通用观测模型下基于演化的定时不透明性

Zhe Zhang、Martijn Goorden 和 Michel Reniers

arXiv:2603.26573v1 [cs.FL] 27 Mar 2026

摘要——**现有关于定时不透明性的文献，针对定时自动机的受限子类或有限观测模型采用了特定定义。由于缺乏统一定义，难以建立形式关系并比较不同不透明性变体的表达能力。本文通过为定时自动机引入通用观测模型，建立了一个统一的定时不透明性框架。首先，我们引入一种对时间延迟进行完全观测、对位置、时钟和事件进行部分观测的观测模型。其次，基于该模型，我们定义了基于演化的定时不透明性概念。第三，我们从数学上证明，基于演化的定时不透明性严格蕴含基于语言的定时不透明性，并证明在受限观测下，它与执行时间不透明性形式等价。该框架建立了一个统一的语义层次结构，用于刻画定时不透明性的整体图景。**

I. 引言

在信息物理系统（CPS）中，信息安全至关重要，尤其是对于在严格时间约束下运行的安全关键基础设施 [1]。除传统的访问控制之外，不透明性提供了严格的机密性保证，确保系统的“秘密”行为对于外部观察者而言始终具有合理的可否认性 [2]。尽管不透明性已在离散事件系统（DES）中得到广泛研究， [3]——[5], 稠密时间的引入带来了显著的复杂性 [6]。在由定时自动机（TA） [7], 建模的实时系统中，事件的精确时序充当了关键的信息通道，可能泄露在无定时抽象中原本会被隐藏的秘密。

自 Cassez 揭示定时不透明性的“黑暗面”以来——具体而言，该问题对于定时自动机通常是不可判定的—— [6], 后续研究大多致力于寻找“光明面”，即验证问题变得可判定的情形 [8]。为实现可判定性，这些研究通常采取务实的“自底向上”策略：针对特定的定时自动机子类或受限的观测模型，定义相应的不透明性 [9]。在系统建模方面，研究者常利用结构约束来确保可判定性。例如， [10] 探讨了结构限制，并针对事件记录定时自动机等特定子类定义了不透明性；而 [11] 则通过聚焦于整数重置定时自动机，实现了可判定性。类似地，其他研究通过将约束直接关联到迁移来简化定时结构，例如 [12]使用的实时标记定时自动机以及 [13]使用的时间区间自动机。这些结构会在每一步隐式重置全局时钟，从而将时间记忆有效限制在当前迁移上。在观测方面，通常通过限制观察者的能力来控制复杂度。例如， [14]假设了一种受限的观察者模型，其中可观测内容仅限于执行时间。 [15]的研究进一步通过施加有界时间范围来限制观察者的能力，并保证系统在特定的有限时长内具有安全性。此外， [9]采用离散时间语义简化观测模型，实际上将时间的稠密特性抽象掉，以便于验证。尽管这些方法在各自的领域取得了成功，但这种“可判定性优先”的方法也催生了针对特定情境设计的多种定义。现有定义大多将无定时不透明性的概念加以推广，主要通过使用定时语言（例如基于语言的定时不透明性）将保密性扩展到定时领域。

然而，对特定子类的关注导致理论缺乏连贯性。现有定义，包括基于语言的定时不透明性和执行时间不透明性，往往是为满足特定约束而分别提出的，从而造成了碎片化的局面。这种碎片化带来了两个结构性挑战：（1）缺乏对这些不同不透明性概念之间关系的系统性理解；（2）当前形式体系的表达能力有限，无法为推理不透明性提供统一基础，尤其是在入侵者具备多种观测能力时。例如，现有的基于语言的抽象存在一种结构性局限，我们称之为后缀盲性。由于定时词的抽象会舍弃最后一个可观测离散事件之后的所有时间进展，因此无法捕获通过尾随延迟泄露的机密行为。为应对这些挑战，我们提出一种自顶向下语义框架。我们并不通过限制模型来确保可判定性，而是建立一个全面的语义基准，从根本上刻画定时自动机的连续动态。本文的主要贡献有三点：

- 我们为定时自动机（TA）引入一种观测模型，用以考虑位置、时钟和事件的部分可观测性（第 III节）。
- 基于该观测模型，我们提出一种新的不透明性概念——基于演化的定时不透明性（EBTO），以严格刻画连续状态演化和稠密时间动态（第 IV节）。
- 最后，我们建立了定时不透明性的形式化层级。我们证明，EBTO 提供了严格强于.....的保密性保证——

