arXiv:2301.10807v1 [cs.PL] 25 Jan 2023

知识程序的解释（含证明扩展版）*

Alexander Knapp[1], Heribert Mühlberger[1], 和 Bernhard Reus[2]

[1] 奥格斯堡大学，德国{knapp, muehlber}
@informatik.uni-augsburg.de[2] 英国萨塞克斯大
学 bernhard@sussex.ac.uk

摘要。基于知识的程序使用认知守卫来指定多智能体协议，这些守卫抽象了智能体如何学习并记录事实，或有关其他智能体和环境的信息。对这类程序的解释涉及一种非单调的相互依赖关系：一方面，要在可达状态上评估认知守卫；另一方面，可达状态的推导又取决于认知守卫的评估。我们将为同步编程语言发明的必须/不能分析技术应用于基于知识的程序的解释问题，并证明由此得到的构造性解释是单调的，且存在最小不动点。我们将这种方法与现有的同步程序和异步程序解释方案联系起来。最后，我们描述构造性解释的一种实现，并通过若干示例以及一个针对 Java内存模型的应用来说明这一过程。

1 引言

基于知识的程序 [12] 根据智能体对自身、其他智能体以及环境所知或不知情况的显式知识测试来描述多智能体系统：在扩展标准程序的基础上，智能体可以通过推理其他智能体和环境在所有可能的程序执行中的可能状态，超越其能够直接观测到的范围。这类非局部认知条件抽象了智能体如何学习并记录特定环境事实或有关其他智能体的信息。因此，基于知识的程序更准确地说是（多智能体）协议的规范，而这些协议可以由标准的、可直接执行的程序来实现。然而，要使其首先具备可实现性，就必须确保在所有可能的程序执行中，知识守卫都能得到一致的解析。

例如，考虑比特传输 [12, Ex. 4.1.1, Ex. 7.1.1],：发送方 S 必须通过有损信道向接收方 R 发送一个比特 sbit，而接收方 R 必须通过另一条有损信道确认收到该比特。这可以用状态变量 $\mathsf{sbit} \in \{0,1\}$、$\mathsf{rval} \in \{\bot,0,1\}$ 和 $\mathsf{ack} \in \{0,1\}$ 上的一个基于知识的程序建模，如下所示：S 只能直接观察（读取）sbit 和 ack，而 R 只能观察 rval（但双方都可以写入所有变量）；$(\mathrm{K}_\mathrm{R}\,\mathsf{sbit} = 0) \vee (\mathrm{K}_\mathrm{R}\,\mathsf{sbit} = 1)$ 表示 R 知道 sbit 的值，简写为 $\mathrm{K}_\mathrm{R}\,\mathsf{sbit}$。行为描述由一个循环守卫

* 一篇不含证明的简短版本已提交至 ESOP 23。

命令组成，其中有两个分支（这里 or 表示非确定性选择，skip 表示什么也不做）；该命令以 rval $= \bot$ 和 ack $= 0$ 初始化，而 sbit 保持未确定：

do $\neg \mathsf{K}_\mathrm{S}\, \mathsf{K}_\mathrm{R}\, \mathit{sbit} \twoheadrightarrow (\mathrm{rval} \leftarrow \mathrm{sbit}$ **or skip**$)$ — S
$[\!]\ \mathsf{K}_\mathrm{R}\, \mathit{sbit} \wedge \neg \mathsf{K}_\mathrm{R}\, \mathsf{K}_\mathrm{S}\, \mathsf{K}_\mathrm{R}\, \mathit{sbit} \twoheadrightarrow (\mathrm{ack} \leftarrow 1$ **or skip**$)$ **od** — R

程序中的认知公式 $\mathsf{K}_a\, \varphi$ 按照经典克里普克语义进行解释：φ 在智能体 a 当前认为可能的所有状态（或可能世界）中都成立。这些状态由两方面因素决定：一方面取决于状态信息 a 能够观测到什么：如果当前状态与另一个状态基于这些可用观测而不可区分，那么对该智能体而言，这两个状态都是可能的。不过，在上面的示例中，只有 S 能观测到 sbit；但由于协议的限制，最终应当有可能使 R 知道其值。另一方面，可能状态取决于基于知识的程序实际可能发生哪些运行，即在评估认知守卫并进行状态转换时哪些状态是可达的：如果只执行程序中的操作，就不可能到达同时满足 rval $\neq \bot$ 和 rval $\neq$ sbit 的状态；然而，该状态存在于全局状态空间中。关键在于，它在任何执行中都不可达，这样才能存在某次执行，使得 $\mathsf{K}_\mathrm{R}$sbit 变为真。反过来，也存在某次执行，使 K_R sbit（以及 $\mathsf{K}_\mathrm{S}\, \mathsf{K}_\mathrm{R}$ sbit）始终为假。

基于知识的程序的解释，恰恰取决于这种相互依赖关系：一方面，在可达状态上求值认知守卫；另一方面，根据认知守卫的求值结果推导可达状态。主体的认知状态由可观测量以及共同知晓的协议的可达状态隐式定义，这与 Baltag 的认知动作模型 [4,26], 形成鲜明对比；在后者中，认知状态是给定的，并且会被显式操纵。在许多情况下，包括比特传输协议，可以运用静态分析技术计算可达状态空间，而无需考虑守卫的认知性质。然而，知识与可达性之间的相互作用有时会变得更加复杂：可达状态越多，确定知道的内容就越少，而守卫反过来又会正向或负向地影响哪些状态可达。

再来看另一个例子：变量赋值问题 [12, 例 7.5]，其中有一个智能体 a 和一个状态变量 $\mathrm{x} \in \{0, 1, 2, 3\}$，而 a 无法直接观测 x。该智能体从 $\mathrm{x} = 0$开始执行以下带守卫条件的命令：

if $\mathsf{K}_\mathrm{a}\, \mathrm{x} \neq 1 \twoheadrightarrow \mathrm{x} \leftarrow 3$
$[\!]\ \mathsf{K}_\mathrm{a}\, \mathrm{x} \neq 3 \twoheadrightarrow \mathrm{x} \leftarrow 1$ **fi**

显然，$\mathrm{x} = 0$必然可达，而 $\mathrm{x} = 2$必然不可达。然而，对于其余取值，有两种不同的可达状态集合能够使知识守卫的一致解释成立：$\{\mathrm{x} = 0、\mathrm{x} = 1\}$，此时 $\mathsf{K}_\mathrm{a}\, \mathrm{x} \neq 1$为假而 $\mathsf{K}_\mathrm{a}\, \mathrm{x} \neq 3$为真；以及 $\{\mathrm{x} = 0、\mathrm{x} = 3\}$，此时结果相反。单元素集合 $\{\mathrm{x} = 0\}$ 可以排除，因为两个守卫都会为真，因此 $\mathrm{x} = 3$ 和 $\mathrm{x} = 1$ 都可达；而 $\{\mathrm{x} = 0、\mathrm{x} = 1、\mathrm{x} = 3\}$ 则不可能，因为两个守卫都为假，因此 $\mathrm{x} = 1$ 和 $\mathrm{x} = 3$ 都不可达。打破这一循环的一种方法是让其中一个状态转换不再以知识为条件，例如，像下面这样：

if $\mathsf{K}_\mathrm{a}\, \mathrm{x} \neq 1 \twoheadrightarrow \mathrm{x} \leftarrow 3$
$[\!]\ \mathsf{K}_\mathrm{a}\, \mathrm{x} \neq 3 \twoheadrightarrow \mathrm{x} \leftarrow 2$
$[\!]\ \mathrm{true} \twoheadrightarrow \mathrm{x} \leftarrow 1$ **fi**

由此得到一个具有唯一解 $\{x = 1, x = 2\}$ 的基于知识的程序。不过，要计算其行为，需要经过几个步骤：首先推理出 $x = 1$ 可达，然后推理出 $x = 3$ 不可达，最后推理出 $x = 2$ 可达。

相关工作。 在关于基于知识的程序的引言和开创性专著中， [11,12], Fagin 等人通过这些程序对过去的依赖，刻画了它们的唯一可解释性；这里讨论的是某个非空的迁移系统类：必须确保，对于该类中所有具有当前状态共同过去的解释，知识守卫在某一状态下的求值结果都一致。对过去的依赖的一个充分条件是，程序为该类中的所有解释“提供认知见证”，使得在某个时刻不知道某事时，过去存在一个反例。而提供认知见证的一个充分条件，则是程序“同步”，即所有智能体都能根据各自的局部状态确定全局时间。例如，比特传输协议确实提供了认知见证，因此具有唯一可解释性；但它并不同步。破环变量赋值程序也具有唯一可解释性，但它不提供认知见证，因此并不同步，尽管它只有一个智能体。对于“异步”的基于知识的程序，De Haan 等人 [9] 建议采用非单调可达性泛函的经典迭代，根据当前假定为可达的内容来解释知识模态。计算过程从假定所有状态均可达开始，并在某个状态集合重复出现时停止。这种方法为所有基于知识的程序都确定了一种语义，包括那些存在循环和矛盾，或仅仅自我实现的程序。

守卫求值与可达性相互依赖的问题，也出现在面向嵌入式系统的同步编程语言的设计中，例如 Esterel [6] 或 Lustre [14], 。这些语言依赖“完美同步”：对某些输入作出响应的一个步骤耗时为零，输出信号恰好与输入信号同时产生。因此，由于可以同时查询待产生信号的状态，这就要求满足“逻辑一致性”：当且仅当某个发出（非输入）信号的命令在某一步执行中得到执行时，该信号才会在这一步中出现。Lustre 在语法层面禁止循环程序，而 Berry 的方法则通过静态可执行性分析，从 Esterel [7] 的语义中筛选出“反应式”（至少执行一次）和“确定的”（至多执行一次）程序：分析会计算哪些信号必须出现，即必然会出现；以及哪些信号不可能出现，即不存在发出该信号的执行。这也称为必须/不能分析，需要多次执行，以找到所有信号状态的不动点。值得注意的是，这种分析不需要过去的见证。

贡献。 我们将必须/不能分析的原则应用于基于知识的程序的可解释性问题。在回顾认知逻辑和认知转移结构的一些基本概念之后（第 2 节），我们首先重述 Fagin 等人 [12] 和 De Haan 等人 [9] 提出的方法，这些方法以认知守卫转移系统为基础；这种形式与语法无关，可用于表示基于知识的程序（第 3 节）。与这些设计不同，我们采用基于状态而非基于运行的方案，从而能够进行更直接的分析。我们通过若干示例展示两种解释方案的成果与局限，这些示例阐明了循环、矛盾或自我实现程序中的（非）同步性和非单调解释

。后一种行为是我们将解释问题重新表述为认知必然/可能转移结构的主要动机；这种结构为基于知识的程序的行为提供下界和上界（第 4 节）。我们证明，这种构造性解释始终是单调的，并能得出一个最小不动点。然而，不动点的下界和上界未必总是一致；我们还将已判定不动点与“提供认知见证”和同步性的概念联系起来。随后，我们将必然/可能近似技术推广到具有正、负前提的推理系统（第 5 节）。基于知识的程序的行为可以用规则系统表示，该系统还允许表达某些事实无法推导；单调性和不动点性质可以直接推广到这些一般规则系统。最后，我们介绍了构造性解释方法在“时序认知模型解释器和检查器”（tEmIc，第 6 节）中的实现。对于经解释的基于知识的程序的模型检验，该工具支持 CTLK，即“计算树逻辑”（CTL）与认知逻辑的结合。此外，这种逻辑也可用于程序守卫；对这类时序认知程序的解释扩展了以往的方法。我们还介绍了该方法在 Java内存模型分析中的一些应用。

2 认知逻辑与认知转移结构

我们简要概述用于表达知识守卫 [26,25]的认知逻辑基本概念。随后，我们将认知转移结构定义为知识程序的解释域。这些转移结构将程序执行的时间维度与用于评估主体所知内容的认知维度结合起来。逻辑和转移结构都建立在认知签名 $\Sigma = (P, A)$之上，该签名由一组命题 P和一组主体 A组成。

2.1 认知逻辑

在(P, A)之上的认知结构 $K = (W, R, L)$由一组可能世界 W、一个A族的认知可达关系 $R = (R_a \subseteq W \times W)_{a \in A}$以及一个标记$L$: $W \to \wp P$构成。在具体示例中，我们要求 R_a是一个等价关系，并且如果$(w_1, w_2) \in R_a$，那么智能体 a 无法区分这两个可能世界w_1 和 w_2。(P, A)之上的认知公式$\varphi \in \Phi_{P,\ A}$ 由以下语法定义：

$$\varphi ::= p \mid \text{false} \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid \mathsf{K}_a\, \varphi$$

其中 $p \in P$ 和 $a \in A$。认知公式 $\mathsf{K}_a\, \varphi$ 读作“智能体 a知道 φ”。我们采用通常的命题逻辑缩写：true 表示 $\neg$，false 表示 $\varphi_1 \vee \varphi_2$，而$\neg$表示$\neg\varphi_1 \wedge \neg\varphi_2$($\neg\varphi_1 \wedge \neg\varphi_2$)。此外，我们将认知模态 M 视为 K 的对偶，因此 $\mathsf{M}_a\, \varphi$ 是 $\neg\mathsf{K}_a\, \neg\varphi$ 的缩写，读作“智能体 a 认为 φ 有可能”。认知公式$\varphi \in \Phi_{P,\ A}$ 在认知结构 $K = (W, R, L)$（定义于 (P, A)上）的世界 $w \in W$ 处的满足关系，记作 $K, w \models \varphi$，归纳定义如下：

$$K, w \models p \iff p \in L(w)$$

$K, w \not\models \mathsf{false} K, w \models \neg\varphi \iff K, w \not\models \varphi K,$
$w \models \varphi_1 \wedge \varphi_2 \iff K, w \models \varphi_1$ 和 $K, w \models \varphi_2 K, w \models \mathrm{K}$
$_a\,\varphi \iff K, w' \models \varphi$ f. a. $w' \in W$ 与 $(w, w') \in R_a$

2.2 认知转移结构

认知转移结构将时间转移关系与定义在同一组状态上的认知可及关系结合起来。状态转换描述从初始状态集可以到达哪些状态，可及关系则描述哪些状态彼此不可区分。知识公式在相应的全局认知结构上进行求值。这个导出的结构以可达状态作为其可能世界，并沿用可及关系，但将其限制在可达状态上。

形式上，定义在（P, A）上的认知转移结构 $M = (S, E, L, S_0, T)$由一个认知结构（S, E, L）、一个时间初始状态集初始状态 $S_0 \subseteq S$以及一个时间转移关系 $T \subseteq S \times S$组成。我们用 $S(M)$表示 S，用 $T(M)$表示 T，等等。M的（时间）可达状态 $S_\omega(M) = \bigcup_{0 \le k} S_k(M)$和转移关系$T_\omega(M) = \bigcup_{0 \le k} T_k(M)$通过归纳定义如下

$$S_0(M) = S_0, \quad S_{k+1}(M) = S_k(M) \cup \{s' \mid \text{ex. } s \in S_k(M) \text{ s. t. } (s, s') \in T\}$$
$$T_0(M) = \emptyset, \quad T_{k+1}(M) = T_k(M) \cup \{(s, s') \in T \mid s \in S_k(M)\}\,.$$

M的相关认知结构由 $K(M) = (S_\omega(M)\ E \cap S_\omega(M)^2, L \restriction S_\omega(M))$ 给出。认知公式 $\varphi \in \Phi_{P,\ A}$ 在 M 上、于 $s \in S_\omega(M)$ 处的满足关系，记作 $M, s \models \varphi$，定义如下：

$$M, s \models \varphi \iff K(M), s \models \varphi\,.$$

在 $\Sigma = (P, A)$ 上，与相同认知状态基 $\mathrm{B} = (S, E, L, S_0)$ 共享的认知转移结构集合记作 $\mathscr{M}_\Sigma(\mathrm{B})$。我们称 $M_1 \subseteq M_2$ for$M_1, M_2 \in \mathscr{M}_\Sigma(\mathrm{B})$，若 $T(M_1) \subseteq T(M_2)$；并以类似方式将转移关系上的并集和交集扩展到认知转移结构。

3 基于知识的程序

基于知识的程序通过显式知识测试扩展了标准程序。其解释涉及一个循环：认知守卫的求值取决于程序的可达状态，而可达状态的推导又取决于程序的认知守卫的求值。

我们将基于知识的程序表示为一种与语法无关的形式，即认知守卫转移系统。与认知转移结构类似，这些守卫系统在一个全局状态集合上运行，该集合具有认知可及关系和命题标记。所有程序步骤都表示为知识守卫动作，其形式为$\varphi \supset B$ with φ一个认知公式and B语义状态上的一个关系。通过选择 $\varphi = \mathsf{true}$，可以得到不依赖知识的决策；而任何类型的程序控制结构，都可以通过恰当选择守卫动作来表达。

为了打破为基于知识的程序赋予含义这一循环过程，认知守卫转移系统 Γ 是在认知转移结构 M 上进行解释，从而得到另一个认知转移结构 Γ^M。Γ 中的一个守卫动作 $\varphi \supset B$ 贡献了满足以下条件的那些 (s, s')：$M, s \models \varphi$；其中尤其是，s 在 M 中可达。我们要寻找的是一种一致解释，使得 $\Gamma^M = M$，从而让可达性与知识能够相互确立。要找到这样一种平衡结构并不容易，因为解释泛函通常并非单调：可达的状态越多，已知的就越少，而这又可能导致更多或更少的状态变得可达。

介绍并举例说明了我们所采用的基于知识的程序格式后，我们总结并调整了两种现有的解释方法。这些方法是为基于运行而非基于状态的系统设计的：De Haan 等人 [9] 提出从所有状态均可达的认知转移结构开始，迭代解释泛函。迭代会在达到不动点时停止；若因非单调性而发现矛盾，也会停止。这样，所有基于知识的程序都能获得某种语义，不再区分有意义的程序与矛盾的程序或仅仅自我实现的程序。Fagin 等人 [11,12] 最初提出的方法，则通过「依赖过去」这一概念，刻画出具有唯一一致解释的基于知识的程序。该方法还提出了提供认知见证的一个充分条件，尤其适用于同步基于知识的程序这一子类。

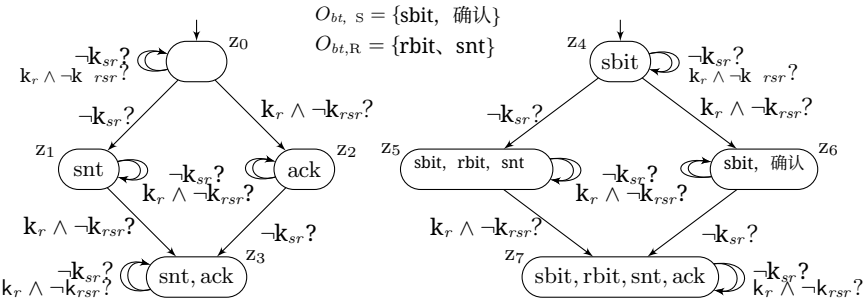
3.1 认知守卫转移系统

一个在 (P, A) 上的认知守卫转移系统 $\Gamma = (S, E, L, S_0, \mathcal{T})$，由一个在 (P, A) 上的认知状态基 (S, E, L, S_0)，以及一组 $\mathcal{T}$ 认知守卫动作 $\varphi \supset B$ 构成。每个动作包含一个认知公式 $\varphi \in \Phi_{P,\ A}$ 作为守卫，以及一个转移关系 $B \subseteq S \times S$。

