 $\{\tau \leq n\} \in \mathrm{F}_n$，则称其为关于 F 的某个滤过 $\{\mathrm{F}_n\}_{n\in\mathbb{N}}$ 的停时。给定一个随机过程 X_n 和一个停时 τ，相应的停止过程 $\{X^\tau_n\}_{n\in\mathbb{N}}$ 定义为

$$X^\tau_n \triangleq \begin{cases} X_n & \text{if } n \leq \tau, \\ X_\tau & \text{if } n > \tau, \end{cases}$$

也就是说，进程在给定的（随机）时刻之后被迫保持同一数值 τ。

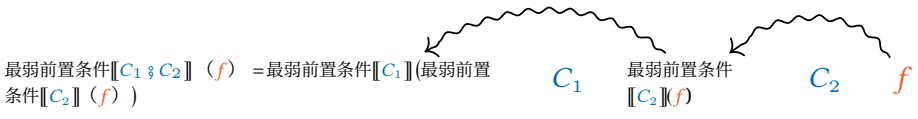

图 7. 我们反向延续传递风格中的最弱前期望变换器 [Hark 等人 2020]

B 最弱前期望的组合推理

根据定义 2，最弱前期望可以按照 McIver 和 Morgan 的最弱前期望演算以组合方式求得。正如 [Hark 等人 2020], 所解释的，该演算采用期望变换器，以延续传递风格在程序中逆向传播，示意见图 7。如果我们关心执行顺序组合 $C_1 ; C_2$后某个后期望f的期望值，那么首先可以计算 C_2 相对于 f的最弱前期望，即 $\mathsf{wp}[\![C_2]\!](f)$。随后，我们可以将中间结果 $\mathsf{wp}[\![C_2]\!](f)$作为后期望，求出 C_1 相对于 $\mathsf{wp}[\![C_2]\!](f)$的最弱前期望。最终，我们得到 $C_1 ; C_2$ 相对于后期望 f的最弱前期望。下面的例子展示了如何以这种逆向的组合方式应用 wp 演算。

例 **例 31（应用 最弱前置条件 演算）**。考虑由以下内容给出的概率程序 C

$$p :\approx \mathtt{uniform}\,(0,1) ; \; n := n-1 \; [p] \; n := n+1 \,,$$

其中 均匀 (0,1) 是 0 到 1 之间的连续均匀分布。假设我们要通过确定 n 终止时的 C 的最弱前置条件$[\![C]\!](n)$来推断其期望值。根据表 1，

$$\begin{aligned}
\mathsf{wp}[\![C]\!](n) &= \mathsf{wp}[\![p :\approx \mathtt{uniform}\,(0,1)]\!](\mathsf{wp}[\![n := n-1 \; [p] \; n := n+1]\!](n)) \\
&= \mathsf{wp}[\![p :\approx \mathtt{uniform}\,(0,1)]\!](p\cdot(n-1)+(1-p)\cdot(n+1)) \\
&= \mathsf{wp}[\![p :\approx \mathtt{uniform}\,(0,1)]\!](n+1-2p) \\
&= \int_{[0,1]} (n+1-2p)\,\mathrm{d}\,p \;=\; n\,.
\end{aligned}$$

这表明， C终止时 n的期望值为 n，即 C不会改变 n的初始值的期望值。◁

C 补充证明

C.1 定理 (12)的证明

Lemma 32. 按照定理 11中的记号，设 ϕ_1 和 ϕ_2 为任意两个谓词，我们有 e

$$\lambda\sigma.\ \int_{D(\neg\phi_1,\phi_2)} f_{C_{\text{loop}}}\,\mathrm{d}\left({}^{\sigma}\mathbb{P}\right) \;=\; \mathsf{wp}[\![\mathtt{while}\,(\,\phi_1\wedge\phi_2\,)\,\{C\}]\!]\,([\neg\phi_1\wedge\phi_2]\cdot f)\ . \tag{17}$$

证明。令 $C^{\wedge}_{\text{loop}}$表示循环 $\mathsf{while}\,(\,\phi_1\wedge\phi_2)\,\{C\}$，对于任意 $l\colon \Sigma\to\mathbb{R}^{\infty}_{\geq 0}$，令 $l_{C^{\wedge}_{\text{loop}}}$表示一个偏函数：当轨迹 $s\in\mathbb{S}$在 σ_n处首次命中 $\neg(\phi_1\wedge\phi_2)$时，将其映射到 $l(\sigma_n)$，即

$$l_{C^{\wedge}_{\text{loop}}}\colon \mathbb{S}\rightharpoonup\mathbb{R}^{\infty}_{\geq 0} \qquad \sigma_0\sigma_1\cdots\sigma_i\cdots\mapsto g(\sigma_n) \quad \text{if } (\sigma_n\models\neg(\phi_1\wedge\phi_2))\wedge(\forall i<n\colon \sigma_i\models(\phi_1\wedge\phi_2))\ .$$