作者就职于荷兰埃因霍温埃因霍温理工大学机械工程系。电子邮箱：{z.zhang4, m.a.goorden, m.a.reniers}@tue.nl本文是提交至第65届 IEEE 决策与控制会议（CDC 2026）的一篇论文的完整版，其中提供了因篇幅限制而未收录于会议版本中的详细技术证明。

基于语言的定时不透明性（LBTO），并证明在受限观察条件下，它与执行时间不透明性（ETO）在结构上等价（第V节）。

这一系统化视角使我们能够将现有的不透明性问题视为统一理论的具体应用，而非彼此孤立的案例。

II. 预备知识

定时自动机（TA）是一种扩展了有限个实值时钟的有限自动机。定时自动机的时间行为由时钟约束刻画，这些约束用作边上的守卫和位置上的不变式。为形式化定义定时自动机，我们首先确立这些约束的语法。

给定一个有限的实值时钟集合 C，其上的 时钟约束 [7]定义如下:

$$\varphi ::= \text{true} \mid x \sim n \mid x - y \sim n \mid \varphi \wedge \varphi \mid \varphi \vee \varphi$$

其中，$x, y \in C$、$n \in \mathbb{N}$以及比较运算符 $\sim$属于集合 $\{<, \leq, =, \geq, >\}$。我们将 C 上所有此类时钟约束构成的集合记为 $\mathcal{G}(C)$。

约束定义了时序的逻辑条件，而系统的时间状态则由时钟赋值刻画。以下定义形式化说明时钟如何持有数值，以及这些数值如何通过重置和时间流逝而变化。

给定一个有限时钟集合 C，时钟赋值是一个函数u: $C \to \mathbb{R}_{\geq 0}$，它为每个时钟 $x \in C$赋予一个非负实数值。我们用 $\mathcal{U}$ 表示所有此类赋值组成的集合，即 $\mathcal{U} = C \to \mathbb{R}_{\geq 0}$。我们用$\mathbf{0}$ 表示零赋值，即 $\mathcal{U}$ 中满足以下条件的唯一赋值：对所有 $x \in C$，$\mathbf{0}(x) = 0$。

我们定义时钟赋值上的以下运算:

1) 重置：给定一个时钟集合 $r \subseteq C$， u 在 r上的重置记为 $u[r]$，其定义为:

$$u[r](x) = \begin{cases} 0 & \text{if } x \in r, \\ u(x) & \text{otherwise.} \end{cases}$$

直观而言， r 中的时钟会被重置为零，而其他时钟保持不变。

2) 时间流逝：给定一个延迟 $\tau \in \mathbb{R}_{\geq 0}$，时间流逝后的赋值 $u + \tau$ 定义为:

$$(u + \tau)(x) = u(x) + \tau \quad \text{for all } x \in C.$$

此运算对所有时钟统一建模时间的流逝。

若时钟赋值 u 满足时钟约束 φ，记作 $u \models \varphi$，则对于 u 赋给每个时钟的值， φ 均为真。在确立这些预备知识后，我们现在可以正式定义定时自动机的结构。

一个定时自动机 [7]是一个六元组（L， L_0， C， Σ， E， I），其中：1） L是有限个位置组成的集合；2） $L_0 \subseteq L$ 是有限个初始位置组成的集合；3） C 是有限个时钟组成的集合；4） Σ 是有限个事件组成的集合；5） $E \subseteq L \times \Sigma \times \mathcal{G}(C) \times 2^C \times L$ 是有限个边组成的集合；6） I： $L \to \mathcal{G}(C)$ 为每个位置 $l \in L$指定一个不变式 $I(l)$，该不变式是来自 $\mathcal{G}(C)$ 的时钟约束。

为了分析定时自动机的内部操作语义，具体来说，分析它如何通过离散事件或时间延迟在状态之间迁移，我们引入定时自动机的语义图 （状态图）。语义图表示定时自动机的无限状态空间，其中状态由位置和具体的时钟赋值构成。

定义 1（状态图 [16]）。给定一个定时自动机 $\mathcal{A} = (L, L_0, C, \Sigma, E, I)$，其状态图 $\mathcal{T} = (S, S_0, \Gamma, \delta)$ 记作 $\mathcal{S}(\mathcal{A})$：