例*1.* (a) 考虑引言中的比特传输问题：

循环 $\neg \mathrm{K_S}\,\mathrm{K_R}$sbit $\twoheadrightarrow$ (返回值 $\leftarrow$ sbit 或跳过) 8 $\mathrm{K_R}$
sbit $\wedge\, \neg \mathrm{K_R}\mathrm{K_S}\,\mathrm{K_R}$ sbit $\twoheadrightarrow$ (确认 $\leftarrow 1$ 或跳过) 结束循环

发送方智能体 S 通过设置 rval $\in \{\perp, 0, 1\}$，经由不可靠信道向接收方智能体 R 发送一位 sbit $\in \{0, 1\}$；R 则通过设置 ack $\in \{0, 1\}$，经由不可靠信道确认收到该位。我们再次将 $(\mathrm{K_R}\,\neg$sbit$)\vee(\mathrm{K_R}$ sbit$)$ 简写为 $\mathrm{K_R}$ sbit，以表示接收方知道要发送的位。我们将这个问题具体化为一个认知守卫转换系统 $\Gamma_{bt} = (\mathrm{B}_{bt}, \mathcal{T}_{bt})$，其中 $\mathrm{B}_{bt} = (S_{bt}, E_{bt}, L_{bt}, S_{bt,\ 0})$ 定义在 $\Sigma_{bt} = (P_{bt}, A_{bt})$ 上，包含命题 $P_{bt} =$ {sbit、rbit、snt、ack} 以及智能体 $A_{bt} =$ {S、R}。由于采用命题编码，我们用命题 rbit 表示 rval $\in \{\perp, 0, 1\}$，用于表示传输的位；并用命题 snt 表示 rbit 的有效性。进一步将知识守卫 $\mathrm{K_R}$ sbit 简写为 k_r，将 $\mathrm{K_S}\,\mathrm{K_R}$ sbit 简写为 k_{sr}，将 $\mathrm{K_R}\,\mathrm{K_S}\,\mathrm{K_R}$ sbit 简写为 k_{rsr}，该转换系统 Γ_{bt} 的图示如下：



状态 S_{bt} 包括 $\{\mathsf{z}_0, \mathsf{z1}、\ldots\ldots、\mathsf{z}_7\}$，其中 $L_{bt}(\mathsf{z}_0) = \emptyset$、$L_{bt}(\mathsf{z}_1) = \{\mathsf{snt}\}$、……、$L_{bt}(\mathsf{z}_7) = \{\mathsf{sbit}、\ \mathsf{rbit}、\ \mathsf{snt}、\ \mathsf{ack}\}$，如上图所示；初始状态集为 $S_{bt,0} = \{\mathsf{z}_0, \mathsf{z}_4\}$。智能体 $a \in A_{bt}$ 的认知可及关系 $E_{bt,a}$ 由可观测集 $O_{bt,a}$ 给出，这些集合规定两个状态 $s_1, s_2 \in S_{bt}$ 在 $O_{bt,a}$ 看来不可区分，记作 $s_1 \sim_{O_{bt,a}} s_2$；若对所有 $p \in O_{bt,a}$，都有 $p \in L_{bt}(s_1) \iff p \in L_{bt}(s_2)$，则有 $E_{bt,a} = \sim_{O_{bt,a}}$，从而 $E_{bt,a}$ 构成等价关系。由于 $\mathsf{sbit} \notin O_{bt,\mathrm{R}}$，接收方 R 无法“看到”sbit，因此无法区分状态 z_0 和 z_4，，但 S 可以。另一方面，R 可以区分 z_1 和 z_5，因为 R 可以访问 rbit。最后，$\mathcal{T}_{bt}$ 由两个认知守卫动作组成。

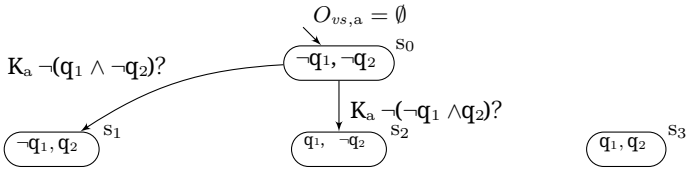
$$\neg \mathsf{K_S}\, \mathsf{K_R}\, sbit \supset \{(\mathsf{z}_i, \mathsf{z}_i) \mid 0 \le i \le 7\} \cup \{(\mathsf{z}_0, \mathsf{z}_1), (\mathsf{z}_2, \mathsf{z}_3), (\mathsf{z}_4, \mathsf{z}_5), (\mathsf{z}_6, \mathsf{z}_7)\}\ ,$$
$$\mathsf{K_R}\, sbit \wedge \neg \mathsf{K_R}\, \mathsf{K_S}\, \mathsf{K_R}\, sbit \supset \{(\mathsf{z}_i, \mathsf{z}_i) \mid 0 \le i \le 7\} \cup \{(\mathsf{z}_0, \mathsf{z}_2), (\mathsf{z}_1, \mathsf{z}_3), (\mathsf{z}_4, \mathsf{z}_6), (\mathsf{z}_5, \mathsf{z}_7)\}\ ,$$

它们直接反映了比特传输问题中的发送和确认操作：如果 S 不知道 R 知道该比特，系统就只能从 z_0 前进到 z_1（以及从 z_4 前进到 z_5）；在这两种情况下，发送均已成功，但系统不一定会取得这样的进展，即发送可能失败。类似地，只有当 R 知道该比特，并且 R 不知道 S 知道 R 知道该比特时，系统才能从 z_1 前进到 z_3（以及从 z_5 前进到 z_7）；在这两种情况下，确认均已成功发送。

（b）考虑引言中单个智能体 a 的变量赋值问题：

if $\mathsf{K_a}\, \mathrm{x} \neq 1 \twoheadrightarrow \mathrm{x} \leftarrow 3$
$[\!]\ \mathsf{K_a}\, \mathrm{x} \neq 3 \twoheadrightarrow \mathrm{x} \leftarrow 1$ **fi**

用两个比特 q_1 和 q_2，对整数 $\mathrm{x} \in \{0, 1, 2, 3\}$ 进行编码，我们将该问题建模为以下认知守卫转移系统 $\Gamma_{vs} = (\mathsf{B}_{vs}, \mathcal{T}_{vs})$，其中 $\mathsf{B}_{vs} = (S_{vs}, E_{vs}, L_{vs}, S_{vs,\ 0})$ 定义在 $\Sigma_{vs} = (P_{vs}, A_{vs})$ 上，且 $P_{vs} = \{\mathsf{q}_1, \mathsf{q}_2\}$ 和 $A_{vs} = \{\mathsf{a}\}$：



$O_{vs,\ \mathrm{a}}$ 表示一个“盲”智能体 a，它认为所有状态都同样可达。状态 s_3 绝对不可达。$\mathcal{T}_{vs}$ 由两个认知守卫动作组成：

$$\mathsf{K_a}\, \neg(\mathsf{q}_1 \wedge \neg \mathsf{q}_2) \supset \{(\mathsf{s}_0, \mathsf{s}_1)\}\ ,$$

$\mathsf{K}_{\mathrm{a}} \neg(\neg \mathrm{q}_1 \wedge \mathrm{q}_2) \supset \{(\mathrm{s}_0, \mathrm{s}_2)\}$. □

3.2 解释受认知约束的迁移系统

在 (P, A) 上的认知守卫转移系统 $\Gamma = (S, E, L, S_0, \mathcal{T})$，通过将每个守卫动作 $(\varphi \supset B)$ 相对于 M 解释为如下形式，来解释于认知转移结构 $M \in \mathscr{M}_{P,\ A}(S, E, L, S_0)$ 上：解释

$$(\varphi \supset B)^M = \{(s, s') \in B \mid s \in S_\omega(M) \text{ and } M, s \models \varphi\} ,$$

并将这些解释合并为认知转移结构

$$\Gamma^M = (S, E, L, S_0, \bigcup_{\tau \in \mathcal{T}} \tau^M) .$$

我们称 M a 解 为 Γ 的解，若 $\Gamma^M = M$。

例*2.* 对于例1(a)中所述的比特传输问题，认知转移结构

$M_{bt} =$ $_{bt}$ T_{bt} $T_{bt} = \{$ $_i$ $_i$ $\mid i \in \{0,1,3,4,5,7\}\} \cup$(B ,)，其中 $\{$ $_0$, $_1$, $_1$, $_3$, $_4$, $_5$, $_5$, $_7$ $\}$ $\Gamma_{bt}{}^{M_{bt}} = M_{bt}$ (z , z) (z z) (z z) (z z) (z z)，满足 。该结构仅省略了状态 z_2 和 z_6，它们满足 $L_{bt}(\mathrm{z}_2) = \{$ 确认$\}$ 和 $L_{bt}(\mathrm{z}_6) = \{$sbit、确认$\}$，显然不可达，因为 K_{R}sbit 在 $\mathrm{z}^0 \sim_{O_{bt}\text{中为假},\ \mathrm{R}} \mathrm{z}_4$。事实上，

$$M_{bt}, s \models \neg \mathsf{K}_{\mathrm{S}} \mathsf{K}_{\mathrm{R}}\, sbit \iff s \in \{\mathrm{z}_0, \mathrm{z}_1, \mathrm{z}_4, \mathrm{z}_5\}$$
$$M_{bt}, s \models \mathsf{K}_{\mathrm{R}}\, sbit \iff s \in \{\mathrm{z}_1, \mathrm{z}_3, \mathrm{z}_5, \mathrm{z}_7\}$$
$$M_{bt}, s \models \neg \mathsf{K}_{\mathrm{R}} \mathsf{K}_{\mathrm{S}} \mathsf{K}_{\mathrm{R}}\, sbit \iff s \in \{\mathrm{z}_0, \mathrm{z}_1, \mathrm{z}_3, \mathrm{z}_4, \mathrm{z}_5, \mathrm{z}_7\}$$ □

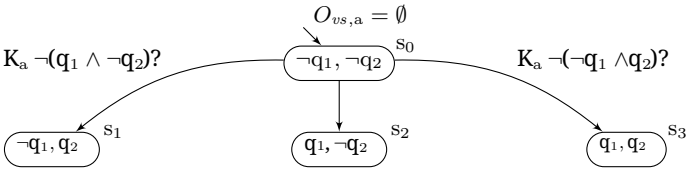
然而，寻找解的复杂之处在于，一般而言，在认知转移结构上解释受认知约束的迁移系统这一泛函并非单调，以下示例对此进行了说明。

例*3*。 (a) 对变量赋值问题 Γ_{vs} 继续例 1(b)，考虑认知转移结构 $M_{vs,0} \in \mathscr{M}_{\Sigma_{vs}}$ (B$_{vs}$)，其转移关系为空$T(M_{vs,0}) = \emptyset$，因此 $S_0(M_{vs,0}) = \{\mathrm{s}_0\}$。对 $0 \leq i \leq 2$依次赋值 $M_{vs,i+1} = \Gamma_{vs}{}^{M_{vs,\ i}}$，我们得到

τ	$\tau^{M_{vs,0}}$	$\tau^{M_{vs,1}}$	$\tau^{M_{vs,2}}$
$\mathsf{K}_{\mathrm{a}} \neg(\mathrm{q}_1 \wedge \neg \mathrm{q}_2) \supset \{(\mathrm{s}_0,\mathrm{s}_1)\}$	$\{(\mathrm{s}_0, \mathrm{s}_1)\}$	$\emptyset$	$\{(\mathrm{s}_0, \mathrm{s}_1)\}$
$\mathsf{K}_{\mathrm{a}} \neg(\neg \mathrm{q}_1 \wedge \mathrm{q}_2) \supset \{(\mathrm{s}_0,\mathrm{s}_2)\}$	$\{(\mathrm{s}_0, \mathrm{s}_2)\}$	$\emptyset$	$\{(\mathrm{s}_0, \mathrm{s}_2)\}$

特别地，M_{vs}、$_2 = \Gamma_{vs}{}^{M_{vs}}$、$_1 = \Gamma_{vs}{}^{\Gamma_{vs}{}^{M_{vs}}}$、$^0 = M_{vs}$、0。然而，对于$M_{vs}$、4、$M_{vs}$、$_5 \in \mathscr{M}_{\Sigma_{vs}}$(B$_{vs}$)，其中 $T(M_{vs}$,4) $= \{(\mathrm{s}_0, \mathrm{s}_1)\}$ 以及 $T(M_{vs}$,5) $= \{(\mathrm{s}_0, \mathrm{s}_2)\}$，我们得到 $\Gamma_{vs}{}^{M_{vs}}$、$^4 = M_{vs}$、4以及$\Gamma_{vs}{}^{M_{vs}}$、$^5 = M_{vs}$、5。

(b) 为了刻画引言中的环断裂变量设定，考虑如下关于 Σ_{vs} 的认知守卫转移系统 $\Gamma_{vsb} = (\mathrm{B}_{vs}, \mathcal{T}_{vsb})$，它与例 1(b) 共享认知状态基 B$_{vs}$：



对于 $M_{vsb,0} = (\mathrm{B}_{vs}, \emptyset)$，其中 $S_0(M_{vsb,0}) = \{\mathrm{s}_0\}$，并令 $M_{vsb,i+1} = \Gamma_{vsb}{}^{M_{vsb,i}}$ for $0 \leq i \leq 3$，我们依次得到

τ	$\tau^{M_{vsb,0}}$	$\tau^{M_{vsb,1}}$	$\tau^{M_{vsb,2}}$	$\tau^{M_{vsb,3}}$
$\mathrm{K_a}\,\neg(\mathrm{q}_1 \wedge \neg\mathrm{q}_2) \supset \{(\mathrm{s}_0,\mathrm{s}_1)\}$	$\{(\mathrm{s}_0,\mathrm{s}_1)\}$	$\emptyset$	$\emptyset$	$\emptyset$
真 $\supset \{(\mathrm{s}_0,\mathrm{s}_2)\}$	$\{(\mathrm{s}_0,\mathrm{s}_2)\}$	$\{(\mathrm{s}_0,\mathrm{s}_2)\}$	$\{(\mathrm{s}_0,\mathrm{s}_2)\}$	$\{(\mathrm{s}_0,\mathrm{s}_2)\}$
$\mathrm{K_a}\,\neg(\neg\mathrm{q}_1 \wedge \mathrm{q}_2) \supset \{(\mathrm{s}_0,\mathrm{s}_3)\}$	$\{(\mathrm{s}_0,\mathrm{s}_3)\}$	$\emptyset$	$\{(\mathrm{s}_0,\mathrm{s}_3)\}$	$\{(\mathrm{s}_0,\mathrm{s}_3)\}$

对于这个认知转移结构 $M_{vsb,3}$ 其中 $S_\omega(M_{vsb,3}) = \{\mathrm{s}_0,\mathrm{s}_1,\mathrm{s}_3\}$ 最终成立的是 $\Gamma_{vsb}{}^{M_{vsb,3}} = M_{vsb,3}$。 □

3.3 迭代语义

为说明解释泛函的非单调性，我们从最小的认知转移结构开始了 Γ 的解释序列，这提示我们寻找最小不动点——但它未必存在。De Haan 等人 [9] 认为，以最大不动点作为替代会更宽松。他们构造了一个超限近似序列，从一个所有状态均可达的 N_0 开始。对于后继序数 α+1，近似值 $N_{\alpha+1}$ 就是 Γ 在 N_α 中的解释；对于极限序数 λ，近似值 N_λ 是“与极限足够接近的近似值之并的交” [9, 第 7] 页。后一种做法优于交之并，因为它包含更多状态，这意味着知识更少，因此“主体 [只有在有充分理由时才知道] 事实”（同上）。

更形式地，通过超限归纳，为认知守卫转移系统 $\Gamma = (S, E, L, S_0, \mathcal{T})$ 在 (P, A) 上定义如下解释序列：

$$N_0 = (S, E, L, S_0, S \times S)$$
$$N_{\alpha+1} = \Gamma^{N_\alpha} \quad \text{for any successor ordinal } \alpha + 1$$
$$N_\lambda = \bigcap_{\alpha<\lambda} \bigcup_{\alpha\leq\beta<\lambda} N_\beta \quad \text{for any limit ordinal } \lambda$$

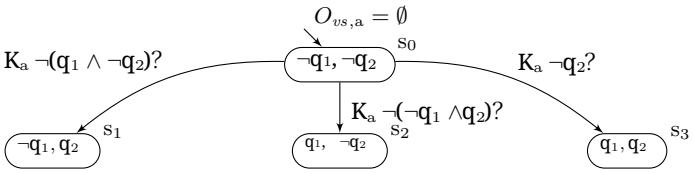
交集和并集指认知转移结构的转移关系，参见第 2.2 节。由于基数的原因，某个认知转移结构必定会重复出现，也就是说，序数 $\eta_\Gamma = \inf\{\alpha \mid \text{ex. } \beta \text{ s. t. } \alpha < \beta \text{ and } N_\alpha = N_\beta\}$是良定义的。如果 $N_{\alpha+1} \subseteq N_\alpha$对所有 $\alpha \geq \eta_\Gamma$都成立，则 $N_{\eta_\Gamma+1} = N_{\eta_\Gamma}$；否则存在某个序数 $\alpha \geq \eta_\Gamma$ 使得 $N_{\alpha+1} \not\subseteq N_\alpha$。因此，序数 $\alpha_\Gamma = \inf\{\alpha \mid \eta_\Gamma \leq \alpha \text{ and } (N_\alpha = N_{\alpha+1} \text{ or } N_{\alpha+1} \not\subseteq N_\alpha)\}$ 是良定义的。 Γ的迭代语义定义为 N_{α_Γ}。

如果解释泛函是单调的，迭代便从所有状态均可达开始，并导向最大不动点。

例4。（a）对于例 1(b) 中的变量赋值问题 Γ_{vs}，解释序列 $(N_{vs,\alpha})_{0\leq\alpha}$ 从 $N_{vs,0}$ 开始，表明 $T(N_{vs,0}) = S_{vs} \times S_{vs}$。利用例 3(a) 中的认知转移结构，对于偶数 k，有 $N_{vs,k+1} = \Gamma_{vs}{}^{N_{vs,k}} = M_{vs,2}$；对于奇数 $k \geq 1$，有 $N_{vs,k+1} = M_{vs,1}$。因此，$N_{vs,1} = N_{vs,3}$，使得 $\eta_{\Gamma_{vs}} = 1 = \alpha_{\Gamma_{vs}}$，因为 $T(N_{vs,2}) = \{(s_0, s_0), (s_0, s_1), (s_0, s_2)\} \not\subseteq \emptyset = T(N_{vs,1})$。因此，$\Gamma_{vs}$ 的迭代语义为 $N_{vs,1} = M_{vs,2}$；由于其转移关系为空，Γ_{vs} 与不含任何受保护动作的认知受保护转移系统具有相同的迭代语义。

