arXiv:2303.03292v1 [cs.FL] 6 Mar 2023

部分可观测随机系统的活性性质黑盒测试

Javier Esparza* 和 Vincent Grande†

我们研究随机系统和任意 ω正则规范的黑盒测试，其中明确包括活性性质。我们给定一个只能从初始状态执行的有限状态概率系统。我们不了解可达状态的数量或概率；此外，我们只能部分观测状态。我们唯一能采取的操作是重启系统。我们设计了重启策略，保证如果规范以非零概率被违例，那么以概率 1，重新启动的次数是有限的，并且在最后一次重启后执行的无限运行违反该规范。这改进了以往要求完全可观测性的研究。我们获得了截至最后一次重启前步数期望值的渐近最优上界。我们在多个基准上开展实验，结果表明，我们的策略能够在远大于以往研究所考虑规模的马尔可夫链中发现违例。

1. 引言

当用户无法访问系统的设计或内部结构时，黑盒测试是一种基本的分析技术 [12, 15]。由于每次只检查系统的一次运行，因此计算成本较低，这使得它往往成为大型系统唯一适用的方法。

我们研究有限状态概率系统和ω-正则规约的黑盒测试问题：给定一个 ω-正则规约，该问题包括

*慕尼黑工业大学
†亚琛工业大学，由德国研究联合会（DFG）通过研究培训组 2236（UnRAVeL）资助

找出违反该性质的程序运行，并假设此类运行的概率非零。

让我们更详细地描述我们的假设。我们无法访问系统的代码或其内部结构，也不知道其状态空间大小的任何上界。我们可以反复运行系统，并随时重启系统。不失一般性，我们假设系统的所有运行都是无限的。我们不假设系统的状态具有完全可观测性，只假设我们能够观测该性质的原子命题当前为真还是为假。例如，如果该性质规定某个系统变量（比如x）应当无限多次取正值，那么我们只假设在每个状态下都能观测x的符号；令 Σ 表示可能观测的集合，则有 $\Sigma = \{+, -\}$，分别表示正值和零值或负值（在引言其余部分，我们将“零值或负值”简称为“负值”）。系统的每次执行都会导出一个观测，也就是 Σ^ω 的一个元素。该性质的违例是仅包含有限个 $+$ 出现的 ω-词 $V \subseteq \Sigma^\omega$。

我们的目标是找到一种策略，在每一步之后决定是中止当前运行并重启系统，还是继续当前运行。该策略必须确保最终执行某个违反性质的运行，也就是说，其观测属于V的运行。策略根据目前为止所作的观测来决定。形式上，给定 Σ 和动作集合$A = \{\mathrm{r}, \mathrm{c}\}$（分别表示“重启”和“继续”），针对$V$ 的策略是一个映射：将$(\Sigma \times A)^*\Sigma$（即目前为止已执行的观测和动作序列）映射到$A$（即下一步决策）。我们的目标是找到满足以下性质的策略 σ：

> 对于 Σ上的每个有限状态程序P，如果$V \subseteq \Sigma^\omega$ 具有正概率，且P 的运行按照 σ重新启动，那么以概率1，重新启动的次数有限，并且最后一次重启后执行的运行的观测属于V。

注意到，这类策略是否存在并不明确。对于安全性质而言，很容易找到这样的策略，因为运行违反性质这一事实可以由一个有限前缀[1]，见证；但对于活性性质，一般不存在这样的前缀。我们证明，对每个 ω-正则语言 V，这类策略都存在。此外，这些策略只需维护一定数量的计数器，其数量仅取决于 V，而与程序无关。因此，为了按照 σ 重启 P，只需使用与当前序列长度的对数成正比的内存。

[1]可以为 σ 选择如下策略：“第 n 次重启后，执行 n 步；如果这次有限执行不是见证，则重启；否则永远继续执行。”事实上，如果最短见证的长度为 k，那么对于每个 $n \geq k$，在第 n 次重启后，该策略以正概率执行一个见证，因此最终以概率 1 执行一个见证。

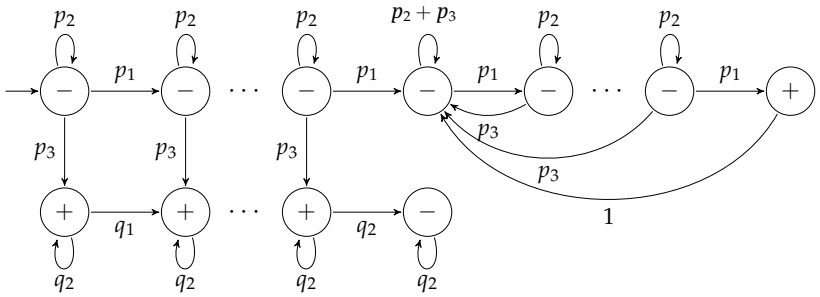

图 1：一个部分可观测马尔可夫链族

例子1.1. 为了初步说明为什么活性性质也存在这类策略，考虑 $\Sigma = \{+, -\}$ 上的性质：变量 x 只有有限多次取正值。违反该性质的运行，是那些无限次访问 $+$-状态的运行。我们的结果表明，以下策略可用于检测违反该性质的运行（以及其他情况）：

> 第n次重启后，反复执行由 $2n$ 步组成的块。如果在执行完第一个块后的某个时刻，迄今执行的块的拼接结果的后半段只包含负状态，则重启。

例如，假设已经重启了 4 次。那么该策略会反复执行由 8 步组成的块。如果执行完这些块中的第 1、2、3.....个块后，最后的 4、8、16.....个状态均为负状态，则该策略会进行第 5 次重启。如果这种情况从未发生，那么重启次数就只有 4 次。图 1 展示了一个马尔可夫链族，朴素策略对其不起作用，但上述策略有效：几乎必然地，重启次数有限，并且最后一次重启后的运行会无限次访问最右侧状态。注意，对于每个$n \geq 0$，该族都存在访问 $+$ 状态至少n 次的执行，也存在每隔至多n 步访问一次 $+$ 状态的执行。

我们还获得了直到最后一次重启的期望时间的渐近最优上界，也就是直到违反该性质的运行开始执行所需时间的上界。这些上界取决于与程序相关联的马尔可夫链的两个参数，分别称为进展半径 和进展概率。我们工作的重要贡献之一，是确定这两个参数是进行分析时的关键参数。

尽管我们的结果是在抽象设定下表述的，但很容易应用于实践。在实际场景中，除了原子命题的取值外，我们还可以观察有用的调试信息，例如某些变量的取值。我们让计算机按照策略，在固定时间t 内运行系统，

σ。如果在t 时，我们观察到上一次重启已经过去很久，那么就停止测试，并返回自上一次重启以来执行的运行，作为该性质可能存在违规的候选。在论文的实验部分，我们利用这一场景检测群体协议中的错误。群体协议是一种分布式计算模型，其状态空间过于庞大，无法通过其他方式找到这些错误。

相关工作。 关于黑盒测试和黑盒检查的文献十分丰富 [12, 15], ，但其底层模型并非概率模型，且这些方法要求已知状态数量的上界。概率模型检测方面的研究假设系统（的模型）是已知的 [2]。此外，还有一些研究通过统计模型检测或统计假设检验，对概率系统进行黑盒验证 [22, 17, 18, 20, 21] （统计模型检测综述另见 [11, 13] ）。这些研究考虑的是不同的问题：我们着重生成反例运行，而黑盒验证的目标是接受或拒绝关于满足某项性质的运行之概率的假设。我们的工作也与运行时强制执行问题 [16, 3, 14, 7, 8], 有关，该问题同样着重识别性质的违例。然而，这些研究要么考虑的不是概率场景，要么只考虑一部分接近安全性质的 ω-正则性质。最后，与我们最接近的论文是 [6], ，它研究的是同一个问题，但对象是完全可观测系统。特别是在最坏情况下， [6] 中提出的策略需要存储一次运行中访问过的完整状态序列，因此它们所需的内存会随当前序列长度线性增长；而我们的策略只需对数内存。

论文结构。 本文的组织如下。第 2 节介绍预备知识。第3节针对具有部分可观测性的任意ω-正则语言引入黑盒测试问题，并说明该问题可以归约为规范语言（称为 Rabin 语言）的问题。第 4 节介绍我们针对 Rabin 语言的黑盒策略，并证明这些策略的正确性。第 5 节给出达到最后一次重启所需时间的渐近最优上界。第 6 节报告一些实验结果。

2. 预备知识

有向图。有向图是一个二元组 $G = (V, E)$，其中 V 是节点集合，$E \subseteq V \times V$ 是边集合。图 G 的路径（无限路径）是由节点组成的有限（无限）序列 $\pi = v_0, v_1, \ldots\ldots$，满足对于每个 $i = 0, 1, \ldots\ldots, (v_i, v_{i+1}) \in E$。一条只包含一个节点的路径是空的。给定两个顶点 v、$v' \in V$，从 v 到 v' 的距离是从 v 到 v'的最短路径长度，而从 v 到集合 $V' \subseteq V$ 的距离，则是对所有 $v' \in V'$ 取从 v 到 v'的距离的最小值。

如果对于任意两个顶点v、v' ，都存在一条从

v 到 v′ 的路径，则图 G 是强连通的。若图 $G' = (V', E')$ 是 G 的子图，记作 $G' \preceq G$，则 $V' \subseteq V$ 且 $E' \subseteq E \cap (V' \times V')$；若 $G' \preceq G$ 且 $G' \neq G$，则记作 $G' \prec G$。若图 $G' \preceq G$ 是 G 的强连通分量 (SCC)，则它是强连通的，并且不存在满足 $G' \prec G'' \preceq G$ 且强连通的图 G''。若 G 的强连通分量 $G' = (V', E')$ 满足：对于任意 $v \in V'$，若 $(v, v') \in E$，则 $v' \in V'$，那么它就是底层强连通分量 (BSCC)。

部分可观测马尔可夫链。固定一个有限的 Σ 观测集合。部分可观测马尔可夫链 是一个元组 $\mathcal{M} = (S, s_{in}, \Sigma, Obs, \mathbf{P})$，其中

- Σ 是一个观测集合；
- S 是有限的状态集合，且$s_{属于} \in S$ 是初始状态；
- $Obs: S \to \Sigma$ 是一个观测函数，为每个状态指定一个观测；并且
- $\mathbf{P} : S \times S \to [0,1]$ 是转移概率矩阵，使得对于每个$s \in S$，都有 $\sum_{s' \in S} \mathbf{P}(s,s') = 1$,

直观来说，Obs(s)描述链访问 s 时我们能够观测到的信息。例如，如果 s 是程序的状态，由程序计数器的值和所有变量的值组成，那么 Obs(s) 可以仅包含程序计数器的值，或某个公共变量子集的值。$\mathcal{M}$ 的图以 S 为节点集合，以 $\{(s, s') \mid P(s, s') > 0\}$ 为边集合。稍微滥用一下语言，我们也用 $\mathcal{M}$ 表示 $\mathcal{M}$的图。$\mathcal{M}$ 的一次运行是 $\mathcal{M}$的一条无限路径 $\rho = s_0 s_1 \cdots$；我们令 $\rho[i]$ 表示状态 s_i。序列 $Obs(\rho) := Obs(s_0)Obs(s_1)\cdots$是与 ρ关联的观测。$\mathcal{M}$ 中的每条路径 π 都确定了运行集合 $Cone(\pi)$，该集合由所有以 π开头的运行组成。我们为 $\mathcal{M}$ 赋予概率空间 $(Runs, \mathcal{F}, \mathbb{P})$，其中 Runs 是 $\mathcal{M}$中所有运行的集合，$\mathcal{F}$是由所有 $Cone(\pi)$生成的 σ-代数，而 $\mathbb{P}$ 是唯一的概率测度，满足$\mathbb{P}[Cone(s_0 s_1 \cdots s_k)] = \mu(s_0) \cdot \prod_{i=1}^{k} P(s_{i-1}, s_i)$，其中空积等于 1。随机变量 $f : Runs \to \mathbb{R}$ 的期望值为 $\mathbb{E}[f] = \int_{Runs} f \, d\, \mathbb{P}$。

部分可观测马尔可夫决策过程。一个 Σ-可观测马尔可夫决策过程（Σ-MDP）是一个元组 $M = (S, s_{in}, \Sigma, Obs, A, \Delta)$，其中 S、$s_{in}$、Σ、Obs 的定义与马尔可夫链中的相同，A 是一个有限的动作集合，而 $\Delta: S \times A \to \mathcal{D}(S)$ 是一个转移函数，对于每个状态 s 和动作 $a \in A(s)$，都会给出后继状态上的一个概率分布。该分布中状态 s′ 的概率记为Δ(s, a, s′)。