令 $h\triangleq[\neg\phi_1\wedge\phi_2]\cdot f$。不难验证，对于 $s\in D(\neg\phi_1,\ \phi_2)$，有 $h_{C^{\wedge}_{\text{loop}}}(s)=f_{C^{\wedge}_{\text{loop}}}(s)$；对于 $s\in D(\neg\phi_2,\ \phi_1)$，有 $h_{C^{\wedge}_{\text{loop}}}(s)=0\cup C$。根据（次）概率测度 ${}^{\sigma}\mathbb{P}$ 的定义，我们有

$$\begin{aligned}
\mathsf{wp}[\![C^{\wedge}_{\text{loop}}]\!]\,([\neg\phi_1\wedge\phi_2]\cdot f) &= \lambda\sigma.\ \int_{\Diamond(\neg(\phi_1\wedge\phi_2))} h_{C^{\wedge}_{\text{loop}}}\,\mathrm{d}\left({}^{\sigma}\mathbb{P}\right) \\
&= \lambda\sigma.\ \int_{D(\neg\phi_1,\phi_2)\uplus D(\neg\phi_2,\phi_1)\uplus C} h_{C^{\wedge}_{\text{loop}}}\,\mathrm{d}\left({}^{\sigma}\mathbb{P}\right) \\
&= \lambda\sigma.\ \int_{D(\neg\phi_1,\phi_2)} h_{C^{\wedge}_{\text{loop}}}\,\mathrm{d}\left({}^{\sigma}\mathbb{P}\right) + \lambda\sigma.\ \int_{D(\neg\phi_2,\phi_1)\cup C} h_{C^{\wedge}_{\text{loop}}}\,\mathrm{d}\left({}^{\sigma}\mathbb{P}\right) \\
&\qquad\qquad [\text{by linearity of } \textstyle\int]
\end{aligned}$$

$$= \lambda\sigma.\ \int_{D(\neg\phi_1,\phi_2)} f_{C^{\wedge}_{\text{loop}}}\ \mathrm{d}\left({}^{\sigma}\mathbb{P}\right)\ , \qquad \text{[by definition of } h_{C^{\wedge}_{\text{loop}}}\text{]}$$

其中第二个等号源于集合分解：

$$\Diamond\left(\neg\left(\phi_1 \wedge \phi_2\right)\right) \ = \ D\left(\neg\phi_1, \phi_2\right) \ \uplus \ D\left(\neg\phi_2, \phi_1\right) \ \uplus \ C\ .$$

证明至此完成。 □

C.2 推论 13 的证明推论 13

推论 13。 给定循环 $C_{\text{loop}} = \texttt{while}(\varphi)\{C\}$和 $C'_{\text{loop}} = \texttt{while}(\varphi')\{C\}$，假设 $\varphi' \Longrightarrow \varphi$，那么对于任意后期望 $f \in \mathbb{E}$，

$$\mathsf{wp}[\![C_{\text{loop}}]\!]\left(f\right) \ \geq \ \mathsf{wp}[\![C'_{\text{loop}}]\!]\left([\neg\varphi]\cdot f\right)\ .$$

证明。 由于 $\varphi' \Longrightarrow \varphi$，我们有 $\varphi \wedge \varphi\prime = \varphi\prime$，$[\neg\varphi \wedge \varphi\prime] = 0$，以及 $B = \emptyset$(即，任何轨迹都不可能在命中 $\neg\varphi$ 之前命中 $\neg\varphi'$)。因此，根据 定理 11，

$$\begin{aligned}
\mathsf{wp}[\![C_{\text{loop}}]\!]\left(f\right) - \mathsf{wp}[\![C'_{\text{loop}}]\!]\left(f\right) \ &= \ \lambda\sigma.\ \int_A f_{C_{\text{loop}}}\ \mathrm{d}\left({}^{\sigma}\mathbb{P}\right) - \mathsf{wp}[\![\texttt{while}\left(\varphi'\right)\{C\}]\!]\left([\varphi\wedge\neg\varphi'\right]\cdot f) \\
&= \ \lambda\sigma.\ \int_A f_{C_{\text{loop}}}\ \mathrm{d}\left({}^{\sigma}\mathbb{P}\right) - \mathsf{wp}[\![\texttt{while}\left(\varphi'\right)\{C\}]\!]\left([\varphi]\cdot f\right) \\
&\qquad\qquad \text{[by definition of wp-transformer, cf. Table 1]} \\
&= \ \lambda\sigma.\ \int_A f_{C_{\text{loop}}}\ \mathrm{d}\left({}^{\sigma}\mathbb{P}\right) - \mathsf{wp}[\![C'_{\text{loop}}]\!]\left([\varphi]\cdot f\right)\ .
\end{aligned}$$