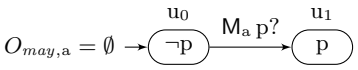
(b) 计算 Ex. 3(b) 的环断裂变量设定 Γ_{vsb} 的迭代语义序列 $(N_{vsb,\,\alpha})_{0\leq k}$ 的过程如下：$N_{vsb,\,k} = M_{vsb,\,k+1}$。由于这一次从 $\alpha = 1$ 起泛函是单调的，迭代语义为 $N_{vsb,\,2}$。

(c) 考虑如下认知守卫转移系统 $\Gamma_{nc} = (B_{vs}, \mathcal{T}_{nc})$，其定义在 Σ_{vs} 上，与 (a) 的变量赋值问题 Γ_{vs} 共享认知基底 B_{vs}，并且仅增加了守卫动作 $K_a \neg q_2 \supset \{(s_0, s_3)\}$：



解释过程与 Γ_{vs} 的情况相同，而空转移关系也是 Γ_{nc} 的迭代语义。不过，存在一个唯一的非空解释：仅由 (s_0, s_1) 构成的转移结构。找到这个解并非通过构造即可完成，因此需要进行一些推测：不存在使 s_2 可达、但 s_1, 不可达的解，因为这样一来，s_3 的（非）可达性就会导致矛盾。因此，唯一剩下的可能性是 s_0 和 s_1 可达，而 s_2 和 s_3 不可达。

（d）对于由下式给出的、定义在 $(\{p\}, \{a\})$ 上的认知守卫转移系统 Γ_{may}



从 $N_{may,\,0}$ 开始的迭代过程，其中 $T(N_{may,\,0}) = \{u_0, u_1\} \times \{u_0, u_1\}$，得出 M_a p 为真；于是我们得到 $N_{may,\,1}$，其中 $T(N_{may,\,1}) = \{(u_0, u_1)\}$，这又在下一次迭代中得到确认，从而产生一个不动点。然而，这种迭代语义带有一丝“事后预言”的意味：p 是可达的，因为 p 可能会变得可达。 □

3.4 唯一解释解

只有当每个知识守卫都能根据执行到当前时刻为止已计算出的内容被稳定地判定时，基于知识的程序才能可靠地逐步执行。尤其是，要通过执行得到一个解，知识就不能被后来才获取的信息推翻。反过来，如果只需查看过去就能判定所有知识守卫，那么至多只有一个解。

基于这一观察，Fagin 等人 [11,12] 通过刻画解“依赖于过去”这一概念，提出了唯一可解释性的形式化表征。他们继而证明，“提供认知见证”是“对过去的依赖”的充分判据，而“同步的”程序总是满足这一条件。我们简要概述他们的主要论证思路，并将其从针对基于知识的程序的基于运行的论述，改写为针对我们的基于状态的认知守卫迁移系统的论述。改写的细节见附录 A。

若对于所有 M_1、$M_2 \in \mathcal{M}$ 和所有 $k \in \mathbb{N}$，只要 $T_k(M_1) = T_k(M_2)$，就有 M_1、$s \models \varphi \iff M_2$、$s \models \varphi$ 对所有 $s \in S_k(M_1) \cap S_k(M_2)$，则称认知公式 $\varphi \in \Phi_{P,A}$ 相对于一类认知转移结构 $\mathcal{M} \subseteq \mathscr{M}_{P,A}(\mathsf{B})$ 依赖于过去；若认知守卫转移系统 $\Gamma = (\mathsf{B}\ \mathcal{T})$ 建立在 (P, A) 上，且依赖于过去 相对于 $\mathcal{M}$，则 $(\varphi \supset B)$ 中的每个 $\varphi \in \mathcal{T}$ 都相对于 $\mathcal{M}$依赖于过去。

例 5. 对于例 3(a)，$\mathsf{K}_a \neg(\mathsf{q}_1 \wedge \neg\mathsf{q}_2)$ 和 $\mathsf{K}_a \neg(\neg\mathsf{q}_1 \wedge \mathsf{q}_2)$ 均不相对于 $\{M_{vs,0}, M_{vs,1}\}$依赖于过去。特别地，$T_0(M_{vs},0) = \emptyset = T_0(M_{vs},1)$ 且 $S_0(M_{vs},0) = \{\mathsf{s}_0\} = S_0(M_{vs},1)$，但 $M_{vs},0, \mathsf{s}_0 \models \mathsf{K}_a \neg(\mathsf{q}_1 \wedge \neg\mathsf{q}_2)$ 和 $M_{vs},1, \mathsf{s}_0 \not\models \mathsf{K}_a \neg(\mathsf{q}_1 \wedge \neg\mathsf{q}_2)$。对于例 3(b) 也类似，这两个公式不相对于 $\{M_{vsb,0}, M_{vsb,1}, M_{vsb,2}, M_{vsb,3}\}$依赖于过去，但它们相对于 $\{M_{vsb,1}, M_{vsb,2},$依赖于过去 $M_{vsb,\ 3}\}$。 □

当且仅当一个认知守卫转移系统 Γ 相对于其所有解都依赖于过去时，该系统至多有一个解。由于对过去的依赖，所有解的连续可达转移关系 $T_k(M)$，即它们的过去，彼此一致。

命题 1。设 $\Gamma = (\mathsf{B}\ \mathcal{T})$ 是一个在Σ上的认知守卫转移系统。那么，当且仅当存在一个 $\mathcal{M} \subseteq \mathscr{M}_\Sigma(\mathsf{B})$，使得$\{M \in \mathscr{M}_\Sigma(\mathsf{B}) \mid \Gamma^M = M\} \subseteq \mathcal{M}$，且 Γ 相对于 $\mathcal{M}$ 依赖于过去时，Γ 至多有一个解。

为了通过执行获得 Γ 的一个解，系统会被反复解释，以构造近似值 $(M_k)_{0 \le k}$，其中 $M_{k+1} = \Gamma^{M_k}$ 对于 $k \ge -1$，从某个 M_{-1} 开始。每个满足 $k \ge 0$ 的近似值 M_k 都贡献一个转移关系 $T_k(M_k)$，这些转移关系可以组合成一个极限 M_ω。如果 Γ 相对于用于构造近似值且也包含该极限的认知转移结构班级依赖于过去，那么对极限 M_ω 的解释会产生一个不动点。

命题 *2.* 设 $\Gamma = (B\ \mathcal{T})$ 是关于 Σ 的认知守卫转移系统。设 $\mathcal{M} \subseteq \mathscr{M}_\Sigma(B)$，使得 $\Gamma^M \in \mathcal{M}$ 对每个 $M \in \mathcal{M}$ 以及所有满足 $T_k(M_{k'}) = T_k(M_k)$ 的 $(M_k)_{0 \le k} \subseteq \mathcal{M}$，都有 $(B \bigcup_{0 \le k} T_k(M_k)) \in \mathcal{M}$。设 Γ 关于 $\mathcal{M}$ 和 $M_{-1} \in \mathcal{M}$依赖于过去，且对所有 $i \ge -1$，$M_{i+1} = \Gamma^{M_i}$，并且 $M_\omega = (B \bigcup_{0 \le k} T_k(M_k))$。那么 $\Gamma^{M_\omega} = \Gamma^{\Gamma^{M_\omega}}$。

通过认知见证，可以得到一类全面的认知转移结构的充分判据 $\mathcal{M}$，使得 Γ 相对于 $\mathcal{M}$ 依赖于过去：如果解释某个认知转移结构的某个状态不满足 Γ 的某个知识公式 $\mathsf{K}_a\varphi$，那么该结构的过去中就存在证据说明它为何不满足。形式上，如果对于所有 $k \ge 0$、$s \in S_k(M)$，只要 M，$s \not\models \mathsf{K}_a\varphi$成立，就存在一个 $s' \in S_k(M)$，使得$(s, s') \in E_a$ 且 $M, s' \not\models \varphi$，则结构$M \in \mathscr{M}_{P,\ A}(\mathsf{B})$ 为公式 K，A 提供认知见证。

引理 1. 设 $\Gamma = (\mathsf{B}\ \mathcal{T})$ 是定义在 (P, A)上的认知守卫转移系统，并设 $\mathcal{M} \subseteq \mathscr{M}_{P,A}(S, E, L, S_0)$ 满足：所有 $M \in \mathcal{M}$ 都为 Γ中的所有知识守卫提供认知见证。那么，关于 $\mathcal{M}$，Γ 依赖过去。

反过来，结构$M \in \mathscr{M}_{P,\ A}(S, E, L, S_0)$提供认知见证的充分判据是 M 具有同步性：如果对于所有 $a \in A$ 以及所有可达的 $s_1 \in S_{k_1}(M)$和 $s_2 \in S_{k_2}(M)$，只要$(s_1, s_2) \in E_a$成立，就有 $s_1, s_2 \in S_{\min\{k_1,k_2\}}(M)$。因此，在同步结构中，每个智能体的时间维度和认知维度紧密耦合；智能体既无法访问未来，也无需了解未来。

例*6.* 例2中给出的比特传输问题的解释 M_{bt} 提供了认知见证，但并非同步的：发送方S无法区分在 M_{bt} 深度0处可达的 z_0，与只有在深度1处才可达的 z_1；类似地，接收方R无法区分分别在深度1和2处的 z_1 与 z_3。 □

如果对于每个 $M \in \mathscr{M}_{\Sigma}(\mathsf{B})$，解释 Γ^M 都为 Γ的某些动作守卫中出现的所有知识公式提供认知见证，那么认知守卫转移系统 $\Gamma = (\mathsf{B}\ \mathcal{T})$ 定义在 Σ 之上时提供认知见证；如果每个 Γ^M 都是同步的，那么 Γ就是同步的。此外，若 Γ 是基于轮次的，且所有主体在每一轮都执行某个动作，并在本地记录自己执行过哪些动作，那么从语法上也可以看出 Γ 是同步的（参见 [12, 第 135] 页）。

4 （重新）解释基于知识的程序

Fagin 等人 [11,12] 的研究结果保证了所有同步基于知识的程序都具有唯一的解释；De Haan 等人 [9] 的方法旨在将解释扩展到异步程序，但也为矛盾的或自我实现程序赋予了语义。

避免矛盾或自我实现行为的必要性早已出现在同步编程语言 [5]的设计中：其基本原则是“完美同步”，即程序的任何反应都耗时为零，因此程序针对某个输入所产生的任何输出，都已经与该输入同时存在。由于可以测试信号的存在或缺失，这就要求满足“逻辑一致性”：在一次反应中，一个（非输入）信号存在，当且仅当该信号就在这次反应中被发出。程序既需要具有反应式，即能够产生某种逻辑上一致的信号状态；还需要是确定的，即不会呈现多个这样的状态。例如，在 Esterel [6], 中，程序片段

若信号 S 出现，则不执行任何操作；否则发出信号 S，结束

不是反应式的，而是自相矛盾的：只有在信号 S 未被发出的情况下才会发出信号 S；并且

若信号 S 出现，则发出信号 S；否则不执行任何操作，结束

并非确定的，而是自我实现的：如果发出 S，则 S 会被发出；如果不发出 S，则 S 不会被发出。此类程序可以通过环检测静态分析揭示，正如 Lustre [14], 中所做的那样；或者，对于包含更复杂情形的程序，则可以采用 Berry 针对 Esterel [7]提出的“构造性语义”。在记录每一步所发出内容的“逻辑语义”基础上

进行执行分析，并开展 必须/不能分析：哪些内容必须/不能被发出，哪个分支必须/不能被执行。随后要求能够针对每个信号判定它是否必须存在或不能存在。例如，在并行执行中

[当 S1 出现时，发出 S1，结束]| [当 S1 出现时，接着当 S2 出现时，除此之外
什么也不做，发出 S2，结束，结束]

如果假定 S1 出现而 S2 不出现，则两个信号都可以发出——但没有任何信号必然发出。因此，构造性语义无法判定哪些信号必须出现或不能出现，该程序也就不是构造性的。然而，耐人寻味的是，通过执行恰好可以达到一种一致的信号状态：S1 和 S2 均不出现。

我们将 Berry 的构造性语义方法应用于基于知识的程序。事实上，第一个非反应式 Esterel 程序片段类似于例 3(a) 中描述的变量设置问题，第二个非确定片段直接对应于例 4(d)，而最后的组合片段本质上与例 4(c) 相同。我们首先定义认知转移结构的必然/可能版本，其中包含一个下界（必然）和一个上界（可能）。基于这些结构上认知公式的正向（必然）和负向（不可能）满足关系，我们展示如何解释一个受认知条件保护的转移系统，从而得到另一个认知必然/可能转移结构。为保持统一，我们用公式的否定范式重新表述这一解释，并证明构造性解释始终是单调的，并导出一个最小不动点。对于任何基于知识的程序，该不动点都能可靠地表明哪些执行是必需的、哪些执行是可能的。然而，该不动点不一定是已判定的，可能的情况也可能多于必需的情况。我们证明，同步的程序总能导出已判定不动点。所有步骤的证明均见附录 B。

4.1 认知必然/可能转移结构

在 $\Sigma = (P, A)$ 上的认知必然/可能转移结构 $Y = (S, E, L, S_0, (T_\mu, T_\nu))$由一个认知状态基 $\mathsf{B} = (S, E, L, S_0)$以及两个下 和上转移关系 $T_\mu, T_\nu \subseteq S \times S$给出，其中 $T_\mu \subseteq T_\nu$。特别地， $Y_\mu = (\mathsf{B}\ T_\mu)$ 和 $Y_\nu = (\mathsf{B}\ T_\nu)$ 是在 Σ 上的认知转移结构，其中 $Y_\mu \subseteq Y_\nu$。

认知必然/可能转移结构 Y 中状态 $s \in S_\omega(Y_\nu)$ 处认知公式$\varphi \in \Phi_{P,A}$的正和负满足关系 分别记作$Y, s \models_{\mathrm{p}} \varphi$ 和 $Y, s \models_{\mathrm{n}} \varphi$，定义如下：

$$
\begin{array}{ll}
Y, s \models_{\mathrm{p}} p \iff p \in L(s) & Y, s \models_{\mathrm{n}} p \iff p \notin L(s) \\
Y, s \not\models_{\mathrm{p}} \mathrm{false} & Y, s \models_{\mathrm{n}} \mathrm{false} \\
Y, s \models_{\mathrm{p}} \neg\varphi \iff Y, s \models_{\mathrm{n}} \varphi & Y, s \models_{\mathrm{n}} \neg\varphi \iff Y, s \models_{\mathrm{p}} \varphi \\
Y, s \models_{\mathrm{p}} \varphi_1 \wedge \varphi_2 \iff & Y, s \models_{\mathrm{n}} \varphi_1 \wedge \varphi_2 \iff \\
\quad Y, s \models_{\mathrm{p}} \varphi_1 \text{ and } Y, s \models_{\mathrm{p}} \varphi_2 & \quad Y, s \models_{\mathrm{n}} \varphi_1 \text{ or } Y, s \models_{\mathrm{n}} \varphi_2 \\
Y, s \models_{\mathrm{p}} \mathsf{K}_a \varphi \iff Y, s' \models_{\mathrm{p}} \varphi & Y, s \models_{\mathrm{n}} \mathsf{K}_a \varphi \iff Y, s' \models_{\mathrm{n}} \varphi \\
\quad \text{for all } s' \in S_\omega(Y_\nu) & \quad \text{for some } s' \in S_\omega(Y_\mu) \\
\quad \text{with } (s, s') \in E_a & \quad \text{with } (s, s') \in E_a
\end{array}
$$

如果在可能行为的上界 Y_ν 下，公式在 Y 上必然为真，则称其为正向满足；如果在必要行为的下界 Y_μ 下，公式不可能为真，则称其为负向满足。事实上，必然为真的内容也可能为真：

引理 2。 设 $Y=(S,\ E,\ L,\ S_0,\ (T_\mu,\ T_\nu))$ 是一个定义在 $(P,\ A)$ 上的认知必然/可能迁移结构，且 $\varphi\in\Phi_{P,\ A}$。那么对于所有 $s\in S_\omega(Y_\nu),\ Y,\ s\models_{\mathrm{p}}\varphi$，均有 $Y,\ s\not\models_{\mathrm{n}}\varphi$。

在 Σ 上的认知必然/可能转移结构集合以及认知状态基 B 记作 $\mathscr{Y}_\Sigma$(B)。如果对于 $Y_1,\ Y_2\in\mathscr{Y}_\Sigma$(B) 满足 $Y_1\sqsubseteq Y_2$，我们称 $Y_{1,\ \mu}\subseteq Y_{2,\ \mu}$并且 $Y_{1,\ \nu}\supseteq Y_{2,\ \nu}$：扩展会提高下界并降低上界。

与认知转移结构一样，$\Gamma=(S,E,L,S_0,\mathcal{T})$ 上的认知守卫转移系统在 (P,A) 上可以解释为认知必然/可能转移结构 $Y\in\mathscr{Y}_{P,\ A}(S,E,L,S_0)$：守卫动作 $(\varphi\supset B)$ 相对于 Y 的解释由一对 $(\varphi\supset B)^Y=((\varphi\supset B)^{Y,\ \mu},(\varphi\supset B)^{Y,\ \nu})$ 给出，其中

$$(\varphi\supset B)^{Y,\mu}=\{(s,s')\in B\mid s\in S_\omega(Y_\mu)\text{ and }Y,s\models_{\mathrm{p}}\varphi\},$$
$$(\varphi\supset B)^{Y,\nu}=\{(s,s')\in B\mid s\in S_\omega(Y_\nu)\text{ and }Y,s\not\models_{\mathrm{n}}\varphi\}.$$

根据引理 2，对每个 $\tau\in\mathcal{T}$，都有 $\tau^{Y,\mu}\subseteq\tau^{Y,\nu}$。$\Gamma$ 相对于 Y 的构造性解释 由认知必然/可能转移结构给出

$$\Gamma^Y=(S,E,L,S_0,(\bigcup_{\tau\in\mathcal{T}}\tau^{Y,\mu},\bigcup_{\tau\in\mathcal{T}}\tau^{Y,\nu}))\,.$$

这是良定义的，即 $(\Gamma^Y)_\mu\subseteq(\Gamma^Y)_\nu$。如果$\Gamma^Y=Y$，我们称 Y为 Γ的构造性解；若满足 $Y_\mu=Y_\nu$，则构造性解是已判定 的。

与认知转移结构的情形一样，这种对认知必然/可能迁移结构的解释可以迭代，最终达到稳定结构——而这次解释是单调的。

例 7. (a) 重新考虑例 3(b) 中的破坏变量赋值问题。我们从 $Y_{vsb,0}=(\mathrm{B}_{vs},(\emptyset,S^2_{vs}))$ 开始进行解释，并依次得到以下认知必然/可能转移结构：