策略。对于以 A 为动作集合的 Σ-MDP，策略是一个函数 $\sigma: (\Sigma \times A)^* \Sigma \to A$；给定一条有限路径 $\pi = \ell_0 a_0 \ell_1 a_1 \ldots a_{n-1} \ell_n \in (\Sigma \times A)^* \Sigma$，该函数会给出下一步要采取的动作 $\sigma(\pi) \in A$。请注意，σ 只“观察”Obs(s)，而不是状态 s 本身。因此，它可以应用于任意 Σ-MDP $M = (S, s_{in}, \Sigma, Obs, A, \Delta)$,

从而得到如下定义的马尔可夫链 $M^\sigma = (S^\sigma, s_{in}, \Sigma, Obs, A, P^\sigma)$：$S^\sigma = (S \times A)^* \times S$；对于 M 中以 M 的某个状态 $s \in S$ 结尾的每个状态 $\pi \in S^\sigma$，后继分布定义为 $P^\sigma(\pi, \pi\, a\, s') := \Delta(s, a, s')$（如果 $\sigma(\pi) = a$），否则为 0。

3. 黑盒测试问题

固定一个观测集合 Σ，令 r、c（分别表示重启和继续）为两个动作。对于一个 Σ-可观测马尔可夫链 $\mathcal{M} = (S, s_{in}, \Sigma, Obs, P)$，我们关联一个重启 MDP $M_r = (S, s_{in}, Obs, \{r, c\}, \Delta)$，其中对于任意两个状态 s、$s' \in S$，转移函数定义如下：$\Delta(s, r, s') = 1$ 当 $s' = s_{in}$ 时成立，否则为 0；而 $\Delta(s, c, s') = P(s, s')$。直观地说，在 M_r 的每个状态，我们都可以选择重启链 $\mathcal{M}$或继续运行。

我们考虑 Σ 和 $\{r, c\}$上的黑盒策略。注意，如果 M_r^σ的一次运行 π 中 r 只出现有限次，那么在最后一次出现 r 之后，π 的尾部就是 $\mathcal{M}$ 的一次运行（去掉继续动作 c 的出现后）。更准确地说，如果 $\pi = \pi_0\pi'$，其中 π' 是 π 中不含 r 的最长尾部，那么$\pi' = (\pi_0\, s_{in})\, (\pi_0\, s_{in}\, c\, s_1)\, (\pi_0\, s_{in}\, c\, s_1\, c\, s_2) \ldots$，其中 $s_{in}s_1s_2\ldots$ 是 $\mathcal{M}$的一次运行。$s_{in}s_1s_2\ldots$ 的观测序列是 Σ上的一个无限词，称为 π的尾部；形式上，$tail(\pi) := Obs(s_{in})Obs(s_1)Obs(s_2)\cdots$。

定义 3.1（黑盒测试策略）。设 $L \subseteq \Sigma^\omega$ 是一个 ω-正则语言。若针对 L 的测试策略 σ 满足以下性质，则称其为关于 Σ 和 $\{r,c\}$ 的黑盒策略：对于每个 Σ-可观测马尔可夫链 $\mathcal{M}$，若 $Pr_{\mathcal{M}}(L) > 0$，则以概率 1，M_r^σ 的一次运行只会重启有限次，且其尾部属于L。针对L 的黑盒测试问题 是指寻找一个针对L的黑盒测试策略。

我们用 $\#r(\rho) \in \mathbb{N} \cup \{\infty\}$ 表示 ρ中重启动作 r 出现的次数。直观而言，语言L刻画了给定活性规范可能出现的违例集合。如果我们按照针对L的测试策略，对任意有限状态 Σ-可观测马尔可夫链 $\mathcal{M}$进行采样，那么以概率 1，我们最终会停止重启，并且运行的尾部是一个违例；或者不存在违例。

3.1. 规范黑盒测试问题

利用标准的自动机理论技术，任意 ω-正则语言 L 的黑盒测试问题都可以归约为规范语言的黑盒测试问题。为此，我们需要介绍一些无限词自动机理论中的标准概念。

字母表为 Σ 上的确定性 Rabin 自动机（DRA）是一个元组 $\mathcal{A} = (Q, \Sigma, \gamma, q_0, Acc)$，其中 Q 是有限状态集，$\gamma: Q \times \Sigma \to Q$ 是转移

函数，$q_0 \in Q$ 是初始状态，而 $Acc \subseteq 2^Q \times 2^Q$ 是接受条件。Acc 中的元素称为 Rabin 对。词 $w = a_0a_1a_2\ldots \in \Sigma^\omega$ 若满足以下条件，则称其被 $\mathcal{A}$ 接受： $\mathcal{A}$ 在 w 上的唯一运行 $q_0q_1q_2\ldots$ 满足如下条件：存在一个 Rabin 对 $(E, F) \in Acc$，使得对于无穷多个 i，$a_i \in E \in \mathbb{N}$，且对于有限多个 i，$a_i \in F \in \mathbb{N}$。众所周知，确定性 Rabin 自动机恰好识别 ω-正则语言（例如参见 [2]）。 ω-正则语言 L 的 Rabin 指数，是识别 L 的确定性 Rabin 自动机所需的 Rabin 对的最小数量。

定义 3.2. 设 $k \geq 1$，并设 $M_k = \{e_1, \ldots, e_k, f_1, \ldots, f_k\}$ 为一个标记集合。Rabin 语言 $\mathcal{R}_k \subseteq (2^{M_k})^\omega$ 是满足以下性质的所有词 $w = \alpha_0\alpha_1 \cdots \in (2^{M_k})^\omega$ 组成的语言：存在 $1 \leq j \leq k$，使得对于无穷多个 $i \geq 0$，$e_j \in \alpha_i$ 成立；并且对于至多有限多个 $i \geq 0$，$f_j \in \alpha_i$ 成立。

我们证明，Rabin 指数小于k 的语言的黑盒测试问题可以归约为针对 $\mathcal{R}_k$ 的黑盒测试问题。

引理 3.3. 存在一种算法，给定一个索引为 k 的 ω-正则语言 $L \subseteq \Sigma^\omega$ 以及针对 $\mathcal{R}_k$ 的测试策略 σ_k，即可有效地构造出针对 L 的测试策略 σ_L。

证明。（概要，完整证明见附录。）设 $\mathcal{A} = (Q, \Sigma, \gamma, q_0, Acc)$ 是一个识别 $L \subseteq \Sigma^\omega$ 的确定性 Rabin 自动机，其接受条件为 $Acc = \{(E_1, F_1), \ldots, (E_k, F_k)\}$，即$Acc$ 包含k 个 Rabin 对。设 σ_k 是针对 Rabin 语言$\mathcal{R}_k$的黑盒策略。我们构造一个针对L的黑盒策略 σ_L。

令 $w = \ell_1a_1\ell_2 \cdots \ell_{n-1}a_n\ell_n \in (\Sigma \times \{r, c\})^*\Sigma$。我们如下定义动作 $\sigma_L(w)$。令 $q_0q_1 \ldots q_n$ 为 $\mathcal{A}$ 在词 $\ell_1\ell_2 \ldots \ell_n \in \Sigma^*$ 上的唯一运行。将 $v = \ell'_1a_1\ell'_2 \cdots \ell'_{n-1}a_n\ell'_n \in (2^{M_k} \times \{r, c\})^*2^{M_k}$ 定义为如下给出的词：若 $q_i \in E_j$，则为 $e_j \in \ell'_i$；若 $q_i \in F_j$，则为 $f_j \in \ell'_i$。（直观地说，我们用 e_j 标记运行中 DRA 访问 E_j 的位置，用 f_j 标记 DRA 访问 F_j 的位置。）我们令 $\sigma_L(w) := \sigma_k(v)$。我们在附录中证明，$\sigma_L$ 是 L 的黑盒策略。 □

4. Rabin 语言的黑盒策略

我们介绍一类用于 Rabin 语言 $\{\mathcal{R}_k \mid k \geq 1\}$ 的测试策略。我们将在第 4.1 节详细介绍该策略。在第 4.2 节中，我们引入进展半径和进展概率这两个链的参数，它们是证明正确性所需的参数，也是第 5 节进行定量分析所必需的参数。在第 4.3 节中，我们将形式化地证明该策略有效。

4.1. 策略

设 $\mathcal{M}$ 是一个观测取自 2^{M_k} 的马尔可夫链，并设 $\pi = s_0 s_1 s_2 \cdots s_m$ 是 $\mathcal{M}$ 的一条有限路径。其长度为 m，最后状态记作 last(π)，为 s_m。π 的后半段是路径 SecondHalf(π) $:= s_{\lceil m/2 \rceil} \ldots s_m$。将 π 与 $\mathcal{M}$ 的一条有限路径 $\rho = r_0 r_1 \cdots r_l$ 拼接，其中 $s_m = r_0$，所得路径为 $\pi \odot \rho := s_0 s_1 s_2 \cdots s_m r_1 \cdots r_l$。若路径 π 的长度为 0，或存在标记 e_i、$f_i \in M_k$，使得 π 中某个状态 s 满足 $e_i \in$ Obs(s)，且 π 中没有状态 s 满足 $f_i \in$Obs(s)，则称 π 为 i-良好。此外，若 π 对某个 $1 \leq i \leq k$ 是 i-良好的，则称其为良好。

图 2 中描述的策略 $\mathfrak{S}[f]$，由函数 $f\colon \mathbb{N} \to \mathbb{N}$参数化。对 f的唯一要求是 $\limsup_{n\to\infty} f(n) = \infty$。换言之，在第 n 次

$n := 0$ ▷ 重新启动次数**当**
真时$\pi \leftarrow s_{in}$ ▷ 链的初始状态**当后**半段
(π) 是好的**时**从状态$last(\pi)$采样一条长度为 $2 \cdot f(n)$ ▷ 的路径，
为方便起见取偶数长度$\pi \leftarrow \pi \odot \rho$**结束当**▷ 重启$n \leftarrow n + 1$**结束当**

图 2：用于 Rabin 语言 $\mathcal{R}_k$及函数 $f\colon \mathbb{N} \to \mathbb{N}$的策略 $\mathfrak{S}[f]$。

重启后，该策略持续以 $2 \cdot f(n)$ 步数为一块进行采样，直到目前为止所采样完整路径的后半段 是不好的，此时它会重启。例如，在第 n 次重启后，该策略采样一个块 $\pi_0 = \pi_{01} \odot \pi_{02}$，其中$|\pi_{01}| = |\pi_{02}| = f(n)$，并检查 π_{02} 是否是好的；若不是，则重启；否则，它从 $last(\pi_{02})$开始采样一个块 $\pi_1 = \pi_{11} \odot \pi_{12}$，并检查$\pi_{11} \odot \pi_{12}$ 是否是好的；若不是，则重启；若是，则从 $last(\pi_{12})$开始采样一个块 $\pi_2 = \pi_{21} \odot \pi_{22}$，并检查 $\pi_{12} \odot \pi_{21} \odot \pi_{22}$ 是否是好的，依此类推。直观而言，随着重新启动次数增加，f 的增长控制着该策略如何在链中的深度运行与快速重启之间确定优先级。

在本文余下部分，我们将证明策略的正确性，并给出达到最后一次重置所需步数的最优上界。这些上界以链的两个参数表示：进展半径和进展概率。我们将在第 4.2 节介绍这两个参数。

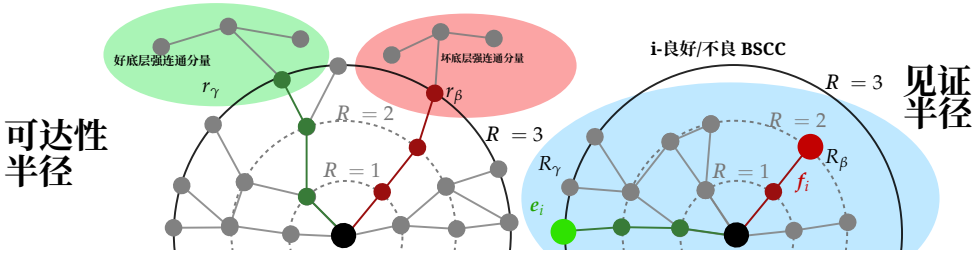

图3：左图：直观而言，r_γ 和r_β 表示到达某个底层强连通分量的难度上界。右图：R_γ 和R_β 衡量在底层强连通分量内到达标签为e_i/f_i 的状态的难度