1） $S = \{(l, u) \in L \times \mathcal{U} \mid u \models I(l)\}$ 是状态集合；

2） $S_0 = \{(l_0, \mathbf{0}) \mid l_0 \in L_0 \wedge \mathbf{0} \models I(l_0)\}$ 是初始状态集合。如果 $S_0 = \varnothing$，则语义图未定义；3） $\Gamma = \Sigma \cup \mathbb{R}_{\geq 0}$ 是动作集合；4） $\delta \subseteq S \times \Gamma \times S$ 是转移关系，定义为满足以下条件的最小关系：

- （事件转移） $((l_s, u_s), \sigma, (l_t, u_s[r])) \in \delta$ 当存在 $(l_s, \sigma, g, r, l_t) \in E$，使得 $u_s \models g \wedge I(l_s)$，且 $u_s[r] \models I(l_t)$ 时；
- （时间转移）$((l, u), \tau, (l, u + \tau)) \in \delta$ 若 $\forall \theta \in [0, \tau]$, $u + \theta \models I(l)$。■

连续时间语义的一个基本特征是，时间的流逝可以任意拆分或合并，而零时间延迟不会改变系统状态。这些性质称为时间可加性、连续性和自反性 [17]。

性质 1（时间可加性、连续性和自反性）。设$\mathcal{A} = (L, L_0, C, \Sigma, E, I)$ 是一个定时自动机，且 $\mathcal{T} = (S, S_0, \Gamma, \delta)$ 是其状态图。对于所有 $l \in L$, $u \in \mathcal{U}$和 $\tau, \tau' \in \mathbb{R}_{\geq 0}$:

$$((l, u), \tau, (l, u + \tau)) \in \delta \wedge ((l, u + \tau), \tau', (l, u + \tau + \tau')) \in \delta$$

$$\iff ((l, u), \tau + \tau', (l, u + \tau + \tau')) \in \delta,$$

$$((l, u), 0, (l, u)) \in \delta.$$

在状态图中，系统的动态行为被表示为状态空间中的一条路径。我们将这条路径定义为一种演化。状态图 $\mathcal{T} = (S, S_0, \Gamma, \delta)$ 的一种演化[1] 是由状态和动作交替组成的序列，其形式为

$$\rho = s^0 \gamma^0 s^1 \gamma^1 \cdots \gamma^{n-1} s^n \in S \cdot (\Gamma \cdot S)^*,$$

对于某个 $n \in \mathbb{N}$，满足对所有 $i < n$，$(s^i, \gamma^i, s^{i+1}) \in \delta$。为便于阅读，以下我们将演化写成箭头形式:

$$s^0 \xrightarrow{\gamma_0} s^1 \xrightarrow{\gamma_1} \cdots \xrightarrow{\gamma_{n-1}} s^n.$$

在系统所有可能的演化中，我们尤其关注那些表示从某个初始状态出发的有效系统运行的演化。给定一个状态图 $\mathcal{T} = (S, S_0, \Gamma, \delta)$，若演化 ρ 满足 $s^0 \in S_0$，则称其为生成的。我们用 $\text{Gen}^{\mathcal{T}} \subseteq S \cdot (\Gamma \cdot S)^*$ 表示所有生成演化构成的集合。

最后，我们正式定义状态图和定时自动机的确定性。设 $\mathcal{T} = (S, S_0, \Gamma, \delta)$ 是一个状态图， $\mathcal{A}$ 是一个定时自动机。

1）当且仅当状态图 $\mathcal{T}$ 是确定性的

$$\forall s \in S, \forall \gamma \in \Gamma: \left|\{ s' \in S \mid (s, \gamma, s') \in \delta \}\right| \leq 1 \quad \text{and} \quad |S_0| = 1.$$

[1]本文始终只考虑有限长度的演化；因此，与芝诺行为相关的问题从根本上得以避免。

2) 当且仅当定时自动机 $\mathcal{A}$ 的状态图 $\mathcal{S}(\mathcal{A})$ 是确定性状态图时，该定时自动机才是确定性的。