由此可得

$$\begin{aligned}
\mathsf{wp}[\![C_{\text{loop}}]\!]\left(f\right) \ &= \ \mathsf{wp}[\![C'_{\text{loop}}]\!]\left(f\right) - \mathsf{wp}[\![C'_{\text{loop}}]\!]\left([\varphi]\cdot f\right) + \lambda\sigma.\ \int_A f_{C_{\text{loop}}}\ \mathrm{d}\left({}^{\sigma}\mathbb{P}\right) \\
&= \ \mathsf{wp}[\![C'_{\text{loop}}]\!]\left([\neg\varphi]\cdot f\right) + \lambda\sigma.\ \int_A f_{C_{\text{loop}}}\ \mathrm{d}\left({}^{\sigma}\mathbb{P}\right) \\
&\qquad\qquad \text{[by linearity of wp-transformer, cf., e.g., [Kaminski 2019, Chap. 8.5]]} \\
&\geq \ \mathsf{wp}[\![C'_{\text{loop}}]\!]\left([\neg\varphi]\cdot f\right)\ . \qquad [f_{C_{\text{loop}}} \geq 0]
\end{aligned}$$

证明到此完成。 □

我们下界规则的与轨迹无关证明 定理 14

定理 14（下界的守卫强化）。给定循环 $C_{\text{loop}} = \texttt{while}(\varphi)\{C\}$、$C'_{\text{loop}} = \texttt{while}(\varphi')\{C\}$ 和后期望 $f \in \mathbb{E}$，令 $l \in \mathbb{E}$，则以下推理规则成立：

$$\frac{\varphi' \Longrightarrow \varphi \qquad l \ \preceq \ \mathsf{wp}[\![C'_{\text{loop}}]\!]\left([\neg\varphi]\cdot f\right)}{l \ \preceq \ \mathsf{wp}[\![C_{\text{loop}}]\!]\left(f\right)}\ \textsc{Guard-Strengthening}\ . \tag{14}$$

证明（与轨迹无关）。只需证明 $\mathsf{wp}[\![C'_{\text{loop}}]\!]\left([\neg\varphi]\cdot f\right) \preceq \mathsf{wp}[\![C_{\text{loop}}]\!]\left(f\right)$。根据 wp-变换器的定义（见 定理 3），我们有

$$\mathsf{wp}[\![C'_{\text{loop}}]\!]\left([\neg\varphi]\cdot f\right) \ = \ \mathsf{lfp}\ {}^{\mathsf{wp}}_{\langle\varphi',C\rangle}\Phi_{[\neg\varphi]\cdot f} \ = \ \lim_{k\to\omega}\left({}^{\mathsf{wp}}_{\langle\varphi',C\rangle}\Phi_{[\neg\varphi]\cdot f}\right)^{k}(0)\ ,$$

类似地，

$$\mathsf{wp}[\![C_{\text{loop}}]\!]\left(f\right) \ = \ \mathsf{lfp}\ {}^{\mathsf{wp}}_{\langle\varphi,C\rangle}\Phi_{f} \ = \ \lim_{k\to\omega}\left({}^{\mathsf{wp}}_{\langle\varphi,C\rangle}\Phi_{f}\right)^{k}(0)\ .$$

现在我们通过归纳法证明，对于任意 $k \in \mathbb{N}$,

$$\left(\mathrm{wp}_{\langle \varphi', C\rangle}\Phi_{[\neg\varphi]\cdot f}\right)^k(0) \;\le\; \lim_{k\to\omega}\left(\mathrm{wp}_{\langle \varphi, C\rangle}\Phi_f\right)^k(0)\;. \tag{18}$$

如果是这种情况，最弱前置条件$[\![C'_{\text{loop}}]\!]([\neg\varphi]\cdot f) \le$ 最弱前置条件$[\![C_{\text{loop}}]\!](f)$ 可通过对 k 取极限，由(18)两边得到。对于 $k=0$的基础步骤，归纳目标(18) 显然成立：

$$\left(\mathrm{wp}_{\langle \varphi', C\rangle}\Phi_{[\neg\varphi]\cdot f}\right)^0(0) \;=\; 0 \;=\; \left(\mathrm{wp}_{\langle \varphi, C\rangle}\Phi_f\right)^0(0)\;. \tag{19}$$

对于归纳步骤，假设(18) 对 $k=i$成立，那么对于 $k=i+1$，有

$$\begin{aligned}\left(\mathrm{wp}_{\langle \varphi', C\rangle}\Phi_{[\neg\varphi]\cdot f}\right)^{i+1}(0) &= [\neg\varphi]\cdot[\neg\varphi']\cdot f + [\varphi']\cdot \mathrm{wp}[\![C]\!]\left(\left(\mathrm{wp}_{\langle \varphi', C\rangle}\Phi_{[\neg\varphi]\cdot f}\right)^{i}(0)\right)\\ &\le [\neg\varphi]\cdot f + [\varphi]\cdot \mathrm{wp}[\![C]\!]\left(\left(\mathrm{wp}_{\langle \varphi, C\rangle}\Phi_{f}\right)^{i}(0)\right)\\ &= \left(\mathrm{wp}_{\langle \varphi, C\rangle}\Phi_f\right)^{i+1}(0)\;.\end{aligned}$$