4.2. 进展半径与进展概率

我们为马尔可夫链 $\mathcal{M}$ （其观测集合为 2^{M_k}，且满足 $\Pr(\mathcal{R}_k) > 0$）定义进展半径和进展概率的概念。直观来说，进展半径是这样一个最小步数：对于链中的任意状态，只执行这么多步，就能朝着产生良好运行或不良运行“取得进展”。进展概率则给出取得进展的路径概率下界。

我们仅针对$k = 1$的情形定义这些概念，这已涵盖所有重要特征。对于任意k的情形，定义更加技术化，详见附录B。

良好运行与好底层强连通分量。 我们将良好路径的定义扩展到马尔可夫链的良好运行和好底层强连通分量。若运行 $\rho = s_0 s_1 s_2 \ldots$ 中e_1 出现无穷多次，而f_1 仅出现有限次，则该运行是良好的；否则为不良的。因此，运行 ρ 是良好的，当且仅当存在一种将 ρ 分解为无限串接 $\rho := \pi_0 \odot \pi_1 \odot \pi_2 \odot \cdots$ 的方法，其中各路径均非空，且 π_1、π_2等都是良好路径。我们用P^{good} 表示 $\mathcal{M}$的良好运行的概率。

$\mathcal{M}$ 的底层强连通分量如果至少包含一个标记为e_1 的状态，且不包含任何标记为f_1, 的状态，则称为好底层强连通分量；否则称为坏底层强连通分量。众所周知，任意有限状态马尔可夫链的运行都会以概率 1 到达某个底层强连通分量，并以概率 1 无限次访问其中的所有状态（定理 10.1 [2, 27]）。因此，良好运行最终会以概率 1 到达好底层强连通分量，而不良运行最终会以概率 1 到达坏底层强连通分量。

进展半径。 直观地说，进展半径R_m 是满足以下条件的最小步数：对于任意状态s，执行 R_m 步后，都可以朝着产生良好运行的方向“取得进展”——到达一个好底层强连通分量，或者如果已经处于其中，则到达一个观测为e_1 的状态——或者产生不良运行。

定义4.1 （良好可达性与良好见证半径）。 设B_γ 为 $\mathcal{M}$ 中属于好底层强连通分量的状态集合，并设S_γ 为可以到达B_γ 的状态集合，其中

可以到达$B\gamma$，并设$s \in S\gamma$。从s 出发的非空路径 π 称为良好进展路径，如果

- $s \in S_\gamma \setminus B\gamma$，并且 π 以 $B\gamma$中的一个状态结束；或者
- $s \in B\gamma$，并且 π 以观测值为 $\boldsymbol{e}1$ 的状态结束。

良好可达半径 $\boldsymbol{r}\gamma$ 是对每个 $s \in S_\gamma \setminus B\gamma$取最短进展路径长度的最大值，其中进展路径针对 s。良好见证半径 $\boldsymbol{R}\gamma$ 的定义相同，但最大值是对每个 $s \in B\gamma$取的。

坏可达半径和坏见证半径分别记为 $r\beta$ 和 $R\beta$ ，其定义类似。只需调整状态$s \in B\beta$ 的进展路径概念。粗略地说，一个坏底层强连通分量要么不包含观测值为 $\boldsymbol{e}_1$, 的状态，要么包含某个观测值为 $\boldsymbol{f}_1$的状态。因此，如果s 所在的底层强连通分量中没有状态的观测值为 $\boldsymbol{e}_1$, ，那么任何以 s 为起点的非空路径都是进展路径；否则，s 的进展路径是以 s 为起点、以观测值为 $\boldsymbol{f}_1$的状态为终点的非空路径。我们在图3中说明可达半径和见证半径的定义。如果链中不包含坏底层强连通分量，因此运行以概率1为好，则不定义 $r\beta$、$R\beta$、$p\beta$和 $P\beta$ 。

定义 4.2 （进展半径）。 进展半径 R_{m} 是 $\mathcal{M}$ 的$r\gamma$、$R\gamma$、$r\beta$和$R\beta$中的最大值。

进展概率。 从马尔可夫链的任意状态出发，都可以通过执行一条长度为R_{m}的进展路径来“取得进展”。然而，这类路径的概率因状态而异。直观而言，进展概率给出了取得进展概率的下界。

定义 4.3。令 $\mathrm{B}\gamma$ 为 $\mathcal{M}$ 中属于好底层强连通分量的状态集合，令 $\mathrm{S}\gamma$ 为能够到达 $\mathrm{B}\gamma$的状态集合，并令 $\mathrm{s} \in \mathrm{S}\gamma$。良可达概率 $\mathrm{p}\gamma$ 是对每个 $\mathrm{s} \in \mathrm{S}_\gamma \setminus \mathrm{B}\gamma$取最小值，即从 s 出发、长度为 $\mathrm{r}\gamma$ 的路径包含一条良好进展路径的概率。良好见证概率 $\mathrm{P}\gamma$ 的定义相同，但取最小值时遍历每个 $\mathrm{s} \in \mathrm{B}\gamma$ ，且路径长度为 $\mathrm{R}\gamma$。相应的坏概率可类似定义。进展概率 $\mathrm{P_m}$ 是 $\mathrm{p}\gamma$、$\mathrm{P}\gamma$、$\mathrm{p}\beta$和 $\mathrm{P}\beta$中的最小值。

4.3. 正确性证明

我们证明，第 4.1 节的策略 $\mathfrak{S}[f]$ 对于任意马尔可夫链 $\mathcal{M}$都是有效的测试策略 $\mathfrak{S}[f]$。首先，我们将给出 $\mathfrak{S}[f]$ “错误地”重新启动的概率上界，也就是说，在状态 $s \in S\gamma$ 处重新启动，而从该状态仍有可能到达某个好底层强连通分量。

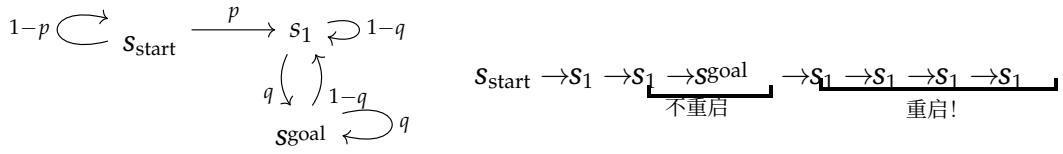

图 4：一个马尔可夫链（左图），以及其一次运行的（有限前缀），其中 $n = 2$和 $f(n) = n$ （右图）。经过 2 步后，运行到达了一个好底层强连通分量 $\mathcal{B}$。经过 4 步后， σ 检查是否重启，但由于第 4 步处的 s^{goal} 而决定不重启。经过 8 步后，它再次检查，这次重启。根据分类讨论的第三种情况，这次重启属于该情况，其中 $k = 4$。运行必定在第 4 步访问过 s^{goal} ，否则最小的 k 将为 3 或更小。

引理 4.4. 设 $\mathcal{M}$ 为一条马尔可夫链，并设 $\mathsf{M}^{\mathfrak{S}[f]}_{\mathsf{r}}$ 为其关联的马尔可夫链，其中 $\mathfrak{S}[f]$ 是重启策略。设 NB_n 为 $\mathsf{M}^{\mathfrak{S}[f]}_{\mathsf{r}}$ 的路径集合，这些路径至少经历 $n-1$ 次重启，并且在第 $(n-1)$ 次重启后只访问 S^γ 中的状态。则有：

$$\Pr[\#\mathsf{r} \geq n \mid NB_n] \leq 3(1-P_{\mathrm{m}})^{\lfloor f(n)/R_{\mathrm{m}} \rfloor - 1}$$

该引理的技术性证明见附录。这里我们给出一个能够说明大部分思想的特殊情形的证明。考虑图 4 顶部所示的、带有 $2^{\{e_1,f_1\}}$ 标签的马尔可夫链。对于状态 s^{goal}，标记函数为 $\mathsf{Obs}(\mathsf{s}^{\text{goal}}) = \{\mathsf{e}_1\}$ ；对于其他所有状态，$\mathsf{Obs}(\mathsf{s}) = \emptyset$ ；并且，当且仅当 ρ 无限次访问 s^{goal} 时，$\mathsf{Obs}(\rho) \in \mathcal{R}_1$ 。集合 S^γ 包含所有状态，因为从每个状态都可以到达 s^{goal} 。唯一的底层强连通分量是 $\mathcal{B} = \{\mathsf{s}_1, \mathsf{s}_{\text{goal}}\}$，并且它是一个好底层强连通分量。根据参数的定义，我们得到 $\mathsf{r}^\gamma = \mathsf{R}_\gamma = 1$、$\mathsf{p}^\gamma = \mathsf{p}$ 和 $\mathsf{P}^\gamma = \mathsf{q}$。此外，由于不存在坏底强连通分量，$\mathsf{r}^\beta$ 和 R^β 未定义，因此 $\mathsf{R}_{\mathrm{m}} = 1$。所以，对于该马尔可夫链，引理 4.4 表明 $\Pr[\#\mathsf{r} \geq \mathsf{n} \mid \mathsf{NB}_n] \leq 3(1-\mathsf{P}_{\mathrm{m}})^{f(\mathsf{n})-1}$。下面来看看其中的原因。

令 ρ 为 $\mathsf{M}^{\mathfrak{S}[f]}_{\mathsf{r}}$ 的一条运行，使得 $\#\mathsf{r}(\rho) \geq n$，即 ρ 至少有 n 次重启。由于 S^γ 包含所有状态，因此 $\rho \in NB_n$ 当且仅当 $\#\mathsf{r}(\rho) \geq n-1$。我们考虑三种情况。在定义这些情况时，我们从第 $(n-1)$ 次重启后立即开始计步，并将 $\rho[a,b]$ 定义为 ρ 的片段：该片段从第 a 步之前立即开始，到第 b 步之后立即结束。

(a) 经过 $f(n)$ 步后， ρ 尚未到达 $\mathcal{B}$。于是， ρ 已在 s_{start} 中连续停留了 $f(n)$ 步；由于 $p = p^\gamma$，这种情况发生的概率至多为 $(1-p^\gamma)^{f(n)}$。(b) 经过 $f(n)$ 步后， ρ 已经到达 $\mathcal{B}$。此外，第 n 次重启恰好发生在第 $2f(n)$ 步之后。

在这种情况下，根据策略的定义， ρ 在区间 $\rho[\mathrm{f(n)}+1, 2\mathrm{f(n)}]$（即 $[0, 2\,\mathrm{f(n)}]$的后半段）内不会访问 $\mathrm{s}^{\mathrm{goal}}$。因此， ρ在区间 $\rho[\mathrm{f(n)}+1, 2\,\mathrm{f(n)}]$ 内停留在 s_1；由于 ρ在第 f(n) 步时已经到达 $\mathcal{B}$，这种情况发生的概率为 $(1-\mathrm{P}\gamma)^{f}(\mathrm{n})$。

(c) 经过$f(n)$ 步后， ρ 已经到达了 $\mathcal{B}$。此外，第n次重启不会早于第 $2f(n)+1$步发生。

由于第 n 次重启会在某个时刻发生，且不会早于第 2 f (n) +1步，根据策略的定义，存在最小的数 $\mathrm{k} \geq \mathrm{f(n)}$，使得 ρ 在区间 $\rho[\mathrm{k}+1, 2\mathrm{k}]$内不会访问 $\mathrm{s}^{\mathrm{goal}}$。因为我们假设第 n 次重启发生在第 2 f (n) 步之后，所以 $\mathrm{k} > \mathrm{f(n)}$。根据 k 的最小性，运行 ρ 会在区间 $\rho[\mathrm{k}, 2\mathrm{k}-2]$内访问 $\mathrm{s}^{\mathrm{goal}}$。因此， ρ在第 k 步移动到 s^{goal}，然后在 s_1 停留 k 步。最终移动到 s^{goal}，随后在 s_1 停留 k 步的运行的概率为 $\mathrm{P}\gamma(1-\mathrm{P}\gamma)^{k}$。

图 4 底部展示了一个运行示例，以及策略如何处理该运行。由于 (a)-(c) 是互斥事件，$\Pr[\#\mathrm{r} \geq n \mid NB_n]$ 有一个上界，即这些事件的概率之和，其中在情形 (c) 下，我们对k的所有可能取值求和。由此可得：

$$Pr[\#\mathrm{r} \geq n \mid NB_n] \leq (1-p_\gamma)^{f(n)} + (1-P_\gamma)^{f(n)} + \sum_{k=f(n)+1}^{\infty} P_\gamma(1-P_\gamma)^k \leq 3(1-P_{\mathrm{m}})^{f(n)}.$$