τ	$\tau^{Y_{vsb,0}}$	$\tau^{Y_{vsb,1}}$	$\tau^{Y_{vsb,2}}$	$\tau^{Y_{vsb,3}}$
$\mathrm{K_a}\neg(\mathrm{q}_1\wedge\neg\mathrm{q}_2)\ \supset\{(\mathrm{s}_0,\mathrm{s}_1)\}$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
	$\{(\mathrm{s}_0,\mathrm{s}_1)\}$	$\emptyset$	$\emptyset$	$\emptyset$
真 $\supset\{(\mathrm{s}_0,\mathrm{s}_2)\}$	$\{(\mathrm{s}_0,\mathrm{s}_2)\}$	$\{(\mathrm{s}_0,\mathrm{s}_2)\}$	$\{(\mathrm{s}_0,\mathrm{s}_2)\}$	$\{(\mathrm{s}_0,\mathrm{s}_2)\}$
	$\{(\mathrm{s}_0,\mathrm{s}_2)\}$	$\{(\mathrm{s}_0,\mathrm{s}_2)\}$	$\{(\mathrm{s}_0,\mathrm{s}_2)\}$	$\{(\mathrm{s}_0,\mathrm{s}_2)\}$
$\mathrm{K_a}\neg(\neg\mathrm{q}_1\wedge\mathrm{q}_2)\ \supset\{(\mathrm{s}_0,\mathrm{s}_3)\}$	$\emptyset$	$\emptyset$	$\{(\mathrm{s}_0,\mathrm{s}_3)\}$	$\{(\mathrm{s}_0,\mathrm{s}_3)\}$
	$\{(\mathrm{s}_0,\mathrm{s}_3)\}$	$\{(\mathrm{s}_0,\mathrm{s}_3)\}$	$\{(\mathrm{s}_0,\mathrm{s}_3)\}$	$\{(\mathrm{s}_0,\mathrm{s}_3)\}$

不仅 $\Gamma_{vsb}{}^{Y_{vsb,\ 3}}=Y_{vsb,\ 3}$ 成立，而且这些解释确实相对于 $\sqsubseteq$ 单调演化。此外，结构 $Y_{vsb,\ 3}$ 已判定，所有可能发生的事情也必然发生，即 $(Y_{vsb,\ 3})_\mu=(Y_{vsb,\ 3})_\nu$。

(b) 对于循环变量赋值问题，参见例 1(b) 和例 3(a)，解释过程是单调的，但只能得到

τ	$\tau^{Y_{vs,0}}$	$\tau^{Y_{vs,1}}$
$\mathrm{K_a}\neg(\mathrm{q}_1\wedge\neg\mathrm{q}_2)\ \supset\{(\mathrm{s}_0,\mathrm{s}_1)\}$	$(\emptyset,\{(\mathrm{s}_0,\mathrm{s}_1)\})$	$(\emptyset,\{(\mathrm{s}_0,\mathrm{s}_1)\})$
$\mathrm{K_a}\neg(\neg\mathrm{q}_1\wedge\mathrm{q}_2)\ \supset\{(\mathrm{s}_0,\mathrm{s}_2)\}$	$(\emptyset,\{(\mathrm{s}_0,\mathrm{s}_2)\})$	$(\emptyset,\{(\mathrm{s}_0,\mathrm{s}_2)\})$

认知必然/可能转移结构 $Y_{vs,\ 1}$ 未被判定，而且确实， Γ_{vs} 有两个以认知转移结构表示的解。然而，例 4(c) 中的非构造性 Γ_{nc} 同样存在这种未判定性；也就是说，构造性解释同样遗漏了唯一解。

□

4.2 构造性解释

在认知 must/can 转移结构 $Y \in \mathscr{Y}_{P,A}(S, E, L, S_0)$ 上，分离的正向（必须）和负向（不能）满足关系可以合并为一个统一的满足关系，而这一关系依赖于认知公式的否定范式，其中否定只出现在命题之前。对于任意 $\varphi \in \Phi_{P,A}$，都存在一个与之等价的否定范式 $\mathrm{nnf}(\varphi) \in \Phi_{P,A}$，使得，特别是

$$\begin{aligned} &\mathrm{nnf}(\neg p) = \neg p && \mathrm{nnf}(\neg\neg\varphi) = \mathrm{nnf}(\varphi) \\ &\mathrm{nnf}(\neg\mathrm{false}) = \mathrm{true} && \mathrm{nnf}(\neg(\varphi_1 \wedge \varphi_2)) = \mathrm{nnf}(\neg\varphi_1) \vee \mathrm{nnf}(\neg\varphi_2) \\ & && \mathrm{nnf}(\neg \mathsf{K}_a\, \varphi) = \mathsf{M}_a\, \mathrm{nnf}(\neg\varphi) \end{aligned}$$

对于处于否定范式的状态 $s \in S_\omega(Y_\nu)$ 和认知公式 $\varphi \in \Phi_{P,A}$，其构造性满足关系 $Y, s \models \varphi$ 的定义与任意认知公式的定义相同，但对 K_a 的全称量词使用上界 Y_ν，对 M_a 的存在量词使用下界 Y_μ；特别是，

$$\begin{aligned} &Y, s \models \neg p \iff p \notin L(s) \\ &Y, s \models \mathsf{K}_a\, \varphi \iff Y, s' \models \varphi \text{ f. a. } s' \in S_\omega(Y_\nu) \text{ with } (s, s') \in E_a \\ &Y, s \models \mathsf{M}_a\, \varphi \iff \text{ex. } s' \in S_\omega(Y_\mu) \text{ s. t. } (s, s') \in E_a \text{ and } Y, s' \models \varphi \end{aligned}$$

构造性满足关系确实结合了 $\models_{\mathrm{p}}$ 和 $\models_{\mathrm{n}}$:

引理 3。令 $Y \in \mathscr{Y}_{P,\ A}(S,\ E,\ L,\ S_0)$、$\varphi \in \Phi_{P,\ A}$ 以及 $s \in S_\omega(Y_\nu)$。则 $Y,\ s \models_{\mathrm{p}} \varphi$ 当且仅当 $Y,\ s \models$ 否定范式(φ)，并且 $Y,\ s \models_{\mathrm{n}} \varphi$ 当且仅当 $Y,\ s \models$ 否定范式$(\neg\varphi)$。

由此可知，如果 $Y_\mu = Y_\nu$，那么 $Y\, s \models \varphi$ 当且仅当 $Y_\mu\, s \models \varphi$，或者等价地，$Y_\nu\ s \models \varphi$。我们还可以得到，在扩展认知必然/可能转移结构时，构造性满足保持不变:

引理 4。令 $Y,\ Y' \in \mathscr{Y}_{P,\ A}(S,\ E,\ L,\ S_0)$，其中 $Y \sqsubseteq Y'$，并令 $\varphi \in \Phi_{P,\ A}$。则 $Y,\ s \models$ 否定范式(φ) 蕴含 $Y',\ s \models$ 否定范式(φ)，对所有 $s \in S_\omega(Y'_\nu)$ 均成立。

这种满足关系的保持性表明，构造性解释是单调的。

命题 3。设 $\Gamma = (S,\ E,\ L,\ S_0,\ \mathcal{T})$ 是定义在 $(P,\ A)$ 上的认知守卫转移系统，并且 $Y,\ Y' \in \mathscr{Y}_{P,\ A}(S,\ E,\ L,\ S_0)$ 满足 $Y \sqsubseteq Y'$。则 $\Gamma^Y \sqsubseteq \Gamma^{Y'}$。

最后，我们可以观察到，对于带有序关系 $\sqsubseteq$ 的 $\mathscr{Y}_\Sigma(\mathrm{B})$，其中 $\mathrm{B} = (S, E, L, S_0)$，它构成一个归纳偏序：每个有向子集 $\Delta \subseteq \mathscr{Y}_\Sigma(\mathrm{B})$ 都有一个关于 $\sqsubseteq$ 的最小上界 $\bigsqcup \Delta$。这里，有向表示任意两个 $Y_1, Y_2 \in \Delta$ 都有一个上界 $Y \in \Delta$，使得 $Y_1 \sqsubseteq Y$ 和 $Y_2 \sqsubseteq Y$；此外，还存在一个底部或最小元素 $\bot_{\Sigma,\ \mathrm{B}} = (S, E, L, S_0, (\emptyset, S \times S)) \in \mathscr{Y}_\Sigma(\mathrm{B})$。

命题 4。 $(\mathscr{Y}_\Sigma(\mathsf{B}) \sqsubseteq, \bot_{\Sigma,\mathsf{B}})$ 是一个归纳偏序。

Pataraia 不动点定理 [8, §8.22] 现在保证，对于每个认知守卫转移系统 $\Gamma = (\mathsf{B}\ \mathcal{T})$，单调算子 $Y \mapsto \Gamma^Y$ 在该归纳偏序中存在一个最小不动点。它可以通过对 $\bot_{\Sigma,\mathsf{B}}$ 反复应用构造性解释来计算，且迭代次数可能是超限的；也就是说，$Y_0 = \bot_{\Sigma,\mathsf{B}}$，$Y_{\alpha+1} = \Gamma^{Y_\alpha}$，其中 $\alpha+1$ 是一个后继序数，并持续迭代 $Y_\lambda = \bigsqcup_{\alpha<\lambda} Y_\alpha$，直到相等 [8, Exc. 8.19]。与第 3.3 节的迭代语义相比，计算构造性语义时无需记录所有先前的近似值来寻找重复。

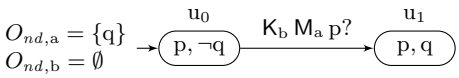
4.3（未）判定的构造性不动点

如果任何具有 $Y \in \mathscr{Y}_\Sigma(\mathsf{B})$ 的构造性不动点 $Y = \Gamma^Y$ 是已判定的，那么就存在以认知转移结构表述的解 $Y_\mu = \Gamma^{Y_\mu} = \Gamma^{Y_\nu} = Y_\nu$，且 Γ 并不矛盾。即使它未被判定，必然／可能结构 $Y_{\mu\mu} = (\mathsf{B}, (T(Y_\mu)\ T(Y_\mu))) \in \mathscr{Y}_\Sigma(\mathsf{B})$ 和 $Y_{\nu\nu} = (\mathsf{B}, (T(Y_\nu)\ T(Y_\nu))) \in \mathscr{Y}_\Sigma(\mathsf{B})$ 也满足 $Y \sqsubseteq Y_{\mu\mu}$ 和 $Y \sqsubseteq Y_{\nu\nu}$，因此根据命题 3 可得 $Y = \Gamma^Y \sqsubseteq \Gamma^{Y_{\mu\mu}}$、$\Gamma^{Y_{\nu\nu}}$，从而得到 $Y_\mu \subseteq \Gamma^{Y_\mu}$ 和 $\Gamma^{Y_\nu} \subseteq Y_\nu$，但一般并不相等。对于最小构造性不动点 $\mu\Gamma$，任何解 $M = \Gamma^M$ 因而都满足 $(\mu\Gamma)_\mu \subseteq M \subseteq (\mu\Gamma)_\nu$，这始终给出可靠的下界和上界；并且，如果 $\mu\Gamma$ 是已判定的，还具有唯一可解性：

命题 5. 设 $\Gamma = (\mathsf{B}\ \mathcal{T})$ 是定义在 Σ 上的认知守卫迁移系统，且 $\mu\Gamma \in \mathscr{Y}_\Sigma(\mathsf{B})$ 已判定。那么 Γ 在 $\mathscr{M}_\Sigma(\mathsf{B})$ 中有唯一解。

然而，即使对于能够提供认知见证的认知守卫迁移系统，也不能保证最小构造性不动点是已判定的：

例 *8.* 考虑如下定义在 $\Sigma_{nd} = (P_{nd}, A_{nd})$ 上的认知守卫迁移系统 $\Gamma_{nd} = (\mathsf{B}_{nd}, \mathcal{T}_{nd})$，其中包含 $P_{nd} = \{\mathsf{p}, \mathsf{q}\}$ 和 $A_{nd} = \{\mathsf{a}, \mathsf{b}\}$：



构造性解释得出非已判定的不动点 Y_{nd}，其中 $T(Y_{nd},\mu) = \emptyset$ 和 $T(Y_{nd},\nu) = \{(\mathrm{u}_0, \mathrm{u}_1)\}$，因为 $Y_{nd}, \mathrm{u}_0 \not\models \mathsf{K}_\mathrm{b}\mathsf{M}_\mathrm{a}\mathrm{p}$，但同时也有 $Y_{nd}, \mathrm{u}_0 \not\models \mathsf{M}_\mathrm{b}\mathsf{K}_\mathrm{a}\neg\mathrm{p}$：状态 u_0 和 u_1 可由智能体 a 区分，而智能体 b 无法判断是否发生过一步转移。在 u_0 中，公式 $\mathsf{M}_\mathrm{a}\,\mathrm{p}$ 相对于 Y_{nd} 成立，但在 u_1，中不成立，因为 $(\mathrm{u}_1,\mathrm{u}_0) \notin E_{nd,a_\circ}$ 另一方面，Γ_{nd} 以病态的方式提供认知见证，因为对于任意 $M \in \mathscr{M}_{\Sigma_{nd}}(\mathsf{B}_{nd})$ 和任意 $s \in S_\omega({\Gamma_{nd}}^M)$，都有 ${\Gamma_{nd}}^M, s \models \mathsf{K}_\mathrm{b}\mathsf{M}_\mathrm{a}\mathrm{p}$，因此有唯一解释；在此情形下，该解释为 ${\Gamma_{nd}}^{Y_{nd},\mu} = Y_{nd,\nu} = {\Gamma_{nd}}^{Y_{nd},\nu}$。 □

然而，对于同步认知守卫转换系统，最小不动点是已判定的，因为所有知识都指向必定已经发生的过去：

引理 5. 设 $\Gamma = (\mathsf{B}\ \mathcal{T})$ 是在 (P, A) 上的一个同步认知守卫转移系统。设 $Y \in \mathscr{Y}_{P,A}(\mathsf{B})$ 满足 $\Gamma^Y = Y$。那么 Y 已判定。

总而言之，用于解释基于知识的程序的构造性方法涵盖了同步程序的解，并提供了一种可靠的过程，可为同步和异步基于知识的程序的执行求得下界和上界。然而，这种方法并不完备：如果最小构造性不动点 $\mu\Gamma$ 未被判定，那么系统 Γ 可能自相矛盾而无解（见例 3(a)），也可能是自我实现的而有多个解（见例 4(d)），或者可能存在一个以认知转移结构表示的唯一解（见例 4(c)）。一种自然而然的策略是进一步分析 Γ，检查使用最小不动点下界 $\mu\Gamma^{\mu}$ 的解释是否满足 $\Gamma_{(\mu\Gamma)^{\mu}} = (\mu\Gamma)_{\nu} = \Gamma_{(\mu\Gamma)^{\nu}}$；这意味着，按照必然发生的情况执行时，所有可能发生的情况都已被涵盖（见例 8）。另一种选择——不过，这会为任何基于知识的程序赋予含义——是重新解释每个守卫动作 $\varphi \supset B$，使其对整体语义的贡献为 $\{(s, s') \mid s \in S_{\omega}((\mu\Gamma)_{\nu})$ 和 $\mu\Gamma, s \models$ 否定范式$(\varphi)\}$。

5 基于知识的程序作为规则系统

认知守卫转移系统 Γ 的“执行”可以表示为两个相互依赖的归纳规则系统的推导，这与归纳定义 [1,15]中的做法类似。其中一个规则系统定义 Γ中的可达性，另一个定义在 Γ上关于否定范式中的知识公式的满足关系。当 Γ 提供认知见证时，可以根据执行的深度对可达性规则系统进行分层，从而解决这种相互依赖关系。在一般情况下，公式满足关系系统对可达性系统的非单调依赖——可达的状态越多，所知信息反而越少——可以通过扩展规则系统的概念，使其同时包含负前提来缓解：如果某条规则的所有（正）前提均可导，但其负前提均不可导，则该规则的结论可导。应用于知识公式时，负前提表示不存在可达的反例。

5.1 归纳规则系统

一个归纳规则系统 R由以下形式的规则 X/y组成，其中前提 $X \subseteq U$和结论 $y \in U$ 取自某个全集的判断 U；规则 X/y的解释是：“如果所有 X 都可以推导出，则 y 可以推导出”。 R中的推导及其前提集合和结论归纳定义如下：

– $y \in U$ 本身就是一个推导；其前提集合为 $\{y\}$，其结论为 y；– 如果 $X/y \in R$ 且（d_x）$_{x\in X}$ 是一族结论为（x）$_{x\in X}$的推导，那么（d_x）$_{x\in X}/y$ 是一个推导；其前提集合是（d_x）$_{x\in X}$中各推导的前提集合之并，其结论为 y。

如果存在一个 R 中的推导，其前提为空集且结论为 y，则称 $y \in U$ 在 R 中是可导的。 R 的可推导结论集合与 $\mu\hat{}R$的不动点$R\hat{}$的最小不动点相重合： $\wp U \to \wp U$由$R(P) = \{y \in U \mid$ ex. $X/y \in R$ s. t. $X \subseteq P\}$定义。

为了将知识公式在认知守卫转换系统 $\Gamma = (S, E, L, S_0, \mathcal{T})$（基于 (P, A)）中的可达性和满足关系表示为归纳规则

系统，我们使用两种判断：一种形式为 $s \in^{\Gamma} S_\omega$ with $s \in S$，表示“状态 s 在 Γ 中可达”；另一种形式为 $s \models^{\Gamma} \varphi$ with $s \in S$ and $\varphi \in \Phi_{P,\,A}$（处于否定范式），表示“状态 s 在 Γ 中满足公式 φ”。可达性的规则如下：

$$\frac{}{s_0 \in^{\Gamma} S_\omega} \text{ if } s_0 \in S_0 \qquad \frac{s \in^{\Gamma} S_\omega}{s' \in^{\Gamma} S_\omega} \begin{array}{l}\text{if ex. } (\varphi \supset B) \in \mathcal{T},\\ (s, s') \in B, \text{ and } s \models^{\Gamma} \varphi\end{array}$$

其中，第二条规则的侧条件 $s \models^{\Gamma} \varphi$ 要求该判断在满足关系的规则系统中是可导的。该系统的规则如下：

$$\frac{}{s \models^{\Gamma} \text{true}} \text{ if } s \in^{\Gamma} S_\omega \qquad \frac{}{s \models^{\Gamma} p} \begin{array}{l}\text{if } s \in^{\Gamma} S_\omega,\\ p \in L(s)\end{array} \qquad \frac{}{s \models^{\Gamma} \neg p} \begin{array}{l}\text{if } s \in^{\Gamma} S_\omega,\\ p \notin L(s)\end{array}$$

$$\frac{s \models^{\Gamma} \varphi_1 \quad s \models^{\Gamma} \varphi_2}{s \models^{\Gamma} \varphi_1 \wedge \varphi_2} \qquad \frac{s \models^{\Gamma} \varphi_1}{s \models^{\Gamma} \varphi_1 \vee \varphi_2} \qquad \frac{s \models^{\Gamma} \varphi_2}{s \models^{\Gamma} \varphi_1 \vee \varphi_2}$$

$$\frac{s' \models^{\Gamma} \varphi}{s \models^{\Gamma} \mathsf{M}_a \varphi} \begin{array}{l}\text{if } (s, s') \in E_a,\\ s' \in^{\Gamma} S_\omega\end{array} \qquad \frac{(s' \models_{\Gamma} \varphi)_{s' \in^{\Gamma} S_\omega,\, (s,s') \in E_a}}{s \models^{\Gamma} \mathsf{K}_a \varphi}$$