因此，(18) 对任意 $k \in \mathbb{N}$均成立。证明完毕。 □

C.4 引理15的详细证明

引理 15（几乎必然终止见证）。给定 $C'_{\text{loop}} =$while循环$(\varphi')\{C\}$，令 $T^{\neg\varphi'}$为 C'_{loop}的循环时间。如果存在 $N \in \mathbb{N}$ 和 $p \in (0,1)$，使得对于任意初始状态 $\sigma \in \Sigma$,

$${}^{\sigma}\mathbb{P}\left(T^{\neg\varphi'} > N\right) \;\le\; p\,, \tag{15}$$

那么 C'_{loop} 几乎必然终止。

证明。我们首先证明，C'_{loop} 在 $n \in \mathbb{N}$ 步内未终止的概率会随 n 指数级下降。为此，对于任意 $k \in \mathbb{N}$，有：

$$\begin{aligned}{}^{\sigma}\mathbb{P}\left(T^{\neg\varphi'} > kN\right) &= {}^{\sigma}\mathbb{P}\left(\forall i \le kN : X_i \models \varphi'\right)\\ &\le \max_{X_0, X_N, \ldots, X_{(k-1)N} \models \varphi'} {}^{X_0}\mathbb{P}\left(T^{\neg\varphi'} > N\right)\cdot {}^{X_N}\mathbb{P}\left(T^{\neg\varphi'} > N\right)\cdots {}^{X_{(k-1)N}}\mathbb{P}\left(T^{\neg\varphi'} > N\right)\\ &\le p\cdot p\cdots p \qquad \text{[by (15)]}\\ &= p^k\;.\end{aligned}$$

由此可知，对于任意 $n \in \mathbb{N}$ 以及任意初始状态 $\sigma \in \Sigma$,

$${}^{\sigma}\mathbb{P}\left(T^{\neg\varphi'} > n\right) \;\le\; p^{\lfloor n/N\rfloor} \;\le\; p^{n/N-1} \;=\; {}^{1}\!/_{p}\cdot \mathrm{e}^{\log(p)\cdot n/N}\;.$$

对于任意固定的 $p \in (0,1)$，有 $\log(p) < 0$，因此 ${}^{\sigma}\mathbb{P}(T^{\neg\varphi'} > n)$ 会随 n 指数级下降。令 n 趋于无穷大，可得

$${}^{\sigma}\mathbb{P}\left(T^{\neg\varphi'} < \infty\right) \;=\; 1 - \lim_{n\to\infty} {}^{\sigma}\mathbb{P}\left(T^{\neg\varphi'} > n\right) \;\ge\; 1 - \lim_{n\to\infty} {}^{1}\!/_{p}\cdot \mathrm{e}^{\log(p)\cdot n/N} \;=\; 1 - 0 \;=\; 1\;.$$

因此，C'_{loop} 几乎必然终止。 □

C.5 定理 Thm.18 的证明

定理 18（一致可积性的正交充分判据）。设 C'_{loop} =while循环 (φ'){ C}满足引理 15中的几乎必然终止条件。则，期望 $h \ll \infty$ 对于 C'_{loop}，若满足 ***(i)*** C'_{loop} 具有有界更新性质[17],，即存在 $c \in \mathbb{R}_{\geq 0}$，使得对任意 $\sigma \in \Sigma$，$^{\sigma}\mathbb{P}(\forall n \in \mathbb{N}\colon\ |X_{n+1} - X_n| \leq c) = 1$，且 ***(ii)*** h由多项式期望所界定[18]。

证明。设 $^{\sigma}\mathbb{P}$是在 C'_{loop}初始状态 $\sigma \in \Sigma$ 上诱导的概率测度，$T^{\neg\varphi'}$是 C'_{loop}的循环时间，且 $\left\{X_n^{T^{\neg\varphi'}}\right\}_{n\in\mathbb{N}}$是相应的停止过程。根据 定义 7，我们需要证明 $\left\{h\left(X_n^{T^{\neg\varphi'}}\right)\right\}_{n\in\mathbb{N}}$在 $^{\sigma}\mathbb{P}$上一致可积。根据 [Williams 1991，定理 13，3],只需证明随机过程 $\left\{h\left(X_n^{T^{\neg\varphi'}}\right)\right\}_{n\in\mathbb{N}}$被某个 可积随机变量支配，即 $\left|h\left(X_n^{T^{\neg\varphi'}}\right)\right|$被某个期望值有限的随机变量所界定。