附录中针对任意马尔可夫链给出的证明具有相同的结构，尤其是同样将情况划分为三个不同的事件。应用引理 4.4，我们现在可以轻松得到（详细证明见附录）：第 n 次重启的概率上界。请注意，此上界涵盖了“正确”和“错误”的重启：

引理 4.5 (重启概率). 设 $\mathcal{M}$ 是一个马尔可夫链，且$\mathrm{M}^{\mathfrak{S}[f]}_{\mathrm{r}}$是其关联的马尔可夫链，其中 $\mathfrak{S}[f]$ 为其重启策略。在 $n-1$ 次重启后再次发生重启的运行概率满足：

$$\Pr[\#\mathrm{r} \geq n \mid \#\mathrm{r} \geq n-1] \leq 1 - P_{good}\left(1 - 3(1-P_{\mathrm{m}})^{\lfloor f(n)/R_{\mathrm{m}} \rfloor - 1}\right)$$

证明。 令NB_n为 $\mathrm{M}^{\mathfrak{S}[f]}_{\mathrm{r}}$中至少重启$n-1$次，且在第$(n-1)$次重启后仅访问$S\gamma$ 中状态的路径集合，令$\overline{NB_n}$ 为其补集。我们有

$$\begin{aligned}\Pr[\#\mathrm{r} \geq n \mid \#\mathrm{r} \geq n-1] = {} & \Pr[\#\mathrm{r} \geq n \mid NB_n] \cdot \Pr[NB_n \mid \#\mathrm{r} \geq n-1] + \\ & \Pr[\#\mathrm{r} \geq n \mid \overline{NB_n}] \cdot \Pr[\overline{NB_n} \mid \#\mathrm{r} \geq n-1].\end{aligned}$$

应用引理 4.4 和 $\Pr[\#\mathrm{r} \geq n \mid NB_n] \leq \overline{1,}$ 得到

$$\Pr[\#\mathrm{r} \geq n \mid \#\mathrm{r} \geq n-1] \leq \left(3(1-P_{\mathrm{m}})^{\lfloor f(n)/R_{\mathrm{m}} \rfloor - 1}\right) \Pr[NB_n \mid \#\mathrm{r} \geq n-1] + \Pr[\overline{NB}_n \mid \#\mathrm{r} \geq n-1]$$

以概率 1， $\mathcal{M}$ 良好运行只访问 S^{γ} 中的状态，因此 $\Pr[NB_n \mid \#\mathrm{r} \geq n-1] \geq P^{\mathrm{good}}$，从而 $\Pr[NB_n \mid \overline{\#\mathrm{r} \geq n-1}] \leq 1 - P^{\mathrm{good}}$，证明至此完成。 □

最后，我们证明 $\mathfrak{S}[f]$ 是一个正确的测试策略。此外，我们证明条件 $\limsup_{n\to\infty} f(n) = \infty$ 不仅是充分条件，也是必要条件。前述引理给出了重启概率的一个上界；随着$f(n)$增大，该上界会降至 1 以下。如果$f(n)$ 在无穷多个n处高于该阈值，只需证明策略 $\mathfrak{S}[f]$ 会重新启动每个不良运行：

定理 4.6. $\mathfrak{S}[f]$ 是 *Rabin* 语言 $\mathcal{R}_k$ 的测试策略，当且仅当函数 f 满足 $\limsup_{n\to\infty} f(n) = \infty$。

证明。 $(\Rightarrow)$：我们证明其逆否命题。如果 $\limsup_{n\to\infty} f(n) < \infty$，那么存在一个界 b，使得对于每个 $n \geq 0$，都有 $f(n) \leq b$。考虑一条包含 $2b+1$ 个状态的路径所构成的马尔可夫链2^{M_1}，其中最后状态以概率 1 转移到自身；最后状态的标签为 e_1，，且没有状态的标签为 f_1。于是，该链有唯一运行：从路径的初始状态到达最后状态，并永远停留在那里；其观测是一个 $\mathcal{R}_1$ 词，因此 $\Pr(\mathcal{R}_1) = 1$。然而，由于 $2f(n) \leq 2b+1$， $\mathfrak{S}[f]$ 总会在到达最后状态之前重启该链。

$(\Leftarrow)$：根据前述引理，我们可以将经过 $\mathrm{n}-1$ 次重启后的重启概率界定为 $1 - \left(1 - 3(1-\mathrm{P_m})^{\lfloor f(\mathrm{n})/\mathrm{R_m} \rfloor - 1}\right) \mathrm{P^{good}}$。由于 $0 < \mathrm{P_m} \leq 1$ 且 $\mathrm{P_{good}} > 0$，当 $\mathrm{f(n)}$ 足够大时，该值小于 $1 - \mathrm{P^{good}}/2 < 1$。由于 $\limsup_{n\to\infty} \mathrm{f(n)} = \infty$，对于无穷多个 n，再次重启运行的概率至多为 $1 - \mathrm{P^{good}}/2$，因此，重启总次数以概率 1 有限。不良运行将以概率 1 进入一个坏底层强连通分量 B，随后会无限多次访问由所有对应于 B 的 f_i 构成的集合。因此， $\mathfrak{S}[\mathrm{f}]$ 将重启该运行；而当它不重启时，则到达一个良好运行。

□

5. 定量分析

测试策略的质量由直到最后一次重启所需的期望步数给出，因为这是直到开始执行某个违规所花费的开销。如 [6], 给定一个带标记马尔可夫链 $\mathcal{M}$ 和一个测试策略 σ，我们将到最后一次重启的步数定义为马尔可夫链 $\mathrm{M}_{\mathrm{r}}^{\sigma}$上的随机变量：

定义 5。1 （S（ρ） 和 S_n（ρ））。 设 ρ 为 $\mathrm{M}_{\mathrm{r}}^{\sigma}$的一次运行。我们定义：如果 r 不出现在 ρ中，则S（ρ） 等于 0；如果 r 在 ρ中至少出现一次且仅有限次，则它等于以 r 结尾的 ρ 的最长前缀的长度；否则等于 ∞。此外，对于每个 $n \geq 1$，我们定义 S_n（ρ）：如果 r 在 ρ中出现的次数少于n次，则其等于 0；否则等于从 ρ的第（$n-1$）次出现（或开头）到 r 的第n次出现之间的片段长度。

本节将考察 $\mathbb{E}[S]$ 对函数 $f(n)$ 的依赖关系。事先并不清楚 $f(n)$ 应该增长得快还是慢。考虑这样一种情况：链的所有底层强连通分量，无论好坏，大小都为 1，并且一次运行最终到达好底层强连通分量的概率为 p。此时，策略会不断重启该链，直到某个样本首次到达好底层强连通分量。如果 $f(n)$ 增长得快，那么经过几次重新启动，比如 r 次之后，后续每次运行都以较大概率到达链的某个底层强连通分量，因此预期重新启动次数很少，至多为 $r + (1/p)$。然而，这几次重新启动期间执行的步数很多，因为$f(n)$ 增长得很快；事实上，仅倒数第二次重新启动之后的运行就已经至少执行了 $2f(r + (1/p) - 1)$ 步数。

首先，我们证明对于任意函数 $f(n) \in 2^{\Omega(n)}$， $\mathbb{E}[S] = \infty$ 都成立。

命题 5.2。 设 $f \in 2^{\Omega(n)}$。则存在一个马尔可夫链，使得图 *2* 中的测试策略满足 $\mathbb{E}(S) = \infty$。

证明。设 f 属于 $2^{\Omega(n)}$。则存在某个正整数 k > 0，使得我们有 lim sup good = $1 - 1\ 2^{1/k}$ $\mathbb{E} = \sum_{n=0}^{\infty} \mathbb{E}\ _n \mid \geq -1 \geq -1$ f (n)

$(1/2)^{n/k} > 0$。考虑一个满足 P (/) 的马尔可夫链。则有 (S) (S #r n)P(#r n)。由于只有良好运行不会被重启，我们有 P(#r $\geq$ n -1 | #r $\geq$ n -2) $\geq 1 - \mathrm{P}^{\mathrm{good}}$。出于同样的原因，我们还有 $\mathbb{E}(\mathrm{S}_n \mid \#\mathrm{r} \geq \mathrm{n} - 1) \geq \mathrm{f}(\mathrm{n})(1 - \mathrm{P}^{\mathrm{good}})$。因此

$$\mathbb{E}[S] = \sum_{n=0}^{\infty} \mathbb{E}(S_n \mid \#\mathrm{r} \geq n-1) P(\#\mathrm{r} \geq n-1) \geq \sum_{n=0}^{\infty} f(n)(1 - P_{\mathrm{good}}) \cdot (1 - P_{\mathrm{good}})^n$$

and hence $\mathbb{E}[S] \geq \sum_{n=0}^{\infty} f(n)(1/2)^{n/k} = \infty.$ □

因此（如果我们仅考虑单调函数——这在实践中并不构成限制），只需考虑满足$f(n)$ $f(n) \in \omega(1) \cap 2^{o(n)}$的函数。本节其余部分将研究对应于多项式函数$f(n) = n^c$ （其中$c \in \mathbb{N}_+$）的策略，并得到一个以上界表示的关于参数$R_{\mathrm{m}}/P_{\mathrm{m}}$、$P^{\mathrm{good}}$和$c$的函数。研究次指数但超多项式函数超出了本文的范围。

5.1. 使用 $f(n) = n^c$ 的策略定量分析

我们给出(S) $\mathbb{E}$的上界，即最后一次重启之前的预期总步数。我们的出发点是引理 4.5，它界定了在已经发生$(n-1)$ 次重新启动的情况下，第n次重启发生的概率。当重新启动次数n 较少时，右端的值大于 1，因此该上界没有用处。我们首先求出一个值X，使得重新启动X 次后，右端降至 1 以下。

引理 *5.3.* 设 $X = \sqrt[c]{R_{\mathrm{m}}\,(2+\ln(1/6)/\ln(1-P_{\mathrm{m}}))}$。对于所有 $n \geq X$，当按照n n进行重启时，均有

$$\Pr[\#\mathsf{r} \geq n \mid \#\mathsf{r} \geq n-1] \leq 1 - P_{good}/2$$

当按照 $\mathfrak{S}[n \mapsto n^c]$进行重启时。

证明。由引理 4.5、重启概率随n增大而降低这一事实、X的定义以及一些计算可立即得出。我们回顾引理 4.5 的陈述：

$$\Pr[\#\mathsf{r} \geq n \mid \#\mathsf{r} \geq n-1] \leq 1 - P_{\mathrm{good}}\left(1 - 3(1-P_{\mathrm{m}})^{\lfloor f(n)/R_{\mathrm{m}} \rfloor - 1}\right)$$

代入一个 $\mathrm{n} \geq X$ 即可验证该结论。 □

现在我们尝试为 $\mathbb{E}[S]$ 找到一个上界：根据期望的线性性，我们有$\mathbb{E}[S] = \sum_{i=1}^{\infty} \mathbb{E}[S_n]$。我们将求和分成两部分：对于 $n < X$，以及对于 $n \geq X$。对于$n < X$，我们只需将 $\Pr[\#\mathsf{r} \geq n-1]$ 近似为 1。借助引理 5.3，对于 $n > X$，我们可以得出更多结论：

$$\begin{aligned}\Pr[\#\mathsf{r} \geq n-1] &= \Pr[\#\mathsf{r} \geq n-1 | \#\mathsf{r} \geq n-2] \cdots \Pr[\#\mathsf{r} \geq X+1 | \#\mathsf{r} \geq X] \cdot \Pr[\#\mathsf{r} \geq X] \\ &\leq \prod_{k=\lceil X \rceil}^{n} \Pr[\#\mathsf{r} \geq k | R \geq k-1] \leq \left(1 - P_{\mathrm{good}}/2\right)^{n-X}\end{aligned}$$

由此可得：

$$\begin{aligned}\mathbb{E}[S] &= \sum_{n=0}^{\infty} \mathbb{E}[S_n \mid \#\mathsf{r} \geq n-1] \Pr[\#\mathsf{r} \geq n-1] \\ &\leq \sum_{n=0}^{X} \mathbb{E}[S_n \mid \#\mathsf{r} \geq n-1] + \sum_{n=X}^{\infty} \mathbb{E}[S_n \mid \#\mathsf{r} \geq n-1] \cdot \left(1 - P_{\mathrm{good}}/2\right)^{n-X} \qquad (1)\end{aligned}$$