这里，事实上，满足关系的最后一条规则对于可达性而言并非单调：为了推导出 $s \models^{\Gamma} \mathrm{K}_a \varphi$，不必对所有满足 $(s, s') \in E_a$ 的 s' 都推导出 $s' \models^{\Gamma} \varphi$，只需对能够推导出 $s' \in^{\Gamma} S_\omega$ 的那些对象推导即可——当然，也包括所有这些对象。

提供认知见证这一概念使我们能够根据相关深度 $k \geq 0$ 对归纳规则系统进行分层：我们将判断 $s \in^{\Gamma} S_\omega$特化为 $s \in^{\Gamma} S_k$，意为“状态 s 可在 Γ 中经至多 k 步到达”；类似地，将判断 $s \models^{\Gamma} \varphi$ 特化为 $s \models^{\Gamma}_k \varphi$，意为“公式 φ 在 Γ 的状态 s 下满足关系成立，其中考虑的是经至多 k 步可达的状态”。对所有$k \geq 0$，可达性的规则如下：

$$\frac{}{s_0 \in^{\Gamma} S_k} \text{ if } s_0 \in^{\Gamma} S_0 \qquad \frac{s \in^{\Gamma} S_k}{s' \in^{\Gamma} S_{k+1}} \begin{array}{l}\text{if ex. } (\varphi \supset B) \in \mathcal{T},\\ (s, s') \in B, \text{ and } s \models^{\Gamma}_k \varphi\end{array}$$

Ana类似地，满足关系的规则对所有 $k \geq 0$:

$$\frac{}{s \models^{\Gamma}_k \text{true}} \text{ if } s \in^{\Gamma} S_k \qquad \frac{}{s \models^{\Gamma}_k p} \begin{array}{l}\text{if } s \in^{\Gamma} S_k,\\ p \in L(s)\end{array} \qquad \frac{}{s \models^{\Gamma}_k \neg p} \begin{array}{l}\text{if } s \in^{\Gamma} S_k,\\ p \notin L(s)\end{array}$$

$$\frac{s \models^{\Gamma}_k \varphi_1 \quad s \models^{\Gamma}_k \varphi_2}{s \models^{\Gamma}_k \varphi_1 \wedge \varphi_2} \qquad \frac{s \models^{\Gamma}_k \varphi_1}{s \models^{\Gamma}_k \varphi_1 \vee \varphi_2} \qquad \frac{s \models^{\Gamma}_k \varphi_2}{s \models^{\Gamma}_k \varphi_1 \vee \varphi_2}$$

$$\frac{s' \models^{\Gamma}_k \varphi}{s \models^{\Gamma}_k \mathsf{M}_a \varphi} \begin{array}{l}\text{if } (s, s') \in E_a,\\ s' \in^{\Gamma} S_k\end{array} \qquad \frac{(s' \models^{\Gamma}_k \varphi)_{s' \in^{\Gamma} S_k,\, (s,s') \in E_a}}{s \models^{\Gamma}_k \mathsf{K}_a \varphi}$$

特别地，$s \models^{\Gamma}_k \mathrm{M}_a \varphi$和 $s \models^{\Gamma}_k \mathrm{K}_a \varphi$的规则对于提供认知见证的认知守卫转移系统是可靠的。

“提供认知见证”这一概念要求：如果 $\mathrm{K}_a \varphi$ 在可达性深度 k处不成立，则存在一个反例，表明 φ 在可达性深度 $\leq k$处不成立。

一般情况可以通过取消深度要求，并考虑到以下事实来涵盖：当且仅当存在某个可达且与 a不可区分的状态 s'，使得 φ 不成立时，$\mathsf{K}_a\,\varphi$ 才不会在某个状态 s 上成立。因此，为了推导出 $\mathsf{K}_a\,\varphi$ 确实在某个可达状态 s上成立，必要且充分的条件是证明：不 可能推导出 $\neg\varphi$ 在某个可达且与 a不可区分的状态 s'上成立。

5.2 含正前提和负前提的一般规则系统

为用规则系统表达负信息，我们在规则的正前提之外补充负前提：考虑定义在全集 U 上的一般规则系统规则系统 R，其由形如 $(X, \not\in Z)/y$ 的规则组成，其中 $X, Z \subseteq U$ 分别是正前提和负前提，而 $y \in U$ 是结论；其含义是 “ 如果可以推导出所有 X，但无法推导出任何 Z，那么就可以推导出 y”。R 中的推导，以及它们的正前提集和负前提集 与结论，同样归纳定义如下：

– $y \in U$ 本身就是一个推导；其正前提集为 $\{y\}$，负前提集为 $\emptyset$，结论为 y；– 若 $(X, \not\in Z)/y \in R$ 且 $(d_x)_{x\in X}$ 是一族结论为 $(x)_{x\in X}$ 的推导，则 $((d_x)_{x\in X}, \not\in Z)/y$ 是一个推导；其正前提集是 $(d_x)_{x\in X}$ 的正前提集的并集，负前提集是 $(d_x)_{x\in X}$ 的负前提集与 Z 的并集，结论为 y。

¯对于一个 $B \subseteq U$，令 $R(B)$表示所有满足以下条件的 $y \in U$：在 B中，存在一个 R 内针对 y 的推导，其正前提集合为空，且没有负前提。R 的可导的¯结论集合由 R 的最小不动点给出（如果该不动点存在）。

借助这种广义的规则系统概念，我们可以通过使用单个判断 $s \models^{\Gamma}_{\omega} \varphi$，重新表述并合并认知守卫转移系统 $\Gamma = (S, E, L, S_0, \mathcal{T})$中关于可达性和满足关系的两个推理系统。该系统定义在(P, A)上，而这个判断表示“状态s 在 Γ中满足 φ，且状态 s 在 Γ中可达”。因此，负前提 $\not\in(s \models^{\Gamma}_{\omega} \mathsf{true})$表示“无法推导出$s \in^{\Gamma} S_\omega$ ”。包含负前提的新规则如下：

$$\frac{}{s_0 \models^{\Gamma}_{\omega} \mathrm{true}}\ \text{if } s_0 \in S_0 \qquad \frac{s \models^{\Gamma}_{\omega} \varphi}{s' \models^{\Gamma}_{\omega} \mathrm{true}}\ \begin{array}{l}\text{if ex. } (\varphi \supset B) \in \mathcal{T},\\ (s, s') \in B\end{array}$$

$$\frac{s \models^{\Gamma}_{\omega} \mathrm{true}}{s \models^{\Gamma}_{\omega} p}\ \text{if } p \in L(s) \qquad \frac{s \models^{\Gamma}_{\omega} \mathrm{true}}{s \models^{\Gamma}_{\omega} \neg p}\ \text{if } p \notin L(s)$$

$$\frac{s \models^{\Gamma}_{\omega} \varphi_1 \quad s \models^{\Gamma}_{\omega} \varphi_2}{s \models^{\Gamma}_{\omega} \varphi_1 \wedge \varphi_2} \qquad \frac{s \models^{\Gamma}_{\omega} \varphi_1}{s \models^{\Gamma}_{\omega} \varphi_1 \vee \varphi_2} \qquad \frac{s \models^{\Gamma}_{\omega} \varphi_2}{s \models^{\Gamma}_{\omega} \varphi_1 \vee \varphi_2}$$

$$\frac{s' \models^{\Gamma}_{\omega} \varphi}{s \models^{\Gamma}_{\omega} \mathsf{M}_a\,\varphi}\ \text{if } (s, s') \in E_a \qquad \frac{s \models^{\Gamma}_{\omega} \mathrm{true} \quad \not\in(s' \models^{\Gamma}_{\omega} \mathrm{nnf}(\neg\varphi))_{(s,s')\in E_a}}{s \models^{\Gamma}_{\omega} \mathsf{K}_a\,\varphi}$$

$s \models^{\Gamma}_{\omega} \mathsf{K}_a\,\varphi$ 的规则会检查 s 是否可达，同时检查在任何与 a不可区分的状态下，是否都无法到达 φ 的反例。

借助一般规则系统，认知守卫转移系统的可解性问题可转化为计算可导结论的问题。对于基于知识的程序，

仅凭系统 R 的规则，并不能显而易见地判断是否存在解$_R(B) = B$，也无法判断是否存在最小解。

例 *9.* (a) 该一般规则系统

$$R_0 = \left\{ \frac{x_1}{x_1}, \frac{\not\vdash x_1 \ \not\vdash x_2}{x_2} \right\} \quad \text{over} \quad \{x_1, x_2\}$$

没有可推导结论集，因为 $\bar{R}_0$ 没有不动点；特别是，$\bar{R}_0(\emptyset) = \{x_2\}$ 且 $\bar{R}_0(\{x_1\}) = \emptyset = \bar{R}_0(\{x_2\})$。$R_0$ 还表明，一般规则系统的可推导结论集 R 不一定与算子 R 的最小不动点重合：$\wp U \to \wp U$从归纳规则系统移植而来，此时令 $\hat{}R(P) = \{y \in U \mid \text{ex. } (X, \not\vdash Z)/y \in R \text{s.t. } X \subseteq P, P \cap Z = \emptyset\}$: $\mu \hat{} R_0 = \{x_1\}$。另一方面，鉴于认知守卫转移系统的一般规则系统 R_0 也可以改写为一个只有单个智能体 a 和单个变量 x $\in \{0, 1, 2\}$的基于知识的程序，其中 a 无法观察该变量，且初始时 x $= 0$:

if $\mathsf{M}_\mathrm{a}\,\mathrm{x} = 1 \twoheadrightarrow \mathrm{x} \leftarrow 1$
$[\!]\ \mathsf{K}_\mathrm{a}(\mathrm{x} \neq 1 \wedge \mathrm{x} \neq 2) \twoheadrightarrow \mathrm{x} \leftarrow 2$ **fi**

类似地，仅第二条规则，即一般规则系统

$$R_1 = \left\{ \frac{\not\vdash x_1 \ \not\vdash x_2}{x_2} \right\} \quad \text{over} \quad \{x_1, x_2\}$$

没有任何解，也就是 R_1 的不动点：x_1 不能包含在任何解中，因为它不可导，而 x_2 会导致矛盾。同样的结论也适用于

$$R_2 = \left\{ \frac{\not\vdash x_1}{x_2}, \frac{\not\vdash x_2}{x_3}, \frac{\not\vdash x_3}{x_1} \right\} \quad \text{over} \quad \{x_1, x_2, x_3\}$$

其中，如果 x_2 可导，那么 x_3 就不可导，从而 x_1 可导，这意味着 x_2 不可导——反之亦然；

(b) 一般规则系统可能有多个解，但没有最小解：

$$R_3 = \left\{ \frac{\not\vdash x_1}{x_3}, \frac{\not\vdash x_3}{x_1} \right\} \quad \text{over} \quad \{x_1, x_3\}$$

其解为 $\{x_1\}$ 和 $\{x_3\}$，但 $\emptyset$ 不是解。它对应于引言中的“变量设定”知识程序

if $\mathsf{K}_\mathrm{a}\,\mathrm{x} \neq 1 \twoheadrightarrow \mathrm{x} \leftarrow 3$
$[\!]\ \mathsf{K}_\mathrm{a}\,\mathrm{x} \neq 3 \twoheadrightarrow \mathrm{x} \leftarrow 1$ **fi**

参见例 1(b)。对于具有无限论域和无限多条规则的一般规则系统，考虑

$$R_4 = \left\{ \frac{\not\vdash x_{n+1}}{x_n} \;\middle|\; n \in \mathbb{N} \right\} \quad \text{over} \quad \{x_n \mid n \in \mathbb{N}\}$$

它有不可比较的解 $\{x_{2n} \mid n \in \mathbb{N}\}$ 和 $\{x_{2n+1} \mid n \in \mathbb{N}\}$。

(c) 将显示矛盾规则的规则系统 R_1 与包含非确定性规则的规则系统 R_3 结合起来，我们得到

$$R_5 = \left\{ \frac{\not\vdash x_1}{x_3},\ \frac{\not\vdash x_3}{x_1},\ \frac{\not\vdash x_1 \quad \not\vdash x_2}{x_2} \right\} \quad \text{over} \quad \{x_1, x_2, x_3\}$$

其唯一解为 $\{x_1\}$：如果可以推断出 x_3，即无法推断出 x_1，就会触发针对 x_2 的矛盾规则（参见例 4(c)）。 □

5.3 求解一般规则系统

关于认知必然/可能转移结构和构造性解释的观测与定义，见第 4.2 节；现在可以将其直接推广到对一般规则系统的更抽象描述。对于全集 U，定义集合 $\wp^{\pm}U$ 为 $\{(P,Q) \in \wp U \times \wp U \mid P \subseteq Q\}$，并定义关系 $\subseteq^{\pm} \subseteq \wp^{\pm}U \times \wp^{\pm}U$ 为 $(P,Q) \subseteq^{\pm} (P',Q')$，当且仅当 $P \subseteq P'$ 和 $Q \supseteq Q'$。

引理6。$(\wp^{\pm}U,\ \subseteq^{\pm},\ \bot_U^{\pm})$ 满足 $\bot_U^{\pm} = (\emptyset,\ U)$，是一个归纳偏序。

对于一个带有正前提和负前提、定义在 R 之上的一般规则系统 U，定义算子 $\check{R}: \wp^{\pm}U \to \wp^{\pm}U$，用于描述在假定哪些内容必然可导、哪些内容可能可导的情况下，哪些内容必须 可导以及哪些内容可以 可导：

$$\begin{aligned}\check{R}(P,Q) = (&\{y \in U \mid \text{ex. } (X, \not\vdash Z)/y \in R \text{ s. t. } X \subseteq P,\ Q \cap Z = \emptyset\},\\ &\{y \in U \mid \text{ex. } (X, \not\vdash Z)/y \in R \text{ s. t. } X \subseteq Q,\ P \cap Z = \emptyset\})\end{aligned}$$

这是定义良好的：若 $(P,Q) \in \wp^{\pm}U$，则 $\check{R}(P,Q) \in \wp^{\pm}U$，因为对于 $P \subseteq Q$ 以及满足 $X \subseteq P$ 和 $Q \cap Z = \emptyset$ 的每个 $(X, \not\vdash Z)/y \in R$，都有 $X \subseteq Q$ 和 $P \cap Z = \emptyset$。该算子总是单调的：

引理7. 设 R 是定义在 U 之上的规则系统。若 $(P_1,\ Q_1) \subseteq^{\pm} (P_2,\ Q_2)$，则 $\check{R}(P_1,\ Q_1) \subseteq^{\pm} \check{R}(P_2,\ Q_2)$。

对于构造性解释，Pataraia 不动点定理现在保证，归纳偏序 $(\wp^{\pm}U, \subseteq^{\pm}, \bot_U^{\pm})$ 上的单调算子 $\check{R}$ 存在一个最小不动点。同样，可以通过对 $\bot_U^{\pm}$ 反复应用 $\check{R}$（可能需要超限多次）来“计算”该不动点。然而，如果 $\check{R}$ 还是连续的，那么根据 Kleene不动点定理，只需考虑所有有限近似值，即 $\mu\check{R} = \bigcup_{n\in\mathbb{N}}^{\pm} \check{R}^n(\bot_U^{\pm})$；$\check{R}$ 是连续的，意味着若 $\Delta \subseteq \wp^{\pm}U$ 是有向的，则 $\bigcup^{\pm} \check{R}(\Delta) = \check{R}(\bigcup^{\pm} \Delta)$。

引理 8。设 R 是基于 U 的规则系统，且 R 的每条规则都只包含有限多个 $\check{}$ 正前提和负前提。那么 R 是连续的。

认知守卫转移系统 $\Gamma = (S, E, L, S_0, \mathcal{T})$ 在 (P, A) 上的规则系统始终只显示有限多个正前提；如果对于每个 $s \in S$ 和每个 $a \in A$，集合 $\{s' \in S \mid (s,s') \in E_a\}$ 都是有限的，那么负前提的数量也有限，因此相应的 must/can 算子是连续的。

6 基于知识的程序推理

我们已在原型“时序认知模型解释器和检查器”（tEmIc[3]）中实现了基于知识的程序的构造性解释。该工具首先计算一个（有限状态）认知守卫转移系统的最小构造性不动点。如果最小不动点已判定，则已找到以认知转移结构表示的最小解；否则，将检查使用未判定的最小不动点的下界进行重新解释能否得出一个解。如果其中任一方法成功，就可以检查所得模型的性质。这些性质可以用 CTLK 表达，它结合了分支时序逻辑“计算树逻辑”（CTL）和认知逻辑 [17]。此外，tEmIc 也可将 CTLK 用于动作守卫。构造性解释只需在上界上对 CTL 公式的每个全称量词——A，表示“在所有路径上”——求值，并在下界上对每个存在量词——E，表示“在某条路径上”——求值。这将时间维度纳入了基于知识的程序的应用领域。对于 Fagin 等人 [11], 的基于运行的解释系统，Van der Hoek 和 Woolridge [16] 以及 Su [22] 提供了基于局部命题的线性时间模型检测转换，不过这些转换针对的是固定的一组运行，不会随知识守卫的求值而变化。CTLK模型检查器 MCMAS [17] 同样针对固定的预定模型运行。在动态认知逻辑及其模型检查器 DEMO [26], 中，转移结构由认知动作给出。

我们先简要回顾 CTLK，再展示如何在认知必然/可能转移结构上对其进行构造性求值。接着，我们通过比特传输问题以及“意外考试”这一小型悖论练习来介绍 tEmIc；tEmIc 发行版还包含对著名问题“泥孩问题” [26, 第 93 页及后续页] 和“和与积问题” [26, 第 96 页及后续页]的规范描述。最后，我们将探讨一个应用，其中 CTLK 也用于动作守卫：Java内存模型。

6.1 CTLK

(P, A) 上的 *CTLK* 公式 由以下语法定义：

$$\varphi ::= p \mid \mathrm{false} \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid \mathsf{K}_a\,\varphi \mid \mathsf{EX}\,\varphi \mid \mathsf{EG}\,\varphi \mid \mathsf{E}[\varphi_1\,\mathsf{U}\,\varphi_2]$$