根据 C'_{loop}的有界更新性质，存在 $c \in \mathbb{R}_{\geq 0}$ 使得

$$\forall n \in \mathbb{N}\colon\ |X_n| \leq |X_n - X_{n-1}| + |X_{n-1} - X_{n-2}| + \ldots + |X_1 - X_0| + |X_0| \leq c \cdot n + |\sigma|$$

几乎必然成立。此外，由于 h 由多项式期望所界定，我们有

$$|h(X_{n+1}) - h(X_n)| \leq poly(n)$$

对于某个关于 n的多项式 $poly$ 成立。此外，注意到

$$\left|h\left(X_n^{T^{\neg\varphi'}}\right)\right| \leq |h(X_0)| + \sum_{k=0}^{\infty} |h(X_{k+1}) - h(X_k)| \cdot \left[T^{\neg\varphi'} > k\right]. \tag{20}$$

因此，只需 证明 (20) 右侧的期望值有限。注意 t

$$\begin{aligned} {}^{\sigma}E\left[|h(X_{k+1}) - h(X_k)| \cdot \left[T^{\neg\varphi'} > k\right]\right] &\leq {}^{\sigma}E\left[poly(k) \cdot \left[T^{\neg\varphi'} > k\right]\right] \\ &= poly(k) \cdot {}^{\sigma}\mathbb{P}\left(T^{\neg\varphi'} > k\right) \\ &\leq poly(k) \cdot a \cdot \mathrm{e}^{-b\cdot k}. \quad [\text{for } a, b \in \mathbb{R}_{>0}, \text{cf. proof of Lem. 15}] \end{aligned}$$

由此可知，(20) 右侧的期望值有限，即

$$\begin{aligned} {}^{\sigma}E\left[|h(X_0)| + \sum_{k=0}^{\infty} |h(X_{k+1}) - h(X_k)| \cdot \left[T^{\neg\varphi'} > k\right]\right] &\leq {}^{\sigma}E[|h(X_0)|] + \sum_{k=0}^{\infty} poly(k) \cdot a \cdot \mathrm{e}^{-b\cdot k} \\ &< \infty. \end{aligned}$$

证明至此完成。 □

C.6 引理 引理 20的详细证明

引理 20。给定循环 C_{loop} =while(φ){ C}和 C'_{loop} =while(φ'){ C}，假设 $\varphi' \Longrightarrow \varphi$，那么对于任意后期望 $f \in \mathbb{E}$,

$$\text{wp}[\![C_{\text{loop}}]\!](f) - \text{wp}[\![C'_{\text{loop}}]\!]([\neg\varphi] \cdot f) \leq \text{wp}[\![C'_{\text{loop}}]\!]([\varphi]) \cdot \sup_{\sigma \models \neg\varphi' \wedge \varphi} \text{wp}[\![C_{\text{loop}}]\!](f)(\sigma).$$

证明。如推论 13的证明中所示，我们有

$$\text{wp}[\![C_{\text{loop}}]\!](f) - \text{wp}[\![C'_{\text{loop}}]\!]([\neg\varphi] \cdot f) = \lambda\sigma. \int_A f_{C_{\text{loop}}} \, \mathrm{d}\left({}^{\sigma}\mathbb{P}\right).$$

[17]有界更新性质已被用于分析非确定性概率程序的期望成本 [Wang 等人 2019]；它涵盖了常概率程序这一类 [Giesl 等人 2019]。 [18]可以将 (ii) 替换为 **(ii')** h 有界于一个分段多项式期望，定理仍然成立。

因此，只需给出上述积分的上界。回顾一下，在 $\varphi' \Longrightarrow \varphi, A \subseteq \mathbb{S}$ 是在到达 $\neg\varphi$ 之前到达 $\neg\varphi' \wedge \varphi$ 的轨迹集合，而 $f_{C_{\text{loop}}}$ 将轨迹 $s \in \mathbb{S}$ 映射为 $f(\sigma_n)$，当且仅当 s 首次在 σ_n 到达 $\neg\varphi$。令 X 将轨迹 $s \in \mathbb{S}$ 映射为 σ_n，当且仅当 s 首次在 σ_n 到达 $\neg\varphi'$，即 $X(\sigma_0\sigma_1\cdots\sigma_i\cdots) \triangleq \sigma_n$，如果 $(\sigma_n \models \neg\varphi_\prime) \wedge (\forall i < n\colon\ \sigma_i \models \varphi')$；并令 $[\varphi]_{C'_{\text{loop}}}$ 将轨迹 $s \in \mathbb{S}$ 映射为 $[\varphi](X(s))$。我们有