接下来需要界定两次重新启动之间的期望步数 $\mathbb{E}[S_n \mid \#\mathsf{r} \geq n-1]$，这将在下文的引理 5.4 中完成。证明见附录。证明首先指出，到达一个好底层强连通分量或坏底层强连通分量所需的期望步数分别为 r_γ/p_γ 和 r_β/p_β。然后，我们给出一个界，说明首次在坏底层强连通分量内执行进展路径所需的期望步数，或者在第 $(\mathrm{n} \geq)$ 次重启之后的某个时刻，在好底层强连通分量内连续整个运行的后半段都不执行进展路径所需的期望步数；该界同样以 R/P 和 R/P(P) 表示。

项 $2f(n)$ 源于策略总是至少执行 $2f(n)$ 步。项 $2R_{\mathrm{m}}$ 则是分析粒度造成的结果：我们将运行划分为长度为 R_{m} 步的块。

引理5.4 (片段中的期望步数)。对于策略 $\mathfrak{S}[n \mapsto n^c]$，我们有：

$$\mathbb{E}[S_n \mid \#\mathsf{r} \geq n-1] \leq 2(R_{\mathrm{m}} + f(n)) + 9\left(\frac{R_{\mathrm{m}}}{P_{\mathrm{m}}(1-P_\gamma)}\right). \tag{5.5}$$

将引理 5.4 代入 **(1)**，最终得到（见附录）：

定理5.6 (总步数的期望数量)。对于策略 $\mathfrak{S}[n \mapsto n^c]$，我们有：

$$\mathbb{E}[S] \in \mathcal{O}\left((c+1)! \cdot 2^c \cdot \left(\frac{R_{\mathrm{m}}}{P_{\mathrm{m}}}\right)^{1+1/c} + \frac{2^c(c+1)!}{P_{good}^{c+1}} + (c+1)!(2c)^{c+1}\right).$$

如果固定一个值c，就能得到一个简单得多的结论：

推论5.7。对于固定的 c，策略 $\mathfrak{S}[n \mapsto n^c]$ 满足：

$$\mathbb{E}[S] \in \mathcal{O}\left(\left(\frac{R_{\mathrm{m}}}{P_{\mathrm{m}}}\right)^{1+1/c} + \frac{1}{P_{good}^{c+1}}\right).$$

因此，总步数上界取决于两个量，$R_{\mathrm{m}}/P_{\mathrm{m}}$和$P_{\mathrm{good}}$。较小的$c$ 有利于$R_{\mathrm{m}}/P_{\mathrm{m}}$ 对上界的影响，而较大的c 则有利于P_{good}的影响。在第 6 节中，我们将看到，这与不同 c 取值下算法在合成马尔可夫链以及 PRISM 基准测试集中的马尔可夫链上的表现高度吻合。

5.2. 策略 $f(n) = n^c$ 的最优性

我们将证明以下关于我们策略的最优性保证。

定理 5.8. 对于每个 $c \in \mathbb{N}_+$，都存在一族马尔可夫链，使得推论 *5.7* 中关于 $\mathfrak{S}[n \mapsto n^c]$ 的上界在渐近意义下是最优的，即不存在渐近复杂度类更优的黑盒测试策略。

这证明了两点：第一，我们的界限无法得到实质性改进。第二，要为 c 选取最优值，就必须掌握有关 $R_{\mathrm{m}}P_{\mathrm{m}}$ 和 P_{good} 的信息；如果没有任何信息，那么所有取值都同样理想。

证明。考虑图 5 顶部的马尔可夫链族。任取 $k > 1$，并令 $M = k^{c-1}$，且 $p = q = 1/k$。作此选择后，我们有 $P_{good} = P_m = 1/k$，且 $R_m = k^{c-1}$。根据引理 5.6，策略 $\mathfrak{S}[n \mapsto n^c]$。满足$\mathbb{E}[S] \in \mathcal{O}((R_m/P_m)^{1+1/c} + (1/P_{good})^{c+1}) = \mathcal{O}(k^{c+1})$

我们将其与最后一次重启之前的期望步数最优值进行比较。由于以概率 1，至少访问过一次 s_{goal} 的运行是良好运行，因此任何最优策略都恰好在访问 s_{goal} 后停止重启。我们声称，每个这样的策略都满足 $\mathbb{E}[S] \geq R_m/(P_{good}P_m)(1 - P_{good})$。为此，我们作出四点观察。第一，良好运行的概率为 P_{good}。第二，良好运行首次访问 s_{goal} 之前的期望步数为 R_m/P_m。第三，区分不良运行（即处于左侧底层强连通分量中）与良好运行所需的最少步数等于 R_m，因为在执行 R_m 步之前，所有访问到的状态都带有相同的标签。因此，每个策略在首次到达状态 s_{goal} 之前，平均需要走 $R_m/(P_{good}P_m)$ 步。第四，平均需要尝试 $1/P_{good}$ 次，才能有一次尝试产生良好运行。因此，在最后一次重启之前，平均至少有 $1/P_1^{good-1}/P_{good}$ 的 $R_m/(P_{good}P_m)$ 步已经发生。由于 $1/P_1^{good-1}/P_{good} = (1 - P_{good})$，这就证明了上述断言。现在，~~$R_m/(P_{good}P_m)(1 - P_{good}) = k^{c+1} - k^c \in \Theta(k^{c+1})$，证毕。~~

□

6. 实验

我们报告了对三类系统开展的实验。首先，我们对两个合成系列的马尔可夫链进行了实验。其次，我们使用黑盒策略，在标准 PRISM 基准测试套件 [10] 中的模型上重复了 [6] 的实验。最后，我们对 Peregrine 工具 [4, 5]的基准测试套件中的群体协议进行了实验。

合成实验。考虑图 5 顶部的两个（系列）带标记的马尔可夫链。标签为 a 和 b。在顶部的链中，状态 s_{goal} 被标记为 a，其余状态均标记为 b。在底部的链中，状态 s_2 至 s_M 以及 s_{goal} 被标记为 $\{a, s_{start}\}$ 和 s_{sink} 被标记为 b。语言 L 是包含无限多个 a 的词的集合。在顶部链的初始状态，我们分别以概率 q 和 $(1 - q)$ 向右或向左移动。向左移动的运行是不好的，而向右移动的运行以概率 1 为好的。由此可得 $P_{good} = q$、$R_m = M$ 以及 $P_m = \min(p, q)$。在实验中，我们固定 $q = 1/2$。通过控制 M 和 p，对于固定的 $P_{good} = 1/2$，我们可以获得具有不同 R_m 和 P_m 值的链。在底部链中，$R_\beta = R_\gamma = 1$，$R_m = r_\gamma = M$，$p_\gamma = p^M$，$p_\beta = (1 - p)$，以及 $P_m = \min(p^M, 1 - p)$ 和 $P_{good} = p^M$。

回顾上一节得到的界为 $\mathbb{E}[S] \leq f(c)(R_m/P_m)^{1+1/c} +$

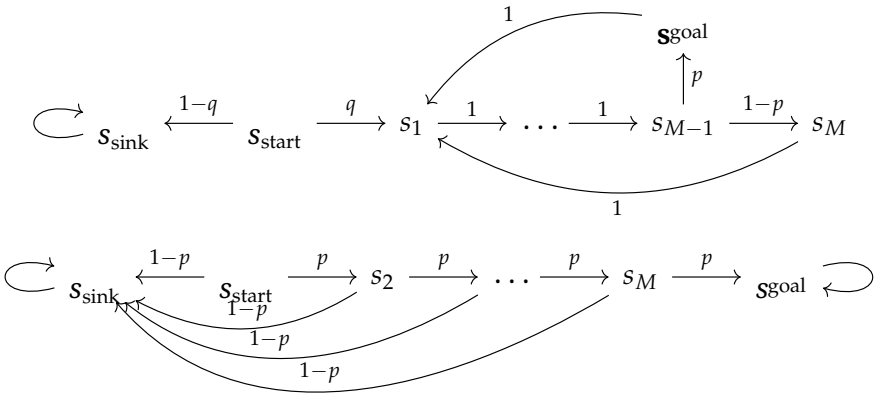

图 5：两类马尔可夫链。初始状态为 s_{start}。良好运行是指无限次访问 s^{goal} 的运行。对于上方链，$P^{\text{good}} = q$、$R_{\text{m}} = M$ 和 $P_{\text{m}} = p$。对于下方链，$P^{\text{good}} = p^M$、$R_{\text{m}} = M$、$P_{\text{m}} = p^M$。

$g(c)(1/P^{good})^{c+1}$，其中 f(c) 和 g(c) 是关于 c 的快速增长函数。如果 P^{good} 和 R_m/P_m 较小，那么 f(c) 和 g(c) 将主导步数，因此 c 较小的策略应表现得更好。数据证实了这一预测。此外，对于固定的 P^{good}，该界预测 $\mathbb{E}[S] \in O((R_m/P_m)^{1+1/c})$，因此随着 R_m/P_m 增大，c 较大的策略应表现得更好。左图证实了这一点。此外，在双对数图中，曲线变成直线，这证实了所预测的多项式增长。最后，当 R_m/P_m 和 $1/P^{good}$ 以与下层马尔可夫链大致相同的速度增长时，该界预测对于 $c = 2, 3$，有 $\mathbb{E}[S] \in O(1/P^{c+1}\ \text{good})$，对于 $c = 1$，有 $\mathbb{E}[S] \in O(M^2/P^{c+1}\ \text{good})$，因此随着 P^{good} 和 R_m/P_m增大，c 较小的策略表现更好。同样，右图证实了这一点。

关于 PRISM 数据集的实验。 我们针对不同的 c 值，在 PRISM 基准测试套件 [10]，中的离散时间马尔可夫链基准上，评估黑盒测试策略的性能，并将其与 [6]针对完全可观测系统的策略进行比较。结果见表1。检查的性质形式为 **GF**、(**GF** $\rightarrow$ **F G**)，或它们的否定形式。我们还添加了一个网格世界示例[2]，记为 GW，并采用较大的参数值，使状态数增加到 $\sim 5 \cdot 10^8$。在尝试构造相应的马尔可夫链时，Storm 遇到了超时。运行样本由 Storm 模型检查器 [9] 的模拟器和 Python 扩展 Stormpy 生成。若运行在 10^6 步后仍未重启，我们便中止该运行。（最多

[2]遗憾的是，[6] 的实验设置无法应用于此示例 [19]。

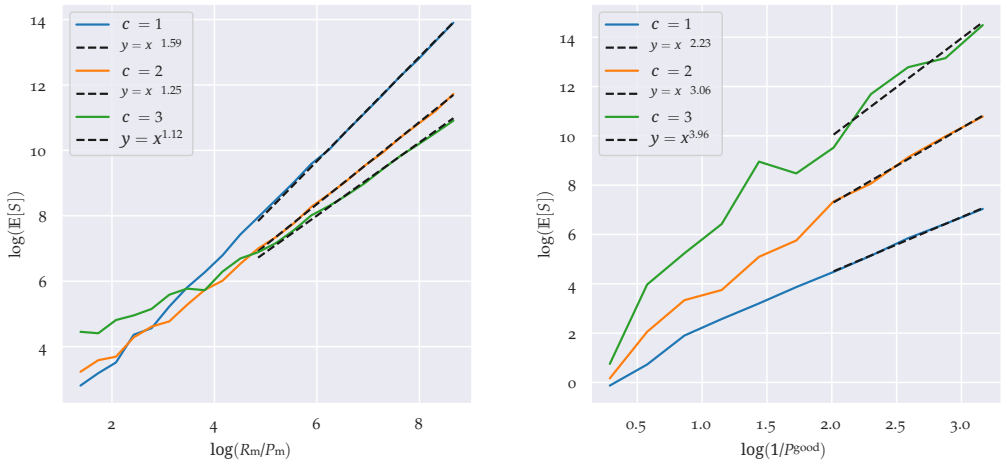

图 6：左图为双对数图，展示了图 5 顶部的链在不同策略 (2) 下，在重启前的预期总步数 $\mathbb{E}(S)$ 随 R_m/P_m 的变化，其中 $f(n) = n^c$，并改变 c。右图展示了底部链的相同关系，以 $1/P_{good}$为变量。图中还显示了线性回归结果。主导指数可从图例中读取。

$3 \cdot 10^7$ 对于网格世界示例 gw、gw 和 GW~~)~~，在未重启的情况下运行 $3 \cdot 10^7$ 步。再次重启的概率可以忽略不计。