本文余下部分所考虑的所有 TA 和 SG 均为确定性的。因此，任何所考虑 TA 的初始位置集都限制为单个初始位置（通常记为 l_0）。

III. 通用观测模型

一般而言，在离散事件系统中，不透明性要求系统的秘密行为对于外部观察者而言始终具有合理的可否认性；该观察者通过投影映射观测系统执行（屏蔽不可观测事件）[18]。然而，稠密时间的引入使这一情况变得复杂得多。在实时情境中，观测的精确时序构成了一个额外且强大的信息通道。观察者可能仅通过分析事件之间的延迟，就能区分两个可观测事件完全相同的序列，从而可能揭示在无定时抽象中仍会隐藏的秘密 [10]。

首先，我们对观察者的观测能力进行形式化。为完整刻画系统执行的语义，我们考虑一种观测模型，其中观察者只能部分观测位置、时钟赋值和离散事件。具体而言，每个域都被划分为互不相交的可观测子集和不可观测子集：$L = L_{\text{obs}} \cup L_{\text{uo}}$，$C = C_{\text{obs}} \cup C_{\text{uo}}$，$\Sigma = \Sigma_{\text{obs}} \cup \Sigma_{\text{uo}}$，其中

1) L_{obs}（分别对应 L_{uo}）是可观测（分别对应不可观测）位置的集合；2) C_{obs}（分别对应 C_{uo}）是可观测（分别对应不可观测）时钟的集合；3) Σ_{obs}（分别对应 Σ_{uo}）是可观测（分别对应不可观测）事件标签的集合。

对于系统的任意演化，我们假设时间延迟完全可观测。这一设定反映了这样的实际场景：观察者可以使用本地计时设备获取墙上时钟时间。虽然这与标准的基于定时语言的研究中全局可访问时钟的前提一致（例如，[9]–[12], [15]），但严格依赖定时语言结果会导致后缀盲性问题。在标准的基于定时语言的研究中，最后一个可观测事件之后发生的任何时间推移都会在投影中被截断并丢失。为克服这一局限，我们的观测模型基于连续的状态演化，而非事件序列，从而保留这些尾随延迟。第V-A节讨论了一个形式化比较，说明基于语言的定时不透明性如何在后缀盲性的情况下失效。

表I 将我们的设定与其他定时不透明性概念进行了比较。值得注意的是，许多现有研究聚焦于基于事件的观测，并将位置（L）和时钟赋值（C）视为完全不可观测。引入 L_{obs} 和 C_{obs}，是出于实际场景的考虑：传感器只能提供有关位置和时钟值的部分信息。这种建模选择在概念上与为非定时离散事件系统（DES）建立的混合观测结构一致，在这些结构中，状态信息只能被部分访问 [19], [20]。通过纳入 L_{obs} 和 C_{obs}，我们的观测模型为观察者提供了更灵活的观测能力，并且在特定约束下可简化为这些经典的事件中心模型（例如，令 $L_{\text{obs}} = C_{\text{obs}} = \varnothing$）。

表 I：定时不透明性中观测者能力的比较

参考文献	模型	可观测信息			
		Σ	延迟	L	C
[9]	离散定时自动机	✓	✓	×	×
[10]	标准定时自动机	✓	✓	×	×
[11]	整数重置定时自动机	✓	✓	×	×
[12]	实时标记定时自动机	✓	✓	×	×
[13]	时间区间自动机	✓	✓	×	×
[14]	标准定时自动机	×	✓	×	×
[15]	标准定时自动机	✓	$✓_b$	×	×
Ours	**标准定时自动机**	✓	✓	✓	✓

符号：✓：可观测（或部分可观测）；×：不可观测；$✓_b$：有界时间观测。

为表示对观察者隐藏的信息，我们引入特殊符号：位置符号 $l_\epsilon \notin L$、事件符号 $\sigma_\epsilon \notin \Sigma$ 和时钟值 $u_\epsilon \notin \mathbb{R}_{\geq 0}$。这些符号在以下映射中充当不可观测成分的掩码。

定义 2 (观测映射)。设 $\Gamma = \Sigma \cup \mathbb{R}_{\geq 0}$ 为动作集合，其中 $\Sigma = \Sigma_{\text{obs}} \cup \Sigma_{\text{uo}}$、$L = L_{\text{obs}} \cup L_{\text{uo}}$ 和 $C = C_{\text{obs}} \cup C_{\text{uo}}$ 分别为事件、位置和时钟的集合。

我们将可观测时钟赋值集合记为$\mathcal{U}_{\text{obs}}$，并定义为将时钟映射到非负实数值或不可观测符号的函数集合：$\mathcal{U}_{\text{obs}} = C \to \mathbb{R}_{\geq 0} \cup \{u_\epsilon\}$.