$$
\begin{aligned}
\lambda\sigma.\ \int_A f_{C_{\text{loop}}}\ \mathrm{d}\left({}^{\sigma}\mathbb{P}\right) &= \lambda\sigma.\ \int_{\Diamond\neg\varphi'} \left([\varphi]_{C'_{\text{loop}}} \cdot \lambda s.\ \int_{\Diamond\neg\varphi} f_{C_{\text{loop}}}\ \mathrm{d}\left({}^{X(s)}\mathbb{P}\right)\right) \mathrm{d}\left({}^{\sigma}\mathbb{P}\right) \\
&= \lambda\sigma.\ \int_{\Diamond\neg\varphi'} \left([\varphi]_{C'_{\text{loop}}} \cdot \lambda s.\ \mathsf{wp}[\![C_{\text{loop}}]\!]\,(f)\,(X(s))\right) \mathrm{d}\left({}^{\sigma}\mathbb{P}\right) \\
&\leq \lambda\sigma.\ \int_{\Diamond\neg\varphi'} \left([\varphi]_{C'_{\text{loop}}} \cdot \sup_{\sigma\models\neg\varphi'\wedge\varphi} \mathsf{wp}[\![C_{\text{loop}}]\!]\,(f)\,(\sigma)\right) \mathrm{d}\left({}^{\sigma}\mathbb{P}\right) \\
&= \lambda\sigma.\ \int_{\Diamond\neg\varphi'} \left([\varphi]_{C'_{\text{loop}}}\right) \mathrm{d}\left({}^{\sigma}\mathbb{P}\right) \cdot \sup_{\sigma\models\neg\varphi'\wedge\varphi} \mathsf{wp}[\![C_{\text{loop}}]\!]\,(f)\,(\sigma) \\
&= \mathsf{wp}[\![C'_{\text{loop}}]\!]\,([\varphi]) \cdot \sup_{\sigma\models\neg\varphi'\wedge\varphi} \mathsf{wp}[\![C_{\text{loop}}]\!]\,(f)\,(\sigma)\ .
\end{aligned}
$$

证明至此完成。 □

D 示例详解

D.1 检查次不变性和超不变性 例16

我们给出详细计算，以检查 l_M 的次不变性和 l_∞ 的超不变性。首先检查 $l_M \leq \Phi_g^M(l_M)$ 的有效性。根据 Φ_g^M 的定义，我们有

$$
\begin{aligned}
\Phi_g^M\,(l_M) &= [n \leq 0 \vee n \geq M] \cdot [n \leq 0] + [0 < n < M] \cdot (1/3 \cdot l_M\,[n/n-1] + 2/3 \cdot l_M\,[n/n+1]) \\
&= [n \leq 0] + [0 < n < M] \cdot \left(1/3 \cdot \left((1/2)^{n-1} - (1/2)^M\right) + 2/3 \cdot \left((1/2)^{n+1} - (1/2)^M\right)\right) \\
&= [n \leq 0] + [0 < n < M] \cdot \left((1/2)^n - (1/2)^M\right) \\
&\geq [n < 0] + [0 \leq n \leq M] \cdot \left((1/2)^n - (1/2)^M\right) \\
&= l_M\ .
\end{aligned}
$$

对于 $\Phi_f(l_\infty) \preceq l_\infty$ 的有效性，我们有

$$
\begin{aligned}
\Phi_f(l_\infty) &= [n \leq 0] \cdot 1 + [n > 0] \cdot (1/3 \cdot l_\infty\,[n/n-1] + 2/3 \cdot l_\infty\,[n/n+1]) \\
&= [n \leq 0] + [n > 0] \cdot \left(1/3 \cdot (1/2)^{n-1} + 2/3 \cdot (1/2)^{n+1}\right) \\
&= [n \leq 0] + [n > 0] \cdot (1/2)^n \\
&= [n < 0] + [n \geq 0] \cdot (1/2)^n \\
&= l_\infty\ .
\end{aligned}
$$

D.2 检查例17的次不变性

我们详细列出检查 l_M 次不变性的计算过程，即 $l_M \leq \Phi_g^M(l_M)$。回顾

$$
l_M = [a \neq 1] \cdot b + \sum_{i=1}^{\lceil \log_2 M \rceil} [a = 1 \wedge (M/2^i \leq b < M/2^{i-1})] \cdot i \cdot b/2\ .
$$

根据 Φ_g^M 的定义，我们有

$$
\Phi_g^M\,(l_M) = [a \neq 1 \vee b \geq M] \cdot [a \neq 1] \cdot b + [a = 1 \wedge b < M] \cdot (1/2 \cdot l_\infty\,[a/0] + 1/2 \cdot l_\infty\,[b/2b])
$$