[6] 的谨慎$_{10}$策略和激进$_{0.1}$策略会存储所观察到的完整状态序列，因此所需内存随样本长度线性增长。我们的策略最多只需对数级内存，而重启前步数的代价很小，甚至没有代价。我们的策略不会超时，而且令人惊讶的是，所需步数往往少于完全可观测系统的策略。特别是，针对完全可观测系统的策略无法处理网格世界，而只有激进策略能够处理网格世界。造成这种差~~异的一个原~~因是，我们的策略能够自动适应链的大小：随着 n 增长，逐步增大 $f(n)$ 的值。在两种情况下（与非门和蓝牙），完全观测策略的表现好 ~ 2 到 ~ 3倍。相比之下，新提出的黑盒策略相较于白盒策略，在 scale$_{10}$ 中提升了 ~ 50倍，在网格世界中提升了 ~ 90 倍；前者的优势微不足道。

群体协议上的实验。 群体协议是共识协议，其中一群不可区分的智能体决定其初始状态的某个性质

	nand	蓝牙	规模$_{10}$	人群	Herman	gw	$\overline{\texttt{gw}}$	$\overline{\texttt{GW}}$
# 状态	$7{\cdot}10^7$	143 291	121	$1{\cdot}10^7$	$5{\cdot}10^5$	309 327	309 327	$5{\cdot}10^8$
$c = 1$	31 246	4 428	116	**44**	**2**	486	171 219	8 082 659
$c = 2$	18 827	4 548	**75**	61	**1**	404	**152 127**	4 883 449
$c = 3$	32 777	7 615	179	99	**1**	**293**	579 896	**4 252 263**
粗体$_{0.1}$	10 583	4 637	14 528	199	**0**	TO	TO	
谨慎 10	**6 900**	**2 425**	3 670	101	TO	26 361	TO	

表1：最后一次重启前的平均步数，取 300 次运行（Herman 和 GW 为 100 次）的平均值。对于我们的策略$\overline{c}$ $= 1$、2、3，以及 [6]的粗心和谨慎策略，结果如下。

	AvC$_{17,8}$(故障的)		Maj$_{\leq 12}$(故障的)		AvC$_{17,8}$		Maj$_{5,6}$	
$c = 1$	13 645	ce	872	ce	126 294	true	4 264 508	ge
$c = 2$	181 746	ce	4 763	ce	10 485 163	true	11 878 533	ge
Peregrine		TO		ce		TO		true

表 2：使用策略 $\mathfrak{S}[n \mapsto n^c]$ 测试群体协议。实验运行了 100 次，取达到最后一次重启所需步数的平均值；Average and Conquer（AvC）的重启阈值为 250，多数协议的重启阈值为 10000。

通过达到稳定共识 [1, 4]来配置。规范指出，对于每个初始配置，智能体最终都会达到正确的共识（性质成立/不成立）。我们在 Peregrine（群体协议领域最先进的模型检查器）的基准测试套件中的多个协议上测试了我们的策略 [4, 5]。表 2 中的第一个协议存在故障，但 Peregrine 无法证明这一点；我们的策略找到了会导致该协议出现故障的初始配置。对于第二个协议，我们的策略和 Peregrine 都找到了故障配置。第三个协议是正确的；Peregrine 未能证明这一点，而我们的策略也正确地未能找到反例。最后一个协议也是正确的，但共识的期望达到时间只有在经过参数数量呈指数级的步数后才会到来；我们对规范取补，并搜索能够达成共识的一次运行。得益于对数级内存需求，我们的策略可以深入马尔可夫链并找到这样的运行。

7. 结论

我们研究了在黑盒环境中针对 ω-正则规范测试部分可观测随机系统的问题。在这种环境下，测试者只能重启系统，不了解系统规模或概率，也无法观测系统的状态，只能观测其输出。我们证明，尽管存在这些限制，黑盒测试策略依然存在。我们获得了直到最后一次重启为止所需步数的渐近最优界。令人惊讶的是，我们的策略所需步数从不会比针对完全可观测系统的策略多很多 [6]，而且通常还更少。有时，性能提升幅度很大（在我们的实验中最高可达 ~ 90），或者黑盒策略能够解决 [6] 的策略超时的实例。

参考文献

[1] Dana Angluin、James Aspnes、Zoë Diamadi、Michael J. Fischer 和 René Peralta。被动移动有限状态传感器网络中的计算。*DistributedComput.*，18(4):235–253，2006年。[2] Christel Baier 和 Joost-Pieter Katoen。模型检测原理。MIT出版社，马萨诸塞州剑桥，2008年。[3] David A. Basin、Vincent Jugé、Felix Klaedtke 和 Eugen Zalinescu。可强制执行的安全策略再探。*ACMTrans.Inf.Syst.Secur.*，16(1):3:1–3:26，2013年。[4] Michael Blondin、Javier Esparza 和 Stefan Jaax。Peregrine：用于分析群体协议的工具。见 *CAV*（*1*），《计算机科学讲义》第10981卷，第604–611页。Springer，2018年。[5] Javier Esparza、Martin Helfrich、Stefan Jaax 和 Philipp J. Meyer。Peregrine 2.0：通过阶段图解释群体协议的正确性。见 *ATVA*，《计算机科学讲义》第12302卷，第550–556页。Springer，2020年。[6] Javier Esparza、Stefan Kiefer、Jan Kretínský 和 Maximilian Weininger。通过重启在马尔可夫链中强制执行 ω-正则性质。见 *CONCUR*，*LIPIcs*第203卷，第5:1–5:22页。Schloss Dagstuhl - Leibniz-Zentrum für Informatik，2021年。

[7] Yliès Falcone、Laurent Mounier、Jean-Claude Fernandez 和 Jean-Luc Richier。运行时强制监控器：组合、综合和强制能力。*Formal MethodsSyst.Des.*，38(3):223–262，2011年。[8] Yliès Falcone 和 Srinivas Pinisetty。关于定时性质的运行时强制。见 *RV*，《计算机科学讲义》第11757卷，第48–69页。Springer，2019年。[9] Christian Hensel、Sebastian Junges、Joost-Pieter Katoen、Tim Quatmann 和 Matthias Volk。概率模型检测器 Storm。*CoRR*，abs/2002.07080，2020年。[10] Marta Z. Kwiatkowska、Gethin Norman 和 David Parker。PRISM 基准测试套件。见 *QEST*，第203–204页。IEEE计算机学会，2012年。[11] Kim G. Larsen 和 Axel Legay。论统计模型检测的能力。见 *ISoLA*（2），《计算机科学讲义》第9953卷，第843–862页，2016年。[12] David Lee 和 Mihalis Yannakakis。有限状态机测试的原理与方法——综述。*Proc.IEEE*，84(8):1090–1123，1996年。[13] Axel Legay、Benoît Delahaye 和 Saddek Bensalem。统计模型检测：概述。见 *RV*，《计算机科学讲义》第6418卷，第122–135页。Springer，2010年。[14] Jay Ligatti、Lujo Bauer 和 David Walker。非安全策略的运行时强制。*ACM Trans. Inf. Syst.Secur.*，12(3):19:1–19:41，2009年。[15] Doron A. Peled、Moshe Y. Vardi 和 Mihalis Yannakakis。黑盒检测。*J.Autom. Lang. Comb.*，7(2):225–246，2002年。[16] Fred B. Schneider。可强制执行的安全策略。*ACM Trans. Inf.Syst. Secur.*，3(1):30–50，2000年。[17] Koushik Sen、Mahesh Viswanathan 和 Gul Agha。黑盒概率系统的统计模型检测。见*CAV*，第202–215页，2004年。[18] Koushik Sen、Mahesh Viswanathan 和 Gul Agha。关于随机系统的统计模型检测。见 *CAV*，《计算机科学讲义》第3576卷，第266–280页。Springer，2005年。[19] Maximilian Weininger。个人通信，2022年。

[20] Håkan L. S. Younes。《黑箱》系统的概率验证。载于*CAV*，收入《计算机科学讲义》第3576卷，第253–265页。Springer，2005年。

[21] Håkan L. S. Younes、Edmund M. Clarke 和 Paolo Zuliani。利用无界直到对概率性质进行统计验证。载于*SBMF*，收入《计算机科学讲义》第6527卷，第144–160页。Springer，2010年。

[22] Håkan L. S. Younes 和 Reid G. Simmons。使用接受抽样对离散事件系统进行概率验证。载于*CAV*，收入《计算机科学讲义》第2404卷，第223–235页。Springer，2002年。

A. 第3节的证明

引理 3.3. 存在一种算法，给定一个 ω-正则语言 $L \subseteq \Sigma^\omega$，其指标为 k，并给定一个针对 $\mathcal{R}_k$ 的测试策略 σ_k，即可有效地构造出针对 L 的测试策略 σ_L。

证明。设 $\mathcal{A} = (Q, \Sigma, \gamma, q_0, Acc)$ 是一个识别 $L \subseteq \Sigma^\omega$ 的确定性 Rabin 自动机，并假设 $Acc = \{(E_1, F_1), \ldots, (E_k, F_k)\}$。设 σ_k 是 Rabin 语言 $\mathcal{R}_k$ 的黑盒策略。我们构造一个针对 L 的黑盒策略 σ_L。

设 $\mathrm{w} = \ell_1 \mathrm{a}_1 \ell_2 \cdots \ell_{n-1} \mathrm{a}_n \ell_n \in (\Sigma \times \{\mathrm{r}, \mathrm{c}\})^* \Sigma$。我们如下定义动作 $\sigma_L(\mathrm{w})$。设 $\mathrm{q}_0 \mathrm{q}_1 \ldots \mathrm{q}_n$ 是 $\mathcal{A}$ 在词 $\ell_1 \ell_2 \ldots \ell_n \in \Sigma^*$ 上的唯一运行。将 $\mathrm{v} = \ell'_1 \mathrm{a}_1 \ell'_2 \cdots \ell'_{n-1} \mathrm{a}_n \ell'_n \in (2^{M_k} \times \{\mathrm{r}, \mathrm{c}\})^* 2^{M_k}$ 定义为如下词：当 $\mathrm{q}_i \in \mathrm{E}j$ 时为 $\mathrm{e}_j \in \ell'_i$，当 $\mathrm{q}_i \in \mathrm{F}j$ 时为 $\mathrm{f}_j \in \ell'_i$。（直观地说，我们用 $\mathrm{e}j$ 标记运行中确定性 Rabin 自动机访问 $\mathrm{E}j$ 的位置，用 $\mathrm{f}j$ 标记其访问 $\mathrm{F}j$ 的位置。）我们令 $\sigma_L(\mathrm{w}) := \sigma_k(\mathrm{v})$。

我们声称，σ_L 是 L 的黑盒策略。为证明这一点，令 $\mathcal{M} = (S, s_{in}, \Sigma, Obs, \mathbf{P})$ 为一个任意的、标签取自 Σ 的马尔可夫链。将 $\mathcal{M}$ 与 $\mathcal{A}$ 的积定义为带标记马尔可夫链 $\mathcal{M} \otimes \mathcal{A} = (S \times Q, s'_{in}, 2^{M_k}, Obs', \mathbf{P}')$，其中

- $s'_{\text{属于}} = (s_{\text{属于}}, q_0)$；
- $\boldsymbol{e}_j \in Obs'(s, q)$ 当且仅当 $q \in E_j$ 且 $\boldsymbol{f}_j \in Obs'(s, q)$ 当且仅当 $q \in F_j$；
- $\mathbf{P}'((s, q), (s', q')) = \mathbf{P}(s, s')$ 当 $q' = \gamma(q, Obs(s))$ 时成立，否则为 0。

由于 $\mathcal{A}$ 是确定性的，对于 $\mathcal{M}$ 的每个运行 $\pi = \mathrm{s}_{in} \mathrm{s}_1 \mathrm{s}_2 \cdots$，都存在 $\mathcal{M} \otimes \mathcal{A}$ 的唯一运行 $\pi' = (\mathrm{s}_{in}, \mathrm{q}_0)(\mathrm{s}_1, \mathrm{q}_1)(\mathrm{s}_2, \mathrm{q}_2) \cdots$，且将 π' 映射到 π 的映射是一个双射。根据 $\mathcal{A}$ 的接受运行定义，$\mathrm{Obs}(\pi) \in \mathrm{L}$ 当且仅当 $\mathrm{q}_0 \mathrm{q}_1 \mathrm{q}_2 \cdots$ 是 $\mathcal{A}$ 的一个接受运行；根据积的定义，当且仅当 $\mathrm{Obs}'(\pi') \in \mathcal{R}_k$。此外，根据 P' 的定义，我们有 $\Pr_{\mathcal{M}}(\mathrm{L}) = \Pr_{\mathcal{M} \otimes \mathcal{A}}(\mathrm{L}_C)$。