其中 $p \in P$ 和 $a \in A$。路径量词 E 的解释是“存在一条路径”，时序模态 X 表示“下一步”，G 表示“始终”，U 表示“直到”。我们还考虑表示“所有路径”的路径量词 A，以及表示“最终”的模态 F 和表示“释放”的模态 R，使得 $\neg\mathsf{EG}\,\neg\varphi$ 缩写为 $\mathsf{AF}\ \varphi$，而 $\neg\mathsf{E}[\neg\varphi_1\,\mathsf{U}\ \neg\varphi_2]$缩写为 $\mathsf{A}[\varphi_1\,\mathsf{R}\ \varphi_2]$。CTIK 公式 φ 在认知转移结构 $M = (S, E, L, S_0, T)$ 的状态 $s \in S$ 上、相对于 (P, A) 的 满足关系 $M, s \models \varphi$，在 (P, A) 上保守地扩展了认知公式的满足关系：

$$M, s \models \mathsf{EX}\,\varphi \iff \text{ex. } s_0, s_1, \ldots \in \mathscr{P}(M, s) \text{ s. t. } M, s_1 \models \varphi$$
$$M, s \models \mathsf{EG}\,\varphi \iff \text{ex. } s_0, s_1, \ldots \in \mathscr{P}(M, s) \text{ s. t. } M, s_i \models \varphi \text{ f. a. } i \in \mathbb{N}$$

[3] https://www.dropbox.com/s/ofnatog8ualazdh/temic.zip?dl=0

$M, s \models \mathsf{E}[\varphi_1 \,\mathsf{U}\, \varphi_2] \iff$ 存在 $s_0, s_1, \ldots \in \mathscr{P}(M, s)$，并且 $l \in \mathbb{N}$ 使得
$M, s_i \models \varphi_1$ 对于所有 $0 \leq i < l$ 都成立，且 $M, s_l \models \varphi_2$

其中，$\mathscr{P}(M, s)$ 表示 M 的所有路径，即满足 $s_0 = s$ 且对所有 $i \in \mathbb{N}$ 都有 $(s_i, s_{i+1}) \in T$ 的无限状态序列 $s_0, s_1, \ldots \in S$。若 CTLK 公式 φ 在 M 中有效，则记作$M \models \varphi$，也就是说，它在所有初始状态中均成立，即对所有 $s_0 \in S_0(M)$，都有 $M, s_0 \models \varphi$。

要直接定义带有 A 的 CTLK 公式的满足关系，必须将 E 的存在路径量化替换为全称路径量化。与简单认知逻辑一样，CTLK（包括 AX φ、AGφ等）也具有否定范式（参见例如 [3, 第 333 页及后续页]）。在认知必然/可能转移结构 $(S, E, L, S_0, \mathcal{T})$ 上，针对否定范式认知公式的 构造性满足关系，定义在 (P, A) 上的状态 $s \in S_\omega(Y_\nu)$ 处，记作 $Y, s \models \varphi$，保守地扩展了认知公式的构造性满足关系，并将 E 解释为下界 Y_μ，将 A 解释为上界 Y_ν，因此尤其有，

$$Y, s \models \mathsf{EF}\,\varphi \iff \text{ex. } s_0, s_1, \ldots \in \mathscr{P}(Y_\mu, s) \text{ and } i \in \mathbb{N} \text{ s. t. } Y, s_i \models \varphi$$
$$Y, s \models \mathsf{AF}\,\varphi \iff \text{f. a. } s_0, s_1, \ldots \in \mathscr{P}(Y_\nu, s) \text{ ex. } i \in \mathbb{N} \text{ s. t. } Y, s_i \models \varphi$$

如附录 D 所示，此扩展定义良好。

6.2 tEmIc

tEmIc 是一种使用 CTLK 的认知守卫迁移系统符号模型解释器和检验器。它以 Java 编写，并使用二元决策图表示状态空间 [23]；此外，它还支持有界整数及其算术运算。给定一个规范后，tEmIc 首先通过迭代的 must/- can 解释计算最小构造不动点。如果此不动点尚未判定，它会检查使用不动点下界进行另一种解释是否能得到一个解。如果其中任一种方法成功，tEmIc 就会针对给定属性进行模型检验；这些陈述可以指定为必须在所有初始状态中成立的 CTLK 公式，也可以指定为可达性查询。可达的、没有出边状态转换的死锁状态会触发警告。

例如，引言中的比特传输问题（如例 1(a) 中形式化所示）可以表示为如下 tEmIc 规范：

```
var sbit, 确认, rbit, snt : booleaninitial (确认 | rbit | snt) <-> false; 智能体 S
= { sbit, 确认 }; 智能体 R = { rbit, snt }; let R_knows_bit = exists bit:boolean .
K[R] sbit <-> bit; action S_sends_bit_ok guard not K[S] R_knows_bit do rbit :
= sbit, snt :=true; action S_sends_bit_failed guard not K[S] R_knows_bit do ;
action R_sends_ack_ok guard R_knows_bit and not K[R] K[S] R_knows_bit
do 确认 := true; action R_sends_ack_failed guard R_knows_bit and not K[R]
K[S] R_knows_bit do ;
```

构造性解释在几毫秒内即可得出例2的已判定最小不动点，并可据此检查某些CTLK性质：

```
checkinitial EF R_knows_bit；checkinitial EF K[
S] R_knows_bit；checkinitial EF K[R] K[S]
R_knows_bit;
```

据报告，前两个性质成立，但最后一个不成立，因为智能体 R 无法收集足够的信息，确定智能体 S 是否已收到该比特。

再举一个例子，考虑“意外考试”悖论 [9, 第 4.7 节，其中称为“意外绞刑”]（详细介绍请参见，例如 [21, 第 5.2 节及后续各节]）：有人告诉一个班级，下周内将举行一次考试，但考试日期会出人意料。班级可能会推理，考试不可能安排在星期五，因为如果直到星期四都没有考试，那么星期五的考试就不再令人意外；通过逆向归纳，他们可能进一步推理，下周内根本不可能有意外考试。这个问题陈述可以很容易地表示为一个 tEmIc 规范：

```
var day : 0..5 initial day = 0; var 考试 : 0..4; var
written: boolean initial written <-> false;

智能体 P = { day, written };
动作 act1，守卫条件 day < 5 and (day = 考试) and (not K[P] day = 考试)
and not written，执行 written :=true, day := day+1; 动作 act2，守卫条件 day
< 5 and (day != 考试)，执行 day := day+1; 动作 stutter，执行 ;
```

同样，构造性解释只需几毫秒便能得到一个已判定的最小不动点。在这个认知转移结构上，我们可以检查，例如在星期三，考试可以进行，而且确实仍然是一次惊喜：

```
check reachable exam = 2 & written;
```

对于这样的可达性检查，tEmIc 还会提供一个见证，说明 act2 执行两次后，接着执行 act1。然而，以下 CTLK性质并不成立，因为它必须在所有初始状态下都成立——而当考试为 4 时，这个班级就不可能再感到惊讶了：

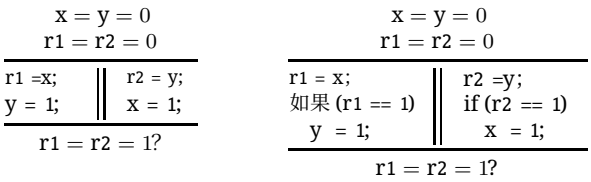
```
check initial EF written;
```

6.3 内存模型

内存模型规范线程、线程的缓存与主存之间的交互 [19]。最初的 Java内存模型——最早的此类形式化模型之一——因使若干编译器优化无法实现而受到严厉批评，随后被一种更宽松的模型所取代 [13, 第 17] 章。在为顺序一致且同步良好的程序保留强保证的同时，对于存在数据竞争的程序，允许对数据无关语句进行重排序，或允许从其他线程进行提前的“预知性”读取。不过，仍应强制执行某些极限，例如与数据或控制流依赖保持一致，以及不允许出现“凭空产生”的值 [20,2]。

例如，在左侧的以下双线程类 Java 程序中，读取全局共享变量 x 和 y 时，两个线程局部寄存器 r1 和 r2 都有可能被赋值为 1：

编译器可以对两个线程中的数据无关语句重新排序。然而，由于右侧示例中存在对称数据依赖，因此应禁止这种行为。



我们希望刻画采用宽松内存模型的多线程（Java）程序的行为，而不必检查所有可能的编译器变换——这些变换的正确性实际上取决于程序语义，包括内存模型。事实上，在当前的 Java内存模型中，乱序执行必须由其他合法执行来证明其合理性。我们将这些证明解释为基于知识的程序意义上的见证；不过，我们目前的阐述忽略了同步。首先，我们用以下 tEmIc 声明来表示上述这类双线程（Java）程序的状态空间：

var x, y, r1, r2 : 0..2 initialx = 0 & y = 0 & r1 = 0 & r2 = 0; var
step1, step2 : 1..3 initialstep1 = 1 & step2 = 1; 智能体 t1 = { step1, r1 };
智能体 t2 = { step2, r2 };

线程代理 t1 和 t2 只能观察自己的局部寄存器和程序计数器。两个线程的程序步骤都被转换为如下形式的动作

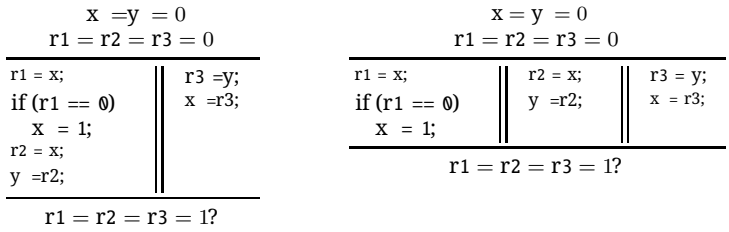
动作 t1_1 guard step1 = 1 do r1 :=x, step1 := step1+1; 动作 t1_2
guard step1 = 2 do y := 1, step1 := step1+1;

此外，我们允许线程 θ 在步骤 s 执行以下动作，将主内存变量 x 的值 v 预知读取到局部变量 r 中：

动作 readθ_x_v_r_$s$guard stepθ = s and K[θ] (EF (r = 0 & x = v) and
EF (r = v & x = v)) do r := v, stepθ := stepθ+1;

如果线程 θ 知道 存在一次执行，其中 x 的值为 v，且不依赖于预先将 r 设置为 v，那么它就可以提前将 v 读入 r；此外，还存在一次执行，可以确认这次提前设置。第一个线程的语句 r1 =x; 被展开为三个读取动作 read1_x_0_r1_1、read1_x_1_r1_1 和 read1_x_2_r1_1，以及普通读取动作 t1_1。通过这种编码，tEmIc 报告称，对于左侧的第一个示例，在最小构造性不动点中确实可以得到 $\mathrm{r1} = \mathrm{r2} = 1$，但对于右侧的示例则不可能。

以下两个示例呈现了一个更耐人寻味的情形：据 Manson等人 [19, 第35页及后续页]（另见 [2]），左侧程序可能导致 $\mathrm{r1} = \mathrm{r2} = \mathrm{r3} = 1$：



编译器可以看出，x 和 y 只可能取 0 和 1，因此“可以将 r2 = x 替换为 r2 = 1，因为要么第 1 行从 x 读出了 1，且期间没有写入操作；要么第 1 行从 x 读出了 0，第 3 行将 1 赋给了 x，且期间没有写入操作”；这种确定赋值可用于将最后一行转换为 y = 1；由于不存在依赖关系，最终还可以将其作为第一个线程的首个操作。但对于右侧程序，同样的转换并不可行，因此应禁止相同的行为。尽管如此，左侧程序正是将第二个线程内联到第一个线程后的结果。我们在 tEmIc 中对这两个程序的编码证实了上述判断；左侧程序的见证确实先将 r3 设为 1，并且直到最后一步将 y 设为 1 时才确认这一点。

7 结论与未来工作

我们提出了一种必然／可能分析，用于解释基于知识的程序，其灵感来自同步编程语言的构造性语义。由此得到的构造性解释为可能的执行提供了下界和上界。我们证明了这种解释具有单调性，并能产生一个最小不动点。我们还将必然／可能方法扩展到带有正前提和负前提的一般规则系统。最后，我们介绍了工具 tEmIc，用于构造性解释以及对 CTLK 的时序—认知模型检测，并展示了知识程序解释的一些应用，包括 CTLK守卫。

我们的认知逻辑可以补充群体知识 [12, Ch. 6],，例如共同知识或分布式知识。时间维度可以扩展到“线性时序逻辑”（LTL），更重要的是，可以纳入某种公平性概念。若能找到除同步性之外，确保必然／可能解释具有已判定最小不动点的判据，将会很有价值。这也适用于一般规则系统的解；将其与非单调归纳定义进行比较（例如，参见 [10],）也值得探讨。另一方面，一般构造性方法或许有助于补充现有的同步编程语言语义的直觉主义方法 [18]。最后，通过解释基于知识的程序，应更全面地涵盖内存模型领域。

参考文献

1. Aczel, P.：归纳定义导论。载于：Barwise, J.（编）《数学逻辑手册》，第 C.7 章，第 783–818 页。North-Holland（1977年）

2. Aspinall, D., Ševčík, J.：Java 内存模型示例：优、劣与丑。载于：《多线程类 Java 程序的验证与分析论文集》（VAMP 2007）（2007） 3. Baier, C., Katoen, J.P.：《模型检验原理》。麻省理工学院出版社（2008） 4. Baltag, A., Moss, L.S.：《认知程序逻辑》。Synth. **139**(2), 165–224（2004）。https://doi.org/10.1023/B:SYNT.0000024912.56773.5e 5. Benveniste, A., Caspi, P., Edwards, S.A., Halbwachs, N., Guernic, P.L., de Simone, R.：十二年后的同步语言。《IEEE 会刊》**91**(1), 64–83（2003） 6. Berry, G.：Esterel 的基础。载于：Plotkin, G., Stirling, C., Tofte, M.（编）《证明、语言与交互：纪念 Robin Milner 文集》，第 425–454 页。计算基础丛书，麻省理工学院出版社（2000） 7. Berry, G.：纯 Esterel 的构造语义，第 3 版草稿（2002），https://www-sop.inria.fr/members/Gerard.Berry/Papers/EsterelConstructiveBook.pdf 8. Davey, B.A., Priestley, H.A.：《格与序导论》。剑桥大学出版社，2nd 版（2002） 9. de Haan, H.W., Hesselink, W.H., de Lavalette, G.R.R.：基于知识的异步编程。《Fund. Inform.》**63**(2-3), 259–281（2004） 10. Denecker, M., Ternovska, E.：非单调归纳定义逻辑。《ACM 计算逻辑汇刊》**9**(2), 14:1–14:52（2008） 11. Fagin, R., Halpern, J.Y., Moses, Y., Vardi, M.Y.：基于知识的程序。《分布式计算》**10**(4), 199–225（1997） 12. Fagin, R., Halpern, J.Y., Moses, Y., Vardi, M.Y.：《关于知识的推理》。麻省理工学院出版社（2003） 13. Gosling, J., Joy, B., Steele, G., Bracha, G.：《Java 语言规范》。Addison-Wesley，3rd 版（2005） 14. Halbwachs, N., Caspi, P., Raymond, P., Pilaud, D.：同步数据流编程语言 Lustre。《IEEE 会刊》**79**(9), 1305–1320（1991） 15. Harper, R.：《编程语言的实践基础》。剑桥大学出版社（2013） 16. van der Hoek, W., Wooldridge, M.J.：知识与时间的模型检验。载于：Bosnacki, D., Leue, S.（编）《软件模型检验国际研讨会论文集》（SPIN 2002）。《计算机科学讲义》，第 2318， 95 111 2002 10 1007 3 540 46017 9_9 卷，第 – 页。17 施普林格（ ）。https://doi.org/ . / - - - . Lomuscio, A., Penczek, W.：时序认知逻辑的模型检验。载于：van Ditmarsch 等人 [24]， 8， 397 441 第 章，第 – 页。Lüttgen, G., 18 Mendler, M.：状态图步骤背后的直觉主义。《ACM 计算逻辑汇刊》**3**504078 19 1 1 41 2002 10 1145 504077 ( ), – ( )。https://doi.org/ . / . . Manson, J., Pugh, W., Adve, S.：Java 内存模型（2005），http://dl.dropbox.com/u/1011627/journal.pdf，草稿 20. Pugh, W.：Java 内存模型（1999–），http://www.cs.umd.edu/~pugh/java/memoryModel/ 21. Sainsbury, R.M.：《悖论》。剑桥大学出版社， 3rd 版（2009） 22. Su, K.：分布式系统中知识时序逻辑的模型检验。载于：McGuiness, D.L., Ferguson, G.（编）《 19th 全国人工智能会议、 16th 人工智能创新应用会议论文集》（AAAI 2004），第 98–103 页。AAAI Press，麻省理工学院出版社（2004） 23. Vahidi, A.：J DD：纯 Java 二元决策图和 Z-BDD 库。https://bitbucket.org/vahidi/jdd（2003） 24. van Ditmarsch, H., Halpern, J.Y., van der Hoek, W., Kooi, B.（编）：《认知逻辑手册》。College Publ.（2015） 25. van Ditmarsch, H., Halpern, J.Y., van der Hoek, W., Kooi, B.：知识与信念逻辑导论。载于：《认知逻辑手册》 [24]， 1， 1 51 第 章，第 – 页。van 26 Ditmarsch, H., van der Hoek, W., Kooi, B.：《动态认知逻辑》，Synthese 丛书，第 337 卷。施普林格（2008）

对过去的依赖与认知见证

引理 A.1. 令 $M_i \in \mathscr{M}_\Sigma(S,\ E,\ L,\ S_0)$ 满足 $1 \le i \le 2$。

1. 若 $T_k(M_1) = T_k(M_2)$ 对某个 $k \ge 0$ 成立，则 $S_k(M_1) = S_k(M_2)$。
2. 对所有 $k \ge 0$，$T_k(M_1) = T_k(M_2)$ 当且仅当 $T_\omega(M_1) = T_\omega(M_2)$。

证明。(1) 对 $k \ge 0$，令 $T_k(M_1) = T_k(M_2)$。若 $k = 0$，则 $T_0(M_1) = \emptyset = T_0(M_2)$ 且 $S_0(M_1) = S_0 = S_0(M_2)$。若 $k > 0$，令 $s_1' \in S_k(M_1)$，并令 $s_1 \in S_{k-1}(M_1)$，其中 $(s_1, s_1') \in T(M_1)$。于是 $(s_1, s_1') \in T_k(M_1) = T_k(M_2)$，使得 $s_1 \in S_{k-1}(M_2)$ 且 $s_1' \in S_k(M_2)$。反向包含关系由对称性可得。
(2) 如果对于所有 $k \ge 0$，都有 $T_k(M_1) = T_k(M_2)$，那么根据定义可得 $T_\omega(M_1) = \bigcup_{0\le k} T_k(M_1) = \bigcup_{0\le k} T_k(M_2) = T_\omega(M_1)$。——反过来，设 $T_\omega(M_1) = T_\omega(M_2)$ 成立。我们对 $k \ge 0$ 作归纳：对于 $k = 0$，$T_0(M_1) = \emptyset = T_\omega(M_2)$。现在，$(s_1, s_1') \in T_{k+1}(M_1)$ 当且仅当根据 (1)，$s_1 \in S_k(M_1) = S_k(M_2)$；而且 $(s_1, s_1') \in T_\omega(M_1) = T_\omega(M_2)$ 当且仅当 $(s_1, s_1') \in T_{k+1}(M_2)$。□