$$
\begin{aligned}
&= [a \neq 1] \cdot b + [a = 1 \wedge b < M] \cdot \left(1/2 \cdot b + 1/2 \cdot \sum_{i=1}^{\lceil \log_2 M \rceil} [M/2^i \leq 2b < M/2^{i-1}] \cdot i \cdot b \right) \\
&= [a \neq 1] \cdot b + [a = 1 \wedge b < M] \cdot \left(1/2 \cdot b + 1/2 \cdot \sum_{i=1}^{\lceil \log_2 M \rceil} [M/2^{i+1} \leq b < M/2^i] \cdot i \cdot b \right) \\
&= [a \neq 1] \cdot b + [a = 1 \wedge b < M] \cdot \left(\sum_{i=0}^{\lceil \log_2 M \rceil} [M/2^{i+1} \leq b < M/2^i] \cdot (i+1) \cdot b/2 \right) \\
&= [a \neq 1] \cdot b + [a = 1 \wedge b < M] \cdot \left(\sum_{i=1}^{\lceil \log_2 M \rceil + 1} [M/2^i \leq b < M/2^{i-1}] \cdot 1 \cdot b/2 \right) \\
&= [a \neq 1] \cdot b + \sum_{i=1}^{\lceil \log_2 M \rceil} [a = 1 \wedge (M/2^i \leq b < M/2^{i-1})] \cdot i \cdot b/2 \\
&= l_M \,.
\end{aligned}
$$

D.3 检查次不变性和非条件差有界性（针对例19

我们给出详细计算，以检验 l_M 的次不变性，即 $l_M \leq \Phi_g^M(l_M)$，并证明 l_M 不满足条件差有界。回顾

$$l_M = [n < 0] \cdot b + [0 \leq n \leq M] \cdot (b + 2 \cdot n) \cdot (1 - n/M) \,.$$

根据 $\Phi_g^M(l_M)$ 的定义，我们有

$$
\begin{aligned}
\Phi_g^M(l_M) &= [n \leq 0] \cdot b + [0 < n < M] \cdot (1/2 \cdot l_M[n/n-1][b/b+2] + 1/2 \cdot l_M[n/n+1][b/b-2]) \\
&= [n \leq 0] \cdot b + 1/2 \cdot [0 < n < M] \cdot (b + 2n) \cdot ((1 - (n-1)/M) + (1 - (n+1)/M)) \\
&= [n \leq 0] \cdot b + [0 < n < M] \cdot (b + 2n) \cdot (1 - n/M) \\
&= [n < 0] \cdot b + [0 \leq n \leq M] \cdot (b + 2n) \cdot (1 - n/M) \\
&= l_M \,.
\end{aligned}
$$

因此，$l_M \leq \Phi_g^M(l_M)$ 成立。

现在我们证明 l_M 不是条件差有界的。令 C_{bubody} 表示 C_{bu} 在 例19中的循环体。回忆一下，l_M 是条件差有界的，当且仅当存在 $c \in \mathbb{R}_{>0}$ 使得最弱前置条件 $[\![C_{\text{bubody}}]\!](|l_M - l_M(\sigma)|) \leq c$ 对任意 σ 满足以下循环守卫的 C_{bu}^M。我们证明

$$\Delta l_M = [0 < n < M] \cdot \text{wp}[\![C_{\text{bubody}}]\!](|l_M - l_M(\sigma)|)$$

是无界的。由于

$$
\begin{aligned}
\Delta l_M &= [0 < n < M] \cdot \frac{1}{2}(|l_M - l_M(\sigma)|[n/n-1][b/b+2] + |l_M - l_M(\sigma)|[n/n+1][b/b-2]) \\
&= [0 < n < M] \cdot \frac{1}{2}(|l_M[n/n-1][b/b+2] - l_M|(\sigma) + |l_M[n/n+1][b/b-2] - l_M|(\sigma)) \\
&= [0 < n < M] \cdot \frac{1}{2}\left(\left| (b+2n)\frac{1}{M} \right|(\sigma) + \left| (b+2n)\frac{1}{M} \right|(\sigma) \right) \\
&= [0 < n < M] \cdot \frac{|b+2n|}{M}(\sigma) \,.
\end{aligned}
$$

当 b 在守卫条件（$0 < n < M$）下可以任意大时，Δl_M 无界。因此，l_M 不是条件差有界的。

D.4 检查例25的次不变性

我们给出关于检查 l_M 的次不变性（即 $l_M \leq \Phi_g^M(l_M)$）的详细计算。回忆一下

$$l_M = [n < 0] \cdot b + [0 \leq n \leq M] \cdot (b + 1/2 \cdot n) \cdot (1 - n/M) \,.$$

根据 Φ_g^M的定义，我们有

$$\begin{aligned}\Phi_g^M\left(l_M\right) &= [n \le 0]\cdot b + [0 < n < M]\cdot \\ &\quad \int_0^1 \left(p\cdot \int_0^1 l_M\left[n/n-1\right]\left[b/b+r_1\right]\,\mathrm{d}\,r_1 + (1-p)\cdot \int_0^1 l_M\left[n/n+1\right]\left[b/b-r_2\right]\,\mathrm{d}\,r_2\right)\mathrm{d}\,p \\ &= [n \le 0]\cdot b + [0 < n < M]\cdot \left(1/2\cdot l_M\left[n/n-1\right]\left[b/b+1/2\right] + 1/2\cdot l_M\left[n/n+1\right]\left[b/b-1/2\right]\right) \\ &= [n \le 0]\cdot b + [0 < n < M]\cdot (b+1/2\cdot n)\cdot (1-n/M) \\ &= [n < 0]\cdot b + [0 \le n \le M]\cdot (b+1/2\cdot n)\cdot (1-n/M) \;=\; l_M\,.\end{aligned}$$