现在考虑马尔可夫链 $\mathrm{M}^{\sigma_k}\mathrm{r}$ 和 $(\mathrm{M} \otimes \mathcal{A})^{\sigma_L}r$。$\mathrm{M}^{\sigma_k}\mathrm{r}$ 的一次运行可以视为一个无限序列 $\Pi = \pi_0 r\ \pi_1 r \cdots$，其中 π_0、π_1、$\cdots$ 是 $\mathcal{M}$ 的路径，表示

$\mathcal{M}$ 在执行 π_0、π_q 等操作后会重启，对于 $(\mathrm{M} \otimes \mathcal{A})^{\sigma_L}{}_r$ 也同理。（我们省略继续操作 c的出现。）我们扩展上述映射，使其将 Π 映射到运行 $\Pi' = \pi'_0 r\ \pi'_0 r\ \cdots$。我们有：$\Pi$ 是 $\mathrm{M}^{\sigma_k}{}_r$ 的一次运行，满足尾部$(\Pi) \in L$，当且仅当 Π' 是 $(\mathrm{M} \otimes \mathcal{A})^{\sigma_L}{}_r$ 的一次运行，满足 尾部$(\Pi') \in \mathcal{R}_k$。此外，由于该运行中的转移概率相同，σ_L 是针对 L 的黑盒策略，命题得证。

□

B. 进展半径和概率的一般定义

现在，我们将重新陈述适用于包含多个 Rabin 对的 Rabin 语言的进展半径和概率定义。它们与第 4.2 节给出的定义仅在一些技术细节上有所不同。为方便起见，我们已将所有差异标出。

良好运行和好底层强连通分量。 我们将好路径的定义扩展到马尔可夫链的良好运行和好底层强连通分量。如果存在一个 Rabin 对 $(\boldsymbol{e}_i, \boldsymbol{f}_i)$，使得$\boldsymbol{e}_i$ 在 ρ 中出现无限多次，而$\boldsymbol{f}_i$ 只出现有限次，则运行 $\rho = s_0 s_1 s_2 \ldots$ 是良好的；否则就是不良的。因此，运行 ρ 是良好的，当且仅当存在一种将 ρ 分解为无限串接 ρ：
$= \pi_0 \odot \pi_1 \odot \pi_2 \odot \cdots$ 的方式，其中每条路径都非空，并且存在一个 $1 \leq i \leq k$，使得 $\pi_1, \pi_2, \ldots$ 都是i-良好的。我们用 P^{good} 表示 $\mathcal{M}$ 的良好运行的概率。

$\mathcal{M}$ 的底层强连通分量是i-良好的，当且仅当它至少包含一个带有标签$\boldsymbol{e}_i$ 的状态，且不包含任何带有标签$\boldsymbol{f}_i$ 的状态。如果某个底层强连通分量对于任何 $1 \leq i \leq k$ 都不是i-良好的，则称它为坏底层强连通分量。

定义 B.1（良好可达性与良好见证半径）**.** 令$B\gamma$ 为 $\mathcal{M}$ 中属于好底层强连通分量的状态集合，令$S\gamma$ 为能够到达$B\gamma$ 的状态集合，并令$s \in S\gamma$。从s 出发的非空路径 π 称为良好进展路径，如果

- $s \in S_\gamma \setminus B\gamma$，且 π 终止于$B\gamma$中的一个状态；或
- $s \in B\gamma$，且 π 终止于观测值为$\boldsymbol{e}_i$ 的状态，并且s 位于一个i-良好的底层强连通分量中。

良好可达半径$\boldsymbol{r}\gamma$ 是对每个$s \in S_\gamma \setminus B\gamma$取最短进展路径长度的最大值。良好见证半径 $\boldsymbol{R}\gamma$ 也是同样的最大值，但取值范围是每个$s \in B\gamma$。

坏可达性半径和坏见证半径，分别记为r^β 和R^β，定义方式类似。只需调整状态$s \in B^\beta$ 的进展路径这一概念。粗略地说，对于每个观测为$\boldsymbol{f}_i$ 的状态，一个坏底层强连通分量中至少包含一个观测为$\boldsymbol{e}_i$的状态。因此，如果s 所在底层强连通分量中没有任何状态具有

观测e_i（对任意i而言），那么任何从s出发的非空路径都是进展路径。否则，s的进展路径是从s出发的一条非空路径，其中对于s所在底层强连通分量中每个观测为e_i的状态，都包含一个观测为f_i的状态。换言之，从坏底层强连通分量B出发的进展路径会访问所有观测为f_i的状态，这些观测阻止B成为好底层强连通分量。注意，—如果链中不包含坏底层强连通分量，我们就不定义坏进展半径和概率，因此运行以概率1为好。

定义 B.2（进展半径）。进展半径 R_{m} 的 $\mathcal{M}$ 是r_γ、R_γ、r_β和R_β中的最大值。

进展概率。进展概率的定义方式与论文正文部分相同。从马尔可夫链的任一状态出发，都可以通过执行长度为R_{m}的进展路径来"取得进展"。然而，这类路径的概率因状态而异。直观而言，进展概率给出了取得进展的概率下界。

定义 B.3。令 B_γ 为 $\mathcal{M}$ 中属于好底层强连通分量的状态集合，令 S_γ 为能够到达 B_γ 的状态集合，并令 $\mathrm{s} \in \mathrm{S}_\gamma$。良可达概率 p_γ 是对每个 $\mathrm{s} \in \mathrm{S}_\gamma \setminus \mathrm{B}_\gamma$取最小值，即从 s 出发、长度为 r_γ 的路径包含良好进展路径的概率的最小值。良好见证概率 P_γ 是相同的最小值，但取遍每个 $\mathrm{s} \in \mathrm{B}_\gamma$，且路径长度为 R_γ。相应的坏概率以类似方式定义。进展概率 P_{m} 是 p_γ、P_γ、p_β和 P_β中的最小值。

C. 第 4 节的证明

本节将给出正文中省略的技术证明。

引理 4.4. 设 $\mathcal{M}$ 为一条马尔可夫链，并设 $\mathsf{M}^{\mathfrak{G}[f]}_{\mathsf{r}}$ 为其关联的马尔可夫链，其中 $\mathfrak{G}[f]$ 为重启策略。设 NB_n 为 $\mathsf{M}^{\mathfrak{G}[f]}_{\mathsf{r}}$ 的路径集合，这些路径至少经历 $n-1$次重新启动，并且在第 $(n-1)$次重启之后只访问 S_γ 中的状态。则有：

$$\Pr[\#\mathsf{r} \geq n \mid NB_n] \leq 3(1-P_{\mathrm{m}})^{\lfloor f(n)/R_{\mathrm{m}} \rfloor - 1}$$

证明。如果 $\lfloor f(n)/R_{\mathrm{m}} \rfloor \leq 1$，则不等式显然成立。因此设 $f(n) \geq 2R_{\mathrm{m}}$。

设 $\rho \in NB_n$。注意到，ρ 最终以概率 1 到达 $\mathcal{M}$ 的一个底层强连通分量；并且由于 ρ只访问 S_γ中的状态，该底层强连通分量是好的。令 B 为这个底层强连通分量。假设 $\#\mathsf{r}(\rho) \geq n$。我们考虑以下情况：从第$(n-1)$次重启之后立即开始计步；对于 $a < b$，路径 $[a, b]$ 是指在第a步之前立即开始，并在第b步之后立即结束的路径。

• 经过 $2f(n)$ 步后， ρ 尚未到达 $\mathcal{B}$。根据$p\gamma$的定义，这种情况发生的概率至多为 $(1-p\gamma)^{f(n)/r\gamma}$。

• 经过 2 f (n) 步后， ρ 已经到达了 $\mathcal{B}$。此外，第 n 次重启发生在路径 [2f (n), 2(f (n) $+$Rγ) $-$ 1]中。在这种情况下，根据 $\mathfrak{S}$[f],的定义，最后一个路径样本的后半部分不包含任何带有标签 ei 且其底层强连通分量为 i-良好的状态。由此可知，路径 [f (n) $+$R$_\gamma$ $+$ 1, 2 f (n)] 不会访问 WB。根据 Pγ 和 Rγ的定义，这种情况发生的概率至多为 (1 $-$Pγ)$^{\lfloor}$f (n)/R$^{\gamma\rfloor-1}$。

• 经过 $f(n)$ 步后， ρ 已经到达了 $\mathcal{B}$。此外，第 n 次重启发生在第 $2f(n)+2R_\gamma-1$ 步之后。在这种情况下，我们令 $k \geq \lfloor f(n)/R_\gamma \rfloor + 1$ 为满足以下条件的最小数：路径 $[(k+1)R_\gamma+1, 2kR_\gamma]$ 不包含任何见证状态，即不包含带有 e_i 标签的状态。

根据 $\mathfrak{S}$[f], 在区间 [2lR$_\gamma$ $+$ 1 内发生 ρ 重启的定义，2(l $+$ 2)R$_\gamma$ $-$ 1]，并且已在前 f (n) 步内到达一个好底层强连通分量 $\mathcal{B}$ ，那么它会因某个满足 $\lfloor$f (n)/R $_\gamma\rfloor+1 \leq$ k $\leq$l 的 k 而被第三种情况涵盖。由于 k 是满足该性质的最小 k，且我们不属于第二种情况，因此该运行在 $\mathcal{B}$ 第 (l $-$ 1)R$_\gamma$ $+$ 1 步与 lRγ 步之间执行了一条进展路径；否则我们早已统计过这种情况。因此，最后两种情况的概率之和可由 (1 $-$ Pγ)$^{\lfloor f}$(n)/R$^{\gamma\rfloor-1}$ $+\sum^{\infty}$k$=\lfloor$f (n)/R$_\gamma\rfloor-1$Pγ(1 $-$ Pγ)^k 进行界定。

因此我们得到：

$$
\begin{aligned}
&Pr[\#\mathsf{r} \geq n \mid NB_n] \\
\leq&(1-p_\gamma)^{\lfloor f(n)/r_\gamma \rfloor} + (1-P_\gamma)^{\lfloor f(n)/R_\gamma \rfloor - 1} + \sum_{k=\lfloor f(n)/R_\gamma \rfloor - 1}^{\infty} P_\gamma (1-P_\gamma)^k \\
\leq&3(1-P_{\mathrm{m}})^{\lfloor f(n)/R_{\mathrm{m}} \rfloor - 1}
\end{aligned}
$$

□

引理 4.5(重启概率)。 设 $\mathcal{M}$ 为一个马尔可夫链，令 M$^{\mathfrak{S}[f]}_{\mathsf{r}}$ 为其关联的马尔可夫链，其中 $\mathfrak{S}[f]$ 是重启策略。经过 n 次 -1 重启后，运行再次重启的概率满足：

$$
\Pr[\#\mathsf{r} \geq n \mid \#\mathsf{r} \geq n-1] \leq 1 - P_{good}\left(1 - 3(1-P_{\mathrm{m}})^{\lfloor f(n)/R_{\mathrm{m}} \rfloor - 1}\right)
$$

证明。我们有

$$\begin{aligned}\Pr[\#\mathsf{r} \geq n \mid R \geq n-1] = \Pr[\#\mathsf{r} \geq n \mid NB_n] \cdot \Pr[NB_n \mid R \geq n-1] + \\ \Pr[\#\mathsf{r} \geq n \mid \overline{NB}_n] \cdot \Pr[\overline{NB}_n \mid \#\mathsf{r} \geq n-1].\end{aligned}$$

令 $\alpha := 3(1-P_{\mathrm{m}})^{\lfloor f(n)/R^{\mathrm{m}} \rfloor - 1}$。应用引理 4.4 和 $\Pr[\#\mathsf{r} \geq n \mid NB_n] \leq 1$，得到

$$\begin{aligned}&\Pr[\#\mathsf{r} \geq n \mid \#\mathsf{r} \geq n-1] \\ &\leq \alpha \Pr[NB_n \mid \#\mathsf{r} \geq n-1] + \Pr[\overline{NB}_n \mid \#\mathsf{r} \geq n-1] \\ &\leq \alpha \Pr[NB_n \mid \#\mathsf{r} \geq n-1] + (1 - \Pr[NB_n \mid \#\mathsf{r} \geq n-1]) \\ &\leq (\alpha - 1) \Pr[NB_n \mid \#\mathsf{r} \geq n-1] + 1\end{aligned}$$