我们将位置、事件和时钟赋值上的观测映射定义为 $\mathcal{M}_L : L \to L_{\text{obs}} \cup \{l_\epsilon\}$、$\mathcal{M}_\Gamma : \Gamma \to \Sigma_{\text{obs}} \cup \{\sigma_\epsilon\} \cup \mathbb{R}_{\geq 0}$ 和 $\mathcal{M}_C : \mathcal{U} \to \mathcal{U}_{\text{obs}}$，定义如下

$$\mathcal{M}_L(l) = \begin{cases} l, & l \in L_{\text{obs}}, \\ l_\epsilon, & l \in L_{\text{uo}}, \end{cases}$$

$$\mathcal{M}_\Gamma(\gamma) = \begin{cases} \gamma, & \gamma \in \Sigma_{\text{obs}} \cup \mathbb{R}_{\geq 0}, \\ \sigma_\epsilon, & \gamma \in \Sigma_{\text{uo}}, \end{cases}$$

$$\mathcal{M}_C(u)(c) = \begin{cases} u(c), & c \in C_{\text{obs}}, \\ u_\epsilon, & c \in C_{\text{uo}}. \end{cases}$$ ■

为了计算可观测时钟赋值上的时间流逝操作，我们将加法运算扩展到域$\mathcal{U}_{\text{obs}}$。对于任意 $u \in \mathcal{U}_{\text{obs}}$ 和 $\tau \in \mathbb{R}_{\geq 0}$，赋值 $u + \tau$ 定义如下：

$$(u + \tau)(c) = \begin{cases} u(c) + \tau, & \text{if } u(c) \in \mathbb{R}_{\geq 0}, \\ u_\epsilon, & \text{if } u(c) = u_\epsilon. \end{cases}$$

基于定义 2，我们可以自然地将观测映射扩展到演化。设 $\mathcal{A} = (L, l_0, C, \Sigma, E, I)$ 是一个定时自动机，且 $\mathcal{T} = \mathcal{S}(\mathcal{A}) = (S, S_0, \Gamma, \delta)$ 是其状态图（其中$S = L \times \mathcal{U}$和 $\Gamma = \Sigma \cup \mathbb{R}_{\geq 0}$）。设 $\mathcal{M}_\rho : S \cdot (\Gamma \cdot S)^* \to S^o \cdot (\Gamma^o \cdot S^o)^*$ 表示演化上的观测映射，其中

$$S^o := (L_{\text{obs}} \cup \{l_\epsilon\}) \times \mathcal{U}_{\text{obs}}, \qquad \Gamma^o := \Sigma_{\text{obs}} \cup \{\sigma_\epsilon\} \cup \mathbb{R}_{\geq 0}.$$

我们首先将单个状态 $s = (l, u) \in S$ 的观测定义为逐分量投影 $\mathcal{M}_{\mathfrak{S}}(s) = (\mathcal{M}_L(l)\ \mathcal{M}_C(u))$。随后根据演化的结构归纳地定义映射 $\mathcal{M}_\rho$：

- 基例：对于长度为[2] 0、由单个状态 $s \in S$, $\mathcal{M}_\rho((s)) = \mathcal{M}_{\mathfrak{S}}(s)$组成的演化。
- 归纳步骤：对于演化 $\rho = \rho' \cdot \gamma \cdot s$，其中 ρ'是另一个演化，$\gamma \in \Gamma$ 是一个动作，而 $s \in S$ 是由此产生的状态：

$$\mathcal{M}_\rho(\rho' \cdot \gamma \cdot s) = \mathcal{M}_\rho(\rho') \cdot \mathcal{M}_\Gamma(\gamma) \cdot \mathcal{M}_{\mathfrak{S}}(s).$$

为简化记号，在下文中，只要参数是演化，我们就用 $\mathcal{M}$ 代替$\mathcal{M}_\rho$。分量映射保留其下标 $\mathcal{M}_L$、 $\mathcal{M}_\Gamma$和 $\mathcal{M}_C$。