D.5 检查 例 26 的次不变性

我们给出　检查 l_M 次不变性的详细计算。为此，我们首先证明

$$\begin{aligned}\mathrm{wp}[\![C^M_{\mathrm{inner}}]\!]\left(h\right) \;&\ge\; [(k-n<-a)\vee(k-n>b)]\cdot h + \\ &\qquad [-a\le k-n\le b]\cdot\left(\frac{b-(k-n)}{b+a}\cdot h\left[k/n-a\right] + \frac{(k-n)+a}{b+a}\cdot h\left[k/n+b\right]\right) \\ &\triangleq\; l_{\mathrm{inner}} \qquad (21)\end{aligned}$$

ho对于任意有界后期望 $h\in\mathbb{E}$ 都成立，其中 C^M_{inner} 是 C^M_{nl} 的内层循环，即

$$C^M_{\mathrm{inner}} = \texttt{while}\,(\,-a<k-n<b\,)\,\{\,k\coloneqq k-1\;[1/2]\;k\coloneqq k+1\,\}\;.$$

由于 C^M_{inner} 至多经过 a 步连续递减的 k，就会以概率 $(1/2)^a$终止，因此根据 引理 15，我们知道它几乎必然终止。此外， l_{inner} 有界，因此根据 定理 8 和 9，$l_{\mathrm{inner}}\preceq$最弱前置条件$[\![C^M_{\mathrm{inner}}]\!]\left(h\right)$若 l_{inner}是关于后期望 h的 C^M_{inner}次不变式，则成立。事实上，

$$\begin{aligned}\Phi_h^{\mathrm{inner}}\left(l_{\mathrm{inner}}\right) \;&=\; [(k-n\le -a)\vee(k-n\ge b)]\cdot h + \\ &\qquad [-a<k-n<b]\cdot\left(1/2\cdot l_{\mathrm{inner}}\left[k/k-1\right] + 1/2\cdot l_{\mathrm{inner}}\left[k/k+1\right]\right) \\ &=\; [(k-n\le -a)\vee(k-n\ge b)]\cdot h + \\ &\qquad [-a<k-n<b]\cdot\left(\frac{b-(k-n)}{b+a}\cdot h\left[k/n-a\right] + \frac{(k-n)+a}{b+a}\cdot h\left[k/n+b\right]\right) \\ &=\; [(k-n<-a)\vee(k-n>b)]\cdot h + \\ &\qquad [-a\le k-n\le b]\cdot\left(\frac{b-(k-n)}{b+a}\cdot h\left[k/n-a\right] + \frac{(k-n)+a}{b+a}\cdot h\left[k/n+b\right]\right) \\ &=\; l_{\mathrm{inner}}\,.\end{aligned}$$

由此可知， l_{inner} 是最弱前置条件$[\![C^M_{\mathrm{inner}}]\!](h)$的下界。现在我们继续计算例 26 ，以检查 l_M的次不变性：

$$\begin{aligned}\Phi_g^M\left(l_M\right) \;&=\; [n\le 0\vee n\ge M]\cdot[n\le 0] + [0<n<M]\cdot\mathrm{wp}[\![C^M_{\mathrm{body}}]\!]\left(l_M\right) \\ &=\; [n\le 0] + [0<n<M]\cdot \\ &\qquad \mathrm{wp}[\![k\coloneqq n\fatsemi C^M_{\mathrm{inner}}]\!]\left([k<n]\cdot l_M\left[n/n-1\right] + [k\ge n]\cdot l_M\left[n/n+1\right]\right) \\ &=\; [n\le 0] + [0<n<M]\cdot \\ &\qquad \mathrm{wp}[\![k\coloneqq n]\!]\left(\mathrm{wp}[\![C^M_{\mathrm{inner}}]\!]\left([k<n]\cdot l_M\left[n/n-1\right] + [k\ge n]\cdot l_M\left[n/n+1\right]\right)\right)\end{aligned}$$

$$
\begin{aligned}
&= [n \le 0] + [0 < n < M] \cdot \\
&\quad \Big(\underbrace{\mathrm{wp}[\![C^M_{\text{inner}}]\!]\,([k < n] \cdot l_M\,[n/n-1] + [k \ge n] \cdot l_M\,[n/n+1])}_{\text{apply (21)}} \Big)\,[k/n] \\
&= [n \le 0] + [0 < n < M] \cdot \left((b/a)^n - (b/a)^M \right) \\
&\ge [n < 0] + [0 \le n \le M] \cdot \left((b/a)^n - (b/a)^M \right) \\
&= l_M\,.
\end{aligned}
$$

由此可知， l_M 是一个次不变式。