以概率 1，$\mathcal{M}$ 的良好运行只访问 S^γ 中的状态。（事实上，如果某条良好运行访问了 S^γ 之外的某个状态，那么该运行只能到达一个坏 BSSC。由于该运行是良好的，因此它根本不能访问任何 BSSC，而这发生的概率只能为 0。）因此，在重启之前只访问 S^γ 中状态的概率，对于任意策略都至少为 P^{good}，即 $\Pr[NB_n \mid \#\mathsf{r} \geq n-1] \geq P^{\mathrm{good}}$。由此可得

$$\Pr[\#\mathsf{r} \geq n \mid \#\mathsf{r} \geq n-1] \leq (\alpha - 1)P_{\mathrm{good}} + 1 = 1 - P_{\mathrm{good}}(1-\alpha)$$

□

D. 第 5 节的证明

我们证明引理 5.4。我们需要一个技术性结果：

引理 D.1 (一个技术性引理)。对于 $c, X \in \mathbb{Z}_{\geq 0}$ 和 $0 < p < 1$，有

$$\sum_{n=X}^{\infty} n^c \cdot p^{n-X} \leq (c+1)! \left(\frac{(X+c)^c}{1-p} + \frac{1}{(1-p)^{c+1}} \right).$$

证明。我们将对 c 进行归纳法证明，从 $c = 0$ 开始。根据等比数列公式，我们有：

$$\sum_{n=X}^{\infty} p^{n-X} = \sum_{i=0}^{\infty} p^i = \frac{1}{1-p}.$$

这证明了归纳法的基础情形。现在假设我们已经证明了

$$S_{c-1}(X) := \sum_{n=X}^{\infty} n^{c-1} \cdot p^{n-X} \leq c! \left(\frac{(X+c-1)^{c-1}}{1-p} + \frac{1}{(1-p)^c} \right).$$

现在考虑

$$S_c(X) \coloneqq \sum_{n=X}^{\infty} n^c \cdot p^{n-X}$$

乘以 $(1-p)$ 后，我们得到如下结果

$$\begin{aligned}
(1-p)S_c(X) &= X^c + \sum_{n=X}^{\infty} \left((n+1)^c - n^c\right) \cdot p^{n-X} \\
&= X^c + \sum_{n=X}^{\infty} \left(\sum_{k=1}^{c} \binom{c}{k} n^{c-k} \right) p^{n-X} \\
&\le X^c + \sum_{n=X}^{\infty} c \left(\sum_{k=0}^{c-1} \binom{c-1}{k} n^{c-k} \right) p^{n-X} \\
&= X^c + \sum_{n=X}^{\infty} c(n+1)^{c-1} p^{n-X} \\
&= X^c + c \cdot \sum_{n=X+1}^{\infty} n^{c-1} p^{n-X-1} \\
&= X^c + cS_{c-1}(X+1) \\
&\le X^c + c \cdot c! \left(\frac{(X+c)^{c-1}}{1-p} + \frac{1}{(1-p)^c} \right) \\
S_c(X) &\le (c+1)! \left(\frac{(X+c)^c}{1-p} + \frac{1}{(1-p)^{c+1}} \right)
\end{aligned}$$

证明至此完成。 □

引理 5.4 （片段中的期望步数）**.** 对于策略 $\mathfrak{S}[n \mapsto n^c]$，我们有：

$$\mathbb{E}[S_n \mid \#\mathsf{r} \ge n-1] \le 2(R_{\mathrm{m}} + f(n)) + 9\left(\frac{R_{\mathrm{m}}}{P_{\mathrm{m}}(1-P_\gamma)}\right). \tag{5.5}$$

证明。 我们考虑三种情况：

（1）运行 ρ 在至多 $2f(n) + 2R_{\mathrm{m}}$ 步后，在第$(n-1)$次重启后，重新启动了n次。此情况下的期望步数可界定为 $2f(n) + 2R_{\mathrm{m}}$。

（2）运行 ρ 至少执行步数 $2f(n) + 2R_{\mathrm{m}} + 1$，在第$(n-1)$次重启后未发生另一次重启，并且只访问$S_\beta$中的状态。此时，到达坏底层强连通分量 $\mathcal{B}$ 之前的期望步数等于r_γ/p_γ。再经过r_γ/p_γ 步后，自上次重启以来访问的状态的后半部分现已包含在 $\mathcal{B}$ 中。然后，执行该底层强连通分量的一条进展路径所需的期望步数为R_β/P_β。至多再经过 $2f(n)$ 步

数后，该策略将重启。因此，在这种情况下，期望步数的上界为 $2r_\beta/p_\beta + R_\beta/P_\beta + 2f(n)$。

(3) 运行 ρ 在第 $2f(n) + 2R_{\mathrm{m}} + 1$ 步之后、$(n-1)$ 次重启后，在没有再次重启的情况下到达，并且只访问 S_γ 中的状态。在这种情况下，平均至多需要 $2r_\gamma/p_\gamma$ 步才能到达一个好底层强连通分量。此后，我们将运行的其余部分划分为长度为 $2R_\gamma$ 的块。令 v 为重启发生在 $2vR_\gamma$ 步与 $2(v+1)R_\gamma$ 步之间的数值。于是有：

(a) ρ 在第 $(v-1)R_\gamma$ 步与 $(v+1)R_\gamma$ 步之间访问了该底层强连通分量的一个接受状态。否则，重启发生在第 $2vR_\gamma$ 步之前。(b) ρ 在第 $(v+1)R_\gamma$ 步与 $2vR_\gamma$ 步之间没有访问该底层强连通分量的接受状态。事实上，如果我们在第 $2vR_\gamma$ 步重启，那么从第 vR_γ 步到第 $2vR_\gamma$ 步之间，我们尚未访问好底层强连通分量的接受状态。如果我们在第 $2(v+1)R_\gamma$ 步重启，则第 $(v+1)R_\gamma$ 步到第 $2(v+1)R_\gamma$ 步之间同样如此。对于发生在第 $2vR_\gamma$ 步与第 $2(v+1)R_\gamma$ 步之间的重启，相应的中间陈述为真。在所有这些情况下，运行从未在第 $(v+1)R_\gamma$ 步与第 $2vR_\gamma$ 步之间访问该底层强连通分量的接受状态。

（a）的概率至少为 $2P_\gamma$，而（b）的概率至多为$(1-P_\gamma)^{v-1}$。但是，如果（a）不成立，我们早已以$(1-P_\gamma)$ 的概率将其计入，且步数至多少 $2R_\gamma$ 步。因此，对于某个v，在$(n-1)$次重启后执行至多 $2(v+1)R_\gamma$ 步的情形，其期望步数可由对所有可能的v值，将 $2P_\gamma(1-P_\gamma)^{v-1}$乘以对应步数后求和来界定。

$$2f(n) + 2R_{\mathrm{m}} + \sum_{v=1}^{\infty} 4R_\gamma (v+1) P_\gamma (1-P_\gamma)^{v-1} = 2f(n) + 2R_{\mathrm{m}} + \frac{4R_\gamma}{P_\gamma(1-P_\gamma)}.$$

我们得到

$$\begin{aligned} E[S_n \mid \#\mathsf{r} \geq n-1] = {} & \left(2f(n) + 2R_{\mathrm{m}}\right) p_1 + \\ & 2r_\beta/p_\beta + R_\beta/P_\beta + 2f(n)p_2 + \\ & 2r_\gamma/p_\gamma + \frac{4R_\gamma}{P_\gamma(1-P_\gamma)} + \left(2f(n) + 2R_\gamma\right)(1-p_1-p_2) \end{aligned}$$

其中p_1, p{v6>分别是（1）和（2）的概率。使用$p_1, p_2 \leq 1$ 并进行简单运算，可得以下宽松界：

$$E[S_n \mid \#\mathsf{r} \geq n-1] \leq 2(R_{\mathrm{m}} + f(n)) + 9\left(\frac{R_{\mathrm{m}}}{P_{\mathrm{m}}(1-P_\gamma)}\right)$$

□

定理5。6 （总步数的期望数量）。对于策略 $\mathfrak{S}[n \mapsto n^c]$ 有 :

$$\mathbb{E}[S] \in \mathcal{O}\left((c+1)! \cdot 2^c \cdot \left(\frac{R_{\mathrm{m}}}{P_{\mathrm{m}}}\right)^{1+1/c} + \frac{2^c(c+1)!}{P_{good}^{c+1}} + (c+1)!(2c)^{c+1}\right).$$

证明。 根据期望的线性性，我们有 $\mathbb{E}[S] = \sum_{i=1}^{\infty} \mathbb{E}(S_n)$。证明思路是将求和拆成两部分：对于$n < X$，以及对于$n \geq X$。对于$n < X$，我们只需将 $\Pr[\#\mathsf{r} \geq n-1]$ 近似为 1。对于$n > X$，借助引理 5.3，我们可以得出更多结论：

$$\begin{aligned}\Pr[\#\mathsf{r} \geq n-1] &= \Pr[\#\mathsf{r} \geq n-1 \mid \#\mathsf{r} \geq n-2] \ldots \Pr[\#\mathsf{r} \geq X+1 \mid \#\mathsf{r} \geq X] \cdot \Pr[\#\mathsf{r} \geq X \quad] \\ &\leq \prod_{k=\lceil X \rceil}^{n} \Pr[\#\mathsf{r} \geq k \mid \#\mathsf{r} \geq k-1] \\ &\leq \left(1 - P_{\mathrm{good}}/2\right)^{n-X}\end{aligned}$$

由此得到：

$$\begin{aligned}E[S] &= \sum_{n=0}^{\infty} E[S_n \mid \#\mathsf{r} \geq n-1] \Pr[\#\mathsf{r} \geq n-1] \\ &\leq \sum_{n=0}^{X} E[S_n \mid \#\mathsf{r} \geq n-1] + \sum_{n=X}^{\infty} E[S_n \mid \#\mathsf{r} \geq n-1] \cdot \left(1 - P_{\mathrm{good}}/2\right)^{n-X}\end{aligned}$$

根据引理 5.4，我们对第一个被加数进行估计：

$$\begin{aligned}&\sum_{n=0}^{X} E[S_n \mid \#\mathsf{r} \geq n-1] \\ \leq &\sum_{n=0}^{X} 2n^c + 2R_{\mathrm{m}} + 9\left(\frac{R_{\mathrm{m}}}{P_{\mathrm{m}}(1-P_\gamma)}\right) \leq 2X^{c+1} + XR_{\mathrm{m}}\left(2 + 9\frac{1}{P_{\mathrm{m}}(1-P_\gamma)}\right).\end{aligned}$$

现在对第二个被加数进行界定，再次应用引理 5.4：

$$\begin{aligned}&\sum_{n=X}^{\infty} E[S_n \mid \#\mathsf{r} \geq n-1] \cdot \left(1 - P_{\mathrm{good}}/2\right)^{n-X} \\ \leq &\sum_{n=X}^{\infty} \left(2n^c + 2R_{\mathrm{m}} + 9\left(\frac{R_{\mathrm{m}}}{P_{\mathrm{m}}(1-P_\gamma)}\right)\right)\left(1 - P_{\mathrm{good}}/2\right)^{n-X} \\ \leq &\frac{2R_{\mathrm{m}}}{P_{\mathrm{good}}}\left(2 + 9\frac{1}{P_{\mathrm{m}}(1-P_\gamma)}\right) + 2\sum_{n=X}^{\infty} n^c \left(1 - P_{\mathrm{good}}/2\right)^{n-X} \\ \leq &\frac{2R_{\mathrm{m}}}{P_{\mathrm{good}}}\left(2 + 9\frac{1}{P_{\mathrm{m}}(1-P_\gamma)}\right) + 2(c+1)!\left(\frac{2(X+c)^c}{P_{\mathrm{good}}} + \frac{2^{c+1}}{P_{\mathrm{good}}^{c+1}}\right)\end{aligned}$$

其中在最后一步中，我们使用了引理 D.1。

$$\mathbb{E}[S] \in \mathcal{O}\left((c+1)! \cdot 2^c \cdot \left(\frac{R_{\mathrm{m}}}{P_{\mathrm{m}}}\right)^{1+1/c} + \frac{2^c(c+1)!}{P_{good}^{c+1}} + (c+1)!(2c)^{c+1}\right)$$

对于固定的c值，即对于特定的策略$f(n) = n^c$，该界限可简化为

$$\mathbb{E}[S] \in \mathcal{O}\left(\left(\frac{R_{\mathrm{m}}}{P_{\mathrm{m}}}\right)^{1+1/c} + \frac{1}{P_{\mathrm{good}}^{c+1}}\right).$$

□