引理 A.2. 设 $(M_k)_{0\le k} \subseteq \mathscr{M}_\Sigma(\mathsf{B})$ 满足条件：对于所有 $k' \ge k \ge 0$，都有 $T_k(M_{k'}) = T_k(M_k)$，且 $M_\omega = (\mathsf{B}, \bigcup_{0\le k} T_k(M_k))$。那么，对于所有 $k \ge 0$，都有 $T_k(M_\omega) = T_k(M_k)$。

证明。我们对 $k \ge 0$ 进行归纳：根据定义，$k = 0$, $T_0(M_\omega) = \emptyset = T_0(M_0)$。设该结论对 $k \ge 0$ 成立。根据定义，$T_{k+1}(M_{k+1}) \subseteq T_{k+1}(M_\omega)$ 显然成立。对于反向包含，设 $(s, s') \in T_{k+1}(M_\omega)$，使得存在一个 $s \in S_k(M_\omega)$，因此由引理 A.1(1) 可得 $s \in S_k(M_k)$，且 $(s, s') \in T(M_\omega)$，即对于某个 $k' > 0$，有 $(s, s') \in T_{k'}(M_{k'})$。若 $k' \le k+1$，则 $(s, s') \in T_{k'}(M_{k'}) = T_{k'}(M_{k+1}) \subseteq T_{k+1}(M_{k+1})$。若 $k' > k+1$，则由引理 A.1(1) 可得 $S_k(M_k) = S_k(M_{k'})$。因此，$s \in S_k(M_{k'})$，且存在 $(s, s') \in T(M_{k'})$，使得 $(s, s') \in T_{k+1}(M_{k'}) = T_{k+1}(M_{k+1})$。□

引理 A.3. 设 $\Gamma = (\mathsf{B}, \mathcal{T})$ 是定义在 Σ上的认知守卫转移系统，并设 $M_1, M_2 \in \mathscr{M}_\Sigma(\mathsf{B})$，使得对所有 $k \ge 0$，均有 $T_k(M_1) = T_k(M_2)$。那么$\Gamma^{M_1} = \Gamma^{M_2}$。

证明. 设 $(s, s') \in T(\Gamma^{M_1})$。存在一个 $(\varphi \supset B) \in \mathcal{T}$，使得 $(s, s') \in B$, $s \in S_\omega(M_1)$，且 $M_1, s \models \varphi$。由引理 A.1(2)，由于 $T_\omega(M_1) = T_\omega(M_2)$，可知$s \in S_\omega(M_1) = S_\omega(M_2)$，因此 $M_2, s \models \varphi$。特别地，$(s, s') \in T(\Gamma^{M_2})$。反向包含关系 $T(\Gamma^{M_2}) \subseteq T(\Gamma^{M_1})$ 同理可证。□

引理 A.4。令 $\Gamma = (\mathsf{B}, \mathcal{T})$ 为关于 $\{M_1, M_2\} \subseteq \mathscr{M}_\Sigma(\mathsf{B})$依赖于过去的认知守卫转移系统，其中 Σ。

1. 如果对于某个 $k \ge 0$，$T_k(M_1) = T_k(\Gamma^{M_1}) = T_k(\Gamma^{M_2}) = T_k(M_2)$，那么 $T_{k+1}(\Gamma^{M_1}) = T_{k+1}(\Gamma^{M_2})$。*2.* 如果对于 $1 \le i \le 2$，$T_\omega(\Gamma^{M_i}) = T_\omega(M_i)$，那么对于所有 $k \ge 0$，$T_k(\Gamma^{M_1}) = T_k(\Gamma^{M_2})$。

证明。(1) 对某个 $k \ge 0$，令 $T_k(M_1) = T_k(\Gamma^{M_1}) = T_k(\Gamma^{M_2}) = T_k(M_2)$。对于每个 $M \in \mathscr{M}_\Sigma(\mathsf{B})$，均有 $T_k(M) \subseteq T_{k+1}(M)$。因此，令 $(s, s') \in T_{k+1}(\Gamma^{M_1}) \setminus T_k(\Gamma^{M_1})$。于是，根据引理 A.1(1)，$s \in S_k(\Gamma^{M_1}) = S_k(M_1)$，且存在一个 $(\varphi \supset B) \in \mathcal{T}$，使得 $(s, s') \in B$且 $M_1, s \models \varphi$。由于相对于 $\{M_1, M_2\}$，Γ 依赖于过去，并且

$T_k(M_1) = T_k(M_2)$，因此存在 $M_2, s \models \varphi$，使得 $s \in S_k(M_2) = S_k(\Gamma^{M_2})$，从而 $(s, s') \in T_{k+1}(\Gamma^{M_2})$。反向包含关系同理可证。

(2) 对于 $1 \leq i \leq 2$，令 $T_\omega(\Gamma^{M_i}) = T_\omega(M_i)$。我们对 $k \geq 0$ 进行归纳：对于 $k = 0$，$T_0(\Gamma^{M_1}) = \emptyset = T_0(\Gamma^{M_2})$。设 $T_k(\Gamma^{M_1}) = T_k(\Gamma^{M_2})$ 对 $k \geq 0$ 成立。由于对于 $1 \leq i \leq 2$，$T_\omega(\Gamma^{M_i}) = T_\omega(M_i)$，根据引理 A.1(2)，可得 $T_k(M_1) = T_k(\Gamma^{M_1}) = T_k(\Gamma^{M_2}) = T_k(M_2)$，使得依据 (1)，$T_{k+1}(\Gamma^{M_1}) = T_{k+1}(\Gamma^{M_2})$。 □

命题 1. 设 $\Gamma = (\mathsf{B}\ \mathcal{T})$ 是一个定义在Σ上的认知守卫转移系统。那么，Γ 有至多一个解，当且仅当存在一个 $\mathcal{M} \subseteq \mathscr{M}_\Sigma(\mathsf{B})$，满足$\{M \in \mathscr{M}_\Sigma(\mathsf{B}) \mid \Gamma^M = M\} \subseteq \mathcal{M}$，使得 Γ 相对于 $\mathcal{M}$ 依赖于过去。

证明。如果 Γ没有解，那么我们可以选择 $\mathcal{M} = \emptyset$；如果 Γ有唯一解 M，那么我们可以选择 $\mathcal{M} = \{M\}$。——反过来，设给定 $\mathcal{M}$，并且对于 M_1、$M_2 \in \mathcal{M}$，有 $\Gamma^{M_1} = M_1$和 $\Gamma^{M_2} = M_2$。由引理 A.4(1)以及 $T_0(M_1) = T_0(\Gamma^{M_1}) = \emptyset = T_0(\Gamma^{M_2}) = T_0(M_2)$，我们得到对所有$k \geq 0$，$T_k(M_1) = T_k(\Gamma^{M_1}) = T_k(\Gamma^{M_2}) = T_k(M_2)$。因此，由引理 A.3 可得 $M_1 = \Gamma^{M_1} = \Gamma^{M_2} = M_2$。 □

命题 *2.* 设 $\Gamma = (B\ \mathcal{T})$是定义在 Σ上的认知守卫转移系统。设 $\mathcal{M} \subseteq \mathscr{M}_\Sigma(B)$满足：对每个 $M \in \mathcal{M}$，都有 $\Gamma^M \in \mathcal{M}$；并且对于所有满足 $T_k(M_{k'}) = T_k(M_k)$的$(M_k)_{0 \leq k} \subseteq \mathcal{M}$，$(B \bigcup_{0 \leq k} T_k(M_k)) \in \mathcal{M}$。设 Γ相对于 $\mathcal{M}$ 和 $M_{-1} \in \mathcal{M}$依赖于过去，对所有 $i \geq -1$都有 $M_{i+1} = \Gamma^{M_i}$，且 $M_\omega = (B \bigcup_{0 \leq k} T_k(M_k))$。那么 $\Gamma^{M_\omega} = \Gamma^{\Gamma^{M_\omega}}$。

证明。我们首先通过对 $0 \leq k$进行归纳，证明对于所有 $0 \leq k \leq k'$，$T_k(M_k) = T_k(M_{k'})$。对于 $k = 0$，对于所有 $0 \leq k'$，有 $T_0(M_0) = \emptyset = T_0(M_{k'})$。对于 $k > 0$，由对于所有 $k - 1 \leq k'$ 均有 $T_{k-1}(M_{k-1}) = T_{k-1}(M_{k'})$，可推出 $T_{k-1}(M_{k-1}) = T_{k-1}(M_k) = T_{k-1}(\Gamma^{M_{k-1}}) = T_{k-1}(\Gamma^{M_{k'-1}}) = T_{k-1}(M_{k'})$；因此，根据引理 A.4(1)，对于所有 $k \leq k'$，$T_k(M_k) = T_k(\Gamma^{M_{k-1}}) = T_k(\Gamma^{M_{k'-1}}) = T_k(M_{k'})$。

现在设 $\Gamma^{M_\omega} \in \mathcal{M}$。接下来我们证明 $T_\omega(\Gamma^{M_\omega}) = T_\omega(M_\omega) = T_\omega(\Gamma^{\Gamma^{M_\omega}})$。根据引理 A.1(2)，只需证明对于所有$k \geq 0$，$T_k(\Gamma^{M_\omega}) = T_k(M_\omega) = T_k(\Gamma^{\Gamma^{M_\omega}})$。由此，根据引理 A.3，$\Gamma^{M_\omega} = \Gamma^{\Gamma^{M_\omega}}$立即成立。根据前述说明，对于所有满足 $T_k(M_\omega) = T_k(M_k)$ 的 $0 \leq k \leq k'$，有 $T_k(M_k) = T_k(M_{k'})$；根据引理 A.2，该结论对所有 $k \geq 0$均成立。

我们通过对 $k \geq 0$进行归纳得到 $T_k(\Gamma^{M_\omega}) = T_k(M_k)$：对于 $k = 0$，结论显然成立。设对于 $k \geq 0$，$T_k(\Gamma^{M_\omega}) = T_k(M_k)$ 成立。由 $T_k(M_\omega) = T_k(M_k)$ 和 $T_k(M_k) = T_k(\Gamma^{M_{k-1}})$，根据引理 A.4(1)可得 $T_{k+1}(\Gamma^{M_\omega}) = T_{k+1}(\Gamma^{M_k}) = T_{k+1}(M_{k+1})$。采用相同的论证，但将$\Gamma^{M_\omega}$替换为 $\Gamma^{\Gamma^{M_\omega}}$，我们通过对 $k \geq 0$进行归纳得到 $T_k(\Gamma^{\Gamma^{M_\omega}}) = T_k(M_k)$。 □

引理 1。 设 $\Gamma = (\mathsf{B}\ \mathcal{T})$ 是定义在 (P, A)上的认知守卫转移系统，并设 $\mathcal{M} \subseteq \mathscr{M}_{P,A}(S, E, L, S_0)$，使得所有 $M \in \mathcal{M}$ 都为 Γ中的所有知识守卫提供认知见证。那么，Γ相对于 $\mathcal{M}$依赖过去。

证明。设 $\varphi \supset B \in \mathcal{T}$, $M_1, M_2 \in \mathcal{M}$和 $k \in \mathbb{N}$ 满足 $T_k(M_1) = T_k(M_2)$。我们需要证明，对于所有 $s \in S_k(M_1) \cap S_k(M_2)$，都有 $M_1, s \models \varphi \iff M_2, s \models \varphi$。我们对认知公式 φ的结构进行归纳；设 $s \in S_k(M_1) \cap S_k(M_2)$。

情形 true、false、p、$\neg\psi$、$\varphi_1 \vee \varphi_2$和 $\varphi_1 \wedge \varphi_2$ 要么显然成立，要么可直接由归纳假设推出。

情形 $\varphi = \mathrm{K}_a\,\psi$：如果 M_1、$s \models \mathrm{K}_a\,\psi$ 和 M_2、$s \models \mathrm{K}_a\,\psi$ 都成立，则结论成立。如果M_1、$s \not\models \mathrm{K}_a\,\psi$，由于 M_1 提供了认知见证，因此存在一个 $s' \in S_k(M_1)$，使得 $(s, s') \in E_a$ 且 $M_1, s' \not\models \psi$。特别地，利用引理 A.1(1)，$s' \in S_k(M_1) \cap S_k(M_2)$。根据归纳假设，$M_2, s' \not\models \psi$，从而 $M_2, s \not\models \mathrm{K}_a\,\psi$。反过来，由$M_2$、$s \not\models \mathrm{K}_a\,\psi$可推出 M_1、$s \not\models \mathrm{K}_a\,\psi$，这可对称地证明。

情形 $\varphi = \mathrm{M}_a\,\psi$：与 $\mathrm{K}_a\,\psi$ 类似。 □

引理 *A.5.* 设 $(M_k)_{0\le k} \subseteq \mathscr{M}_{P,A}(S, E, L, S_0)$ 满足对所有 $k' \ge k \ge 0$，$T_k(M_{k'}) = T_k(M_k)$，并设 $M_\omega = (S, E, L, S_0, \bigcup_{0\le k} T_k(M_k))$。若每个 M_k 都提供认知见证，则 M_ω 也如此。

证明。设 $k \ge 0$, $s \in S_k(M_\omega)$，且 $M_\omega, s \not\models \mathrm{K}_a\,\varphi$。则存在一个 $k' \ge 0$ 和一个 $s' \in S_{k'}(M_\omega)$，使得 $(s, s') \in E_a$ 且 $M_\omega, s' \not\models \varphi$。因此 $M_{k'}, s' \not\models \varphi$，并且由于 $T_{k'}(M_{k'}) = T_{k'}(M_\omega)$，根据引理 A.2 和引理 A.1(1)，也有 $M_{k'}, s \not\models \mathrm{K}_a\,\varphi$。但 $M_{k'}$ 提供认知见证，且 $s \in S_k(M_{k'})$，因此存在一个 $s'' \in S_k(M'_k) \subseteq S_k(M_\omega)$。□

B 构造性解释

引理 2. 设 $Y = (S,\ E,\ L,\ S_0,\ (T_\mu,\ T_\nu))$ 是定义在 $(P,\ A)$ 上的认知必然/可能转移结构，且 $\varphi \in \Phi_{P,\ A}$。那么，对于所有 $s \in S_\omega(Y_\nu)$，Y，$s \models_{\mathrm{p}} \varphi$，均有 Y，$s \not\models_{\mathrm{n}} \varphi$。

证明。我们对 $\varphi \in \Phi_{P,\ A}$ 的结构进行归纳。

情形 $\varphi = p$：那么 $Y, s \models_{\mathrm{p}} p$ 当且仅当 $p \in L(s)$，当且仅当 $Y, s \not\models_{\mathrm{n}} p$。

情形 $\varphi =$ 假：那么 $Y, s \models_{\mathrm{p}}$ 假 当且仅当 $Y, s \not\models_{\mathrm{n}}$ 假。

情形 $\varphi = \neg\psi$：那么 $Y, s \models_{\mathrm{p}} \neg\psi$ 当且仅当 $Y, s \models_{\mathrm{n}} \psi$，根据归纳假设可推出 Y，$s \not\models_{\mathrm{p}} \psi$，因此 $Y, s \not\models_{\mathrm{n}} \neg\psi$。

情形 $\varphi = \mathrm{K}_a\,\psi$：那么 $Y, s \models_{\mathrm{p}} \mathrm{K}_a\,\psi$ 当且仅当对于所有满足 $(s, s') \in E_a$ 的 $s' \in S_\omega(Y_\nu)$，都有 $Y, s' \models_{\mathrm{p}} \psi$；根据归纳假设可推出对于所有满足 $(s, s') \in E_a$ 的 $s' \in S_\omega(Y_\nu)$，都有 $Y, s \not\models_{\mathrm{n}} \psi$，因此 $Y, s \not\models_{\mathrm{n}} \mathrm{K}_a\,\psi$，因为 $S_\omega(Y_\mu) \subseteq S_\omega(Y_\nu)$。 □

引理 3. 设 $Y \in \mathscr{Y}_{P,A}(S, E, L, S_0), \varphi \in \Phi_{P,A}$, *and* $s \in S_\omega(Y_\nu)$。那么 $Y, s \models_{\mathrm{p}} \varphi$当且仅当 $Y, s \models$ 否定范式(φ)，并且 $Y, s \models_{\mathrm{n}} \varphi$ 当且仅当 $Y, s \models$ 否定范式$(\neg\varphi)$。

证明。我们对 $\varphi \in \Phi_{P,A}$ 的结构进行归纳。

情形 $\varphi = p$：则 $Y, s \models_{\mathrm{p}} p$当且仅当 $p \in L(s)$ 当且仅当 $Y, s \models p =$ 否定范式(p)；并且 $Y, s \models_{\mathrm{n}} p$当且仅当$p \notin L(s)$ 当且仅当 $Y, s \models \neg p =$ 否定范式$(\neg p)$。

情形 $\varphi =$ false：则 $Y, s \models_{\mathrm{p}}$ false 当且仅当 $Y, s \models$ false $=$ 否定范式(false)；并且 $Y, s \models_{\mathrm{n}}$ false 当且仅当$Y, s \models$ true $=$ 否定范式(¬false)。

情形 $\varphi = \neg\psi$：则根据归纳假设，$Y, s \models_{\mathrm{p}} \neg\psi$当且仅当 $Y, s \models_{\mathrm{n}} \psi$当且仅当 $Y, s \models$ 否定范式$(\neg\psi)$；并且根据归纳假设，$Y, s \models_{\mathrm{n}} \neg\psi$当且仅当 $Y, s \models_{\mathrm{p}} \psi$当且仅当 $Y, s \models$ 否定范式(ψ) $=$ 否定范式$(\neg\neg\psi)$。

情形 $\varphi = \varphi_1 \wedge \varphi_2$: 那么 $Y, s \models_{\mathrm{p}} \varphi_1 \wedge \varphi_2$当且仅当 $Y, s \models_{\mathrm{p}} \varphi_1$并且 $Y, s \models_{\mathrm{p}} \varphi_2$当且仅当$Y$，$s \models$ 否定范式(φ_1) 并且 $Y, s \models$ 否定范式(φ_2)，根据归纳假设，当且仅当 $Y, s \models$ 否定范式$(\varphi_1) \wedge$

否定范式(φ_2) $=$ 否定范式($\varphi_1 \wedge \varphi_2$)；并且 $Y, s \models_{\mathrm{n}} \varphi_1 \wedge \varphi_2$ 当且仅当 $Y, s \models_{\mathrm{n}} \varphi_1$ 或者 $Y, s \models_{\mathrm{n}} \varphi_2$当且仅当 $Y, s \models$ 否定范式($\neg\varphi_1$) 或者 $Y, s \models$ 否定范式($\neg\varphi_2$)，根据归纳假设，当且仅当 $Y, s \models$否定范式($\neg\varphi_1$) $\vee$否定范式($\neg\varphi_2$) $=$ 否定范式($\neg(\varphi_1 \wedge \varphi_2)$)。
情形 $\varphi = \mathrm{K}_a \psi$: 那么 $Y, s \models_{\mathrm{p}} \mathrm{K}_a \psi$ 当且仅当 $Y, s' \models_{\mathrm{p}} \psi$ 对所有满足 $(s, s') \in E_a$的 $s' \in S_\omega(Y_\nu)$，当且仅当 $Y, s \models$ 否定范式(ψ) 对所有满足 $(s, s') \in E_a$ 的 $s' \in S_\omega(Y_\mu)$，根据归纳假设，当且仅当$Y, s \models \mathrm{K}_a$ 否定范式(ψ) $=$否定范式($\mathrm{K}_a \psi$)；并且 $Y, s \models_{\mathrm{n}} \mathrm{K}_a \psi$ 当且仅当 $Y, s' \models_{\mathrm{n}} \psi$ 存在满足 $(s, s') \in E_a$ 的 $s' \in S_\omega(Y_\mu)$，当且仅当 $Y, s \models$ 否定范式 ($\neg\psi$) 存在满足 $(s, s') \in E_a$ 的 $s' \in S_\omega(Y_\mu)$，根据归纳假设，当且仅当 $Y, s \models \mathrm{M}_a$ 否定范式($\neg\psi$) $=$ 否定范式($\neg\mathrm{K}_a \psi$)。 □