然而，仅有观测映射 $\mathcal{M}$ 不足以完整捕捉观察者视角。在稠密时间设置中，观察者无法区分连续延迟与被不可观测事件打断的碎片化延迟。因此，我们定义一种等价关系，将这些差异规范化，并将语义上不同但观测上相同的行为视为等价。

定义 3（观测等价）。设 $\mathcal{A} = (L, l_0, C, \Sigma, E, I)$ 是一个定时自动机，$\mathcal{T} = (S, s_0, \Gamma, \delta)$ 是其状态图。我们基于左上下文 $\alpha \in (S \cdot \Gamma)^* \cup (S^o \cdot \Gamma^o)^*$ 和右上下文 $\beta \in (\Gamma \cdot S)^* \cup (\Gamma^o \cdot S^o)^*$定义演化上的两种基本等价关系：

1) 静默步等价（$\equiv_\epsilon$）：定义为满足以下条件的最小等价关系，该关系将 σ_ϵ-迁移不会导致原始状态或观测状态发生变化的演化视为等价。对于任意状态 $s \in S \cup S^o$：

$$\alpha\, s \xrightarrow{\sigma_\epsilon} s\, \beta \quad \equiv_\epsilon \quad \alpha\, s\, \beta.$$

2) 时间可加性、连续性和自反等价（$\equiv_\tau$）：定义为满足以下条件的最小等价关系，该关系将仅因延迟的分割或零延迟而不同的演化视为等价。对于任意状态$(l, u) \in S \cup S^o$ 以及延迟 $\tau, \tau' \in \mathbb{R}_{\geq 0}$：

$$\alpha\,(l,u) \xrightarrow{\tau} (l, u{+}\tau) \xrightarrow{\tau'} (l, u{+}\tau{+}\tau')\,\beta \quad \equiv_\tau$$
$$\alpha\,(l,u) \xrightarrow{\tau+\tau'} (l, u{+}\tau{+}\tau')\,\beta,$$
$$\alpha\, s \xrightarrow{0} s\, \beta \quad \equiv_\tau \quad \alpha\, s\, \beta.$$

若两个演化 ρ 和 ρ' 属于这两个关系之并的自反传递闭包，即$(\equiv_\epsilon \cup \equiv_\tau)^*$，则称它们观测等价，记作 $\rho \equiv_{\text{obs}} \rho'$。

在此关系下，演化 ρ 的等价类记为 $[\![\rho]\!]_{\equiv_{\text{obs}}}$。■

[2]我们用动作数来衡量演化长度。对于每个 $s \in S$，序列 $(s) \in S \cdot (\Gamma \cdot S)^*$ 的长度为 0。我们将 S 和 $S \cdot (\Gamma \cdot S)^*$ 视为不相交；特别地，$(s) \neq s$。为清晰起见，正长度的演化仍写作不带括号的形式，例如 $s_0 \cdot \gamma_0 \cdot s_1 \cdots$；括号仅用于零长度情形。

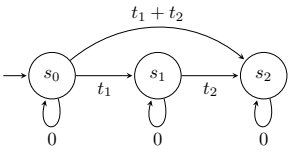


图 1：语义上不可区分的时间延迟演化

IV. EBTO 的概念

建立观测模型后，我们现在可以定义系统不透明的含义。我们引入*EBTO*，它保护整个执行历史的机密性。本文中，观测映射 $\mathcal{M}$由可观测集合的特定配置（$L_{\text{obs}}, C_{\text{obs}}, \Sigma_{\text{obs}}$）所诱导。为聚焦于不透明性的核心数学性质，除非特别讨论观测模型的变更（例如，设置 $L_{\text{obs}} = \varnothing$），否则在后续定义和定理中，我们将省略对这些集合的明确提及。

定义 4 (EBTO)。设 $\mathcal{T} = (S, S_0, \Gamma, \delta)$ 是一个状态图。子集 $\text{Gen}_s^{\mathcal{T}} \subseteq \text{Gen}^{\mathcal{T}}$是一个秘密集合，当且仅当它在时间可加性、连续性和自反等价下封闭：

$$\forall \rho \in \text{Gen}_s^{\mathcal{T}}, \quad [\![\rho]\!]_{\equiv_\tau} \subseteq \text{Gen}_s^{\mathcal{T}}.$$

若系统 $\mathcal{T}$ 相对于秘密集合$\text{Gen}_s^{\mathcal{T}}$和观测映射 $\mathcal{M}$ 满足以下条件，则称其为基于演化的定时不透明$\forall \rho \in \text{Gen}_s^{\mathcal{T}}$，$\exists \rho' \in \text{Gen}^{\mathcal{T}} \setminus \text{Gen}_s^{\mathcal{T}}$，使得 $[\![\mathcal{M}_\rho(\rho)]\!]_{\equiv_{\text{obs}}} = [\![\mathcal{M}_\rho(\rho')]\!]_{\equiv_{\text{obs}}}$.