引理 4. 令 Y, $Y' \in \mathscr{Y}_{P,\ A}(S,\ E,\ L,\ S_0)$ 满足 $Y \sqsubseteq Y'$，并令$\varphi \in \Phi_{P,\ A}$。那么Y，$s \models$ 否定范式(φ) 蕴含 Y'，$s \models$ 否定范式(φ) 对所有 $s \in S_\omega(Y'_\nu)$均成立。

证明。我们对处于否定范式的 nnf(φ) 的结构进行归纳。true 和 false 两种情形显然成立；p 以及 $\neg p$ 对于 $p \in P$，可直接由 Y和 Y'的状态标记不变性得出；$\varphi_1 \vee \varphi_2$ 和 $\varphi_1 \wedge \varphi_2$ 则可通过应用归纳假设直接得出。

情形 nnf(φ) $= \mathrm{K}_a \psi$: 设对于某个 $s \in S_\omega(Y'_\nu) \subseteq S_\omega(Y_\nu)$，有 $Y, s \models \mathrm{K}_a \psi$。那么，对于所有满足 $(s, s') \in E_a$的 $s' \in S_\omega(Y_\nu)$，都有$Y, s' \models \psi$。因此，对于所有满足 $(s, s') \in E_a$的 $s' \in S_\omega(Y'_\nu)$，都有 $Y, s' \models \psi$，因为 $S_\omega(Y_\nu) \supseteq S_\omega(Y'_\nu)$。根据归纳假设，对于所有满足 $(s, s') \in E_a$的 $s' \in S_\omega(Y'_\nu)$，都有 $Y', s' \models \psi$，因此有 $Y', s \models \mathrm{K}_a \psi$。
情形 否定范式(φ) $= \mathrm{M}_a \psi$: 设 $Y, s \models \mathrm{M}_a \psi$对某个 $s \in S_\omega(Y'_\nu) \subseteq S_\omega(Y_\nu)$ 成立。那么 $Y, s' \models \psi$存在某个 $s' \in S_\omega(Y_\mu)$，使得 $(s, s') \in E_a$。因此 $Y, s' \models \psi$存在某个 $s' \in S_\omega(Y'_\mu)$，使得 $(s, s') \in E_a$，因为 $S_\omega(Y_\mu) \subseteq S_\omega(Y'_\mu)$。由于 $S_\omega(Y'_\mu) \subseteq S_\omega(Y'_\nu)$，根据归纳假设可得 $Y', s' \models \psi$存在某个 $s' \in S_\omega(Y'_\mu)$，使得 $(s, s') \in E_a$，进而 $Y', s \models \mathrm{M}_a \psi$。
□

命题 3. 设 $\Gamma = (S,\ E,\ L,\ S_0,\ \mathcal{T})$ 是定义在 $(P,\ A)$ 上的认知守卫转移系统，并且 Y，$Y' \in \mathscr{Y}_{P,\ A}(S,\ E,\ L,\ S_0)$ 满足 $Y \sqsubseteq Y'$。则 $\Gamma^Y \sqsubseteq \Gamma^{Y'}$。

证明。令 $(\varphi \supset B) \in \mathcal{T}$。那么 $(\varphi \supset B)^{Y,\mu} \subseteq (\varphi \supset B)_{Y',\mu}$ 和 $(\varphi \supset B)^{Y,\nu} \supseteq (\varphi \supset B)_{Y',\nu}$ 可由以下蕴含关系推出：对于所有 $s \in S_\omega(Y'_\nu) \supseteq S_\omega(Y'_\mu) \supseteq S_\omega(Y_\mu)$，$Y', s \models$ nnf(φ) 蕴含 $Y, s \models$nnf(φ)；以及对于所有 $s \in S_\omega(Y_\nu) \supseteq S_\omega(Y'_\nu)$，$Y, s \not\models$ nnf($\neg\varphi$) 蕴含 $Y', s \not\models$ nnf($\neg\varphi$)。这些关系由引理 4 给出。 □

命题 4。 $(\mathscr{Y}_\Sigma(\mathrm{B}) \sqsubseteq,\ \bot_{\Sigma,\ \mathrm{B}})$ 是一个归纳偏序。
证明。设 $\Delta \subseteq \mathscr{Y}_\Sigma$(B) 是有向的。那么，由 $Z_\mu = \bigcup_{Y \in \Delta} Y_\mu$ 和 $Z_\nu = \bigcap_{Y \in \Delta} Y_\nu$ 给出的 Z 属于 $\mathscr{Y}_\Sigma$(B)，即 $\bigcup_{Y \in \Delta} Y_\mu \subseteq \bigcap_{Y \in \Delta} Y_\nu$；或者等价地，对所有$Y$，$Y' \in \Delta$。事实上，对每个 Y，$Y' \in \Delta$，由于 Δ 是有向的，存在一个 $Y'' \in \Delta$，使得 Y，$Y' \sqsubseteq Y''$，因此 $Y_\mu \subseteq Y''_\mu \subseteq Y''_\nu \subseteq Y'_\nu$ 成立。此外，对于认知迁移系统，按 $\subseteq$ 和 $\supseteq$，并集与交集构成上确界，因此 $\bigsqcup \Delta = Z$。最后，对于所有 $Y \in \mathscr{Y}_\Sigma$(B)，$\bot_{\Sigma,\ \mathrm{B}} \sqsubseteq Y$。

□

命题 5. </style}设 (B $\mathcal{T}$) </style}是基于 的认知守卫转移系统，且 (B) </style}已判定。那么，在 (B)中有唯一解。

证明。 Γ有解 $(\mu\Gamma)_\mu = (\mu\Gamma)_\nu \in \mathscr{M}_\Sigma(\mathsf{B})$。为证明唯一性，设$M \in \mathscr{M}_\Sigma(\mathsf{B})$满足 $M = \Gamma^M$。令 $Y_M = (\mathsf{B}, (T(M)\ T(M)) \in \mathscr{M}_\Sigma(\mathsf{B})$，使得$Y_M = \Gamma^{Y_M} \in \mathscr{Y}_\Sigma(\mathsf{B})$（参见第 4.3 节）。由于 $\mu\Gamma$是最小构造性不动点，因此有 $\mu\Gamma \sqsubseteq Y_M$，从而 $(\mu\Gamma)_\mu \subseteq M \subseteq (\mu\Gamma)_\nu$。由于 $\mu\Gamma$已判定，我们得到 $(\mu\Gamma)_\mu = M = (\mu\Gamma)_\nu$。 □

引理 5. 设 $\Gamma = (\mathsf{B}\ \mathcal{T})$ 是定义在(P, A)上的同步认知守卫转移系统。设 $Y \in \mathscr{Y}_{P,A}(\mathsf{B})$ 满足 $\Gamma^Y = Y$。则 Y已判定。

证明。 我们证明 $Y_\mu = \Gamma^{Y_\mu}$和 $\Gamma^{Y_\nu} = Y_\nu$，由命题 1 可得 $Y_\mu = Y_\nu$，因为同步性意味着提供见证，而这又意味着对过去的依赖，参见第 3.4 节。我们只证明 $Y_\mu = \Gamma^{Y_\mu}$，另一个等式的证明类似。

根据第 4.3 节，有 $Y_\mu \subseteq \Gamma^{Y_\mu}$。假设存在一个与 $\Gamma^{Y_\mu} \subseteq Y_\mu$矛盾的情形，即存在一个 $(s, s') \in T(\Gamma^{Y_\mu}) \setminus T(Y_\mu)$，并令 $k \geq 0$对于 $s \in S_k(Y_\mu)$为极小的。于是存在一个 $(\varphi \supset B) \in \mathcal{T}$，使得 $Y, s \not\models \varphi$ 且 $\Gamma^{Y_\mu}, s \models \varphi$。此外，由 k的极小性，$T_k(Y_\mu) = T_k(\Gamma^{Y_\mu})$。我们对 nnf($\varphi$) 进行归纳。情形$p$, $\neg p$、false、true、 $\varphi_1 \wedge \varphi_2$和 $\varphi_1 \vee \varphi_2$ 显然成立。

情形 否定范式(φ) $= \mathsf{K}_a\,\psi$: 若 $Y, s \not\models \mathsf{K}_a\,\psi$，则存在某个 $s'' \in S_\omega(Y_\nu)$，使得 $(s, s'') \in E_a$且 $Y, s'' \not\models \psi$。但是 $S_\omega(Y_\nu) \subseteq S_\omega(\Gamma^{Y_\mu})$，因此根据 Γ^{Y_μ}的同步性， $s'' \in S_k(\Gamma^{Y_\mu}) = S_k(Y_\mu)$。由此， $\Gamma^{Y_\mu}, s'' \not\models \psi$，因此根据归纳假设可推出 $\Gamma^{Y_\mu}, s \not\models \mathsf{K}_a\,\psi$。

情形 否定范式(φ) $= \mathsf{M}_a\,\psi$: 若 $\Gamma^{Y_\mu}, s \not\models \mathsf{M}_a\,\psi$，则根据 Γ^{Y_μ}的同步性，存在一个$s'' \in S_k(\Gamma^{Y_\mu}) = S_k(Y_\mu)$，使得 $(s, s'') \in E_a$且 $\Gamma^{Y_\mu}, s'' \models \psi$。由此， $Y, s'' \not\models \psi$，因此根据归纳假设可推出 $Y, s \not\models \mathsf{M}_a\,\psi$。 □

C 求解一般规则系统

引理6. $(\wp^\pm U, \subseteq^\pm, \bot_U^\pm)$ 连同 $\bot_U^\pm = (\emptyset, U)$ 构成一个归纳偏序。
证明。设 $\Delta \subseteq \wp^\pm U$是有向的。那么 $(\bigcup_{(P,Q)\in\Delta} P, \bigcap_{(P,Q)\in\Delta} Q) \in \wp^\pm U$，即$\bigcup_{(P,Q)\in\Delta} P \subseteq \bigcap_{(P,Q)\in\Delta} Q$，或者等价地，对于所有的 (P, Q)、$(P', Q') \in \Delta$， $P \subseteq Q'$。事实上，对于每个 (P, Q)、$(P', Q') \in \Delta$，由于 Δ是有向的，存在一个 $(P'', Q'') \in \Delta$，使得 (P, Q)、$(P', Q') \subseteq^\pm (P'', Q'')$，于是 $P \subseteq P'' \subseteq Q'' \subseteq Q'$成立。此外，并和交关于 $\subseteq$和 $\supseteq$构成上确界，使得 $\bigcup^\pm \Delta = (\bigcup_{(P,Q)\in\Delta} P, \bigcap_{(P,Q)\in\Delta} Q)$。最后，对于所有 $(P, Q) \in \wp^\pm U$，有 $(\emptyset, U) \subseteq^\pm (P, Q)$。 □

引理7。 设 R是一个定义在 U上的规则系统。如果 $(P_1, Q_1) \subseteq^\pm (P_2, Q_2)$，那么 $\check{}R(P_1, Q_1) \subseteq^{\pm\check{}} R(P_2, Q_2)$。

证明。设 $P_1 \subseteq Q_1$、$P_2 \subseteq Q_2$、$P_1 \subseteq P_2$和 $Q_1 \supseteq Q_2$成立。设 $(P_i', Q_i') = \check{}R(P_i, Q_i)$，其中 $1 \leq i \leq 2$满足条件，且 $P_i' \subseteq Q_i'$对 $1 \leq i \leq 2$成立。于是 $P_1' \subseteq P_2'$成立，因为若 $(X, \pi Z)/y \in R$满足条件，且 $X \subseteq P_1$和 $Q_1 \cap Z = \emptyset$成立，则由 $P_1 \subseteq P_2$可得 $X \subseteq P_2$，由 $Q_1 \supseteq Q_2$可得 $Q_2 \cap Z = \emptyset$；并且 $Q_1' \supseteq Q_2'$成立，因为若 $(X, \pi Z)/y \in R$满足条件，且 $X \subseteq Q_2$和 $P_2 \cap Z = \emptyset$成立，则由 $Q_1 \supseteq Q_2$可得 $X \subseteq Q_1$，由 $P_1 \subseteq P_2$可得 $P_1 \cap Z = \emptyset$。 □

引理 8。 设 R 是定义在 U 上的规则系统，且 R 的每条规则都只包含有限多个˘正前提和负前提。那么 R 是连续的。

证明。由于˘R相对于 $\subseteq^{\pm}$是单调的，只需证明对于有向的 $\Delta \subseteq \wp^{\pm}U$，˘$R(\bigcup^{\pm}\Delta) \subseteq^{\pm} \bigcup^{\pm}$˘$R(\Delta)$。首先令 $(X,\pi Z)/y \in R$，使得 $X \subseteq \bigcup_{(P,Q)\in\Delta} P$ 且 $(\bigcap_{(P,Q)\in\Delta} Q) \cap Z = \emptyset$。由于假定 X 和 Z 是有限的，且 Δ 是有向的，因此存在一个 $(P',Q') \in \Delta$，使得 $X \subseteq P'$ 且 $Q' \cap Z = \emptyset$。现在令 $(X,\pi Z)/y \in R$，满足$X \subseteq \bigcap_{(P,Q)\in\Delta} Q$ 且 $(\bigcup_{(P,Q)\in\Delta} P) \cap Z = \emptyset$。于是，对于所有 $(P,Q) \in \Delta$，都有 $X \subseteq Q$ 和 $P \cap Z = \emptyset$。

□

D CTLK 的必然/可能解释

引理 D.1. 设 $Y \in \mathscr{Y}_{P,A}(S,E,L,S_0)$ 且 φ 是关于 (P,A) 的 *CTLK* 公式。那么对于所有 $s \in S_\omega(Y_\nu)$，都有 $Y,s \models$ 否定范式(φ) 蕴含 $Y,s \not\models$ 否定范式($\neg\varphi$)。

证明。 我们通过时序情形，将引理 2（以引理 3 的形式）的归纳推理扩展。

情形 否定范式(φ) $=$EX ψ：那么 否定范式($\neg\varphi$) $=$AX 否定范式($\neg\psi$)。设 $Y,s \models$EX ψ对 $s \in S_\omega(Y_\nu)$成立。那么 $Y,s_1 \models \psi$对于某些 $s_0,s_1,\ldots \in \mathscr{P}(Y_\mu,s)$，使得特别是$s \in S_\omega(Y_\mu)$。由于 $\mathscr{P}(Y_\mu,s) \subseteq \mathscr{P}(Y_\nu,s)$对于 $s \in S_\omega(Y_\mu) \subseteq S_\omega(Y_\nu)$，根据归纳假设，对于某些 $s_0,s_1,\ldots \in \mathscr{P}(Y_\nu,s)$，有 $Y,s_1 \not\models$否定范式($\neg\psi$)。因此 $Y,s \not\models$AX 否定范式($\neg\psi$)。
情形 nnf(φ) $=$AXψ：于是 nnf($\neg\varphi$) $=$EX nnf($\neg\psi$)。设 $Y,s \models$AX ψ 对$s \in S_\omega(Y_\nu)$成立。于是 $Y,s_1 \models \psi$ 对所有 $s_0,s_1,\ldots \in \mathscr{P}(Y_\nu,s)$均成立。若 $s \in S_\omega(Y_\nu)\backslash S_\omega(Y_\mu)$，则从$s$出发在$Y_\mu$中不存在路径，因此 $Y,s \not\models$EX nnf($\neg\psi$)。于是设 $s \in S_\omega(Y_\mu)$。由于对于 $s \in S_\omega(Y_\mu) \subseteq S_\omega(Y_\nu)$，$\mathscr{P}(Y_\mu,s) \subseteq \mathscr{P}(Y_\nu,s)$，根据归纳假设，对所有$s_0,s_1,\ldots \in \mathscr{P}(Y_\mu,s)$，都有 $Y,s_1 \not\models$ nnf($\neg\psi$)。因此再次得到 $Y,s \not\models$EXnnf($\neg\psi$)。
其他情形类似。 □

引理 D.2. 设 $Y,Y' \in \mathscr{Y}_{P,A}(S,E,L,S_0)$ 满足 $Y \sqsubseteq Y'$，并设 φ 是定义在 (P,A)上的 *CTLK* 公式。那么，对于所有 $s \in S_\omega(Y'_\nu)$， $Y,s \models$ 否定范式(φ) 蕴含 $Y',s \models$ 否定范式(φ)。

证明。 我们将引理 4 中的归纳推理扩展到时序情形。
情形 否定范式(φ) $=$EX ψ：设对于某个 $s \in S_\omega(Y'_\nu) \subseteq S_\omega(Y_\nu)$， $Y,s \models$EX ψ成立。那么Y，$s_1 \models \psi$对于某些 $s_0,s_1,\ldots \in \mathscr{P}(Y_\mu,s)$，特别是满足 $s \in S_\omega(Y_\mu)$。因此 $Y,s_1 \models \psi$对于某些 $s_0,s_1,\ldots \in \mathscr{P}(Y'_\mu,s)$，因为 $\mathscr{P}(Y_\mu,s) \subseteq \mathscr{P}(Y'_\mu,s)$。由于$S_\omega(Y_\mu) \subseteq S_\omega(Y'_\mu) \subseteq S_\omega(Y'_\nu)$，根据归纳假设可得 $Y',s_1 \models \psi$对于某些 $s_0,s_1,\ldots \in S_\omega(Y'_\mu,s)$，从而 $Y',s \models$EXψ。

情形 nnf(φ) $=$AX ψ：设 $Y,s \models$AX ψ 对某个 $s \in S_\omega(Y'_\nu) \subseteq S_\omega(Y_\nu)$ 成立。那么 $Y,s_1 \models \psi$ 对所有 $s_0,s_1,\ldots \in \mathscr{P}(Y_\nu,s)$ 都成立。因此 $Y,s_1 \models \psi$ 对所有 $s_0,s_1,\ldots \in \mathscr{P}(Y'_\nu,s)$ 都成立，因为 $\mathscr{P}(Y_\nu,s) \supseteq \mathscr{P}(Y'_\nu,s)$。根据归纳假设， $Y',s_1 \models \psi$ 对所有 $s_0,s_1,\ldots \in\mathscr{P}(Y'_\nu,s)$ 都成立，因此 $Y',s \models$AX ψ。
所有其他情形都类似。 □