A TA $\mathcal{A}$ 当且仅当其状态图是 *EBTO* 时，该系统才是 *EBTO*。 ■

$\text{Gen}_s^{\mathcal{T}}$ 在 $\equiv_\tau$ 下的闭包，严格来说是基于观测的物理现实，而非数学上的便利。在物理系统中，测量时间的观察者无法区分一次持续$\tau + \tau'$的连续延迟，与概念上将完全相同的延迟拆分为τ后接 τ'。同样，零延迟转移（$\xrightarrow{0}$）不耗费实际时间，也不会带来任何物理进程。因此，秘密执行可能被一个非秘密执行“隐藏”起来，二者仅在纸面上有所不同，例如任意拆分一段延迟，或插入一个在物理上毫无意义的零延迟步骤。这会使不透明性条件变得空洞地成立，让系统得以利用数学漏洞而非体现真正的物理不透明性，被判定为安全。

为说明为何这一闭包约束不可或缺，假设秘密集合不必满足这一闭包性质。在此假设下，考虑图1所示的有限符号图（SG），它展示了通过时间延迟迁移从 s_0可到达的状态。假设我们将单步演化 $s_0 \xrightarrow{t_1+t_2} s_2$ 定义为秘密。同时，由于忽略了闭包约束，我们可以将分段逐步演化 $s_0 \xrightarrow{t_1} s_1 \xrightarrow{t_2} s_2$以及具有零延迟的演化 $s_0 \xrightarrow{0} s_0 \xrightarrow{t_1+t_2} s_2$归类为非秘密。在这种情况下，尽管这样的设定在数学上是有效的，但其分析价值有限：无论我们如何选择可观测位置集合 L_{obs}、可观测动作集合 Σ_{obs}或可观测时钟集合 C_{obs}，

这三种演化在时间延迟的标准语义下仍完全无法区分。

V. 不透明性概念之间的转换

本节将根据表达能力建立定时不透明性概念的层级。我们通过构造从现有概念（如 LBTO [10] 和 ETO [14], ）到 EBTO 的归约，说明所提出的框架可作为严格更一般的语义基准，并正式证明反向结论通常不成立。

A. EBTO 与 LBTO 之间的转换

在 LBTO 中， [10], 系统行为由定时词刻画。为形式化描述观察者在此设定下的观测能力，我们回顾定时词及其投影的标准定义。

设 Σ为一个有限事件集合。一个定时词 [7]是其上的有限序列，包含若干对

$$\omega = (\sigma_1, t_1)(\sigma_2, t_2)\cdots(\sigma_n, t_n) \in (\Sigma \times \mathbb{R}_{\geq 0})^n, n \in \mathbb{N},$$

其中，每个 $\sigma_i \in \Sigma$ 都是一个事件， $t_i \in \mathbb{R}_{\geq 0}$ 是一个全局时间戳，且满足 $0 \leq t_1 \leq t_2 \leq \cdots \leq t_n$。其上的定时语言 是由 Σ上的定时词构成的集合，即 Σ， $\mathcal{L} \subseteq (\Sigma \times \mathbb{R}_{\geq 0})^*$。

给定子集 $\Sigma_{\text{obs}} \subseteq \Sigma$，关于定时词的投影 $P_{\Sigma_{\text{obs}}}$ 是一个函数

$$P_{\Sigma_{\text{obs}}} : (\Sigma \times \mathbb{R}_{\geq 0})^* \to (\Sigma_{\text{obs}} \times \mathbb{R}_{\geq 0})^*$$

满足

$$P_{\Sigma_{\text{obs}}}(\epsilon) = \epsilon$$

$$P_{\Sigma_{\text{obs}}}(\omega \cdot (\sigma, t)) = \begin{cases} P_{\Sigma_{\text{obs}}}(\omega) \cdot (\sigma, t) & \text{if } \sigma \in \Sigma_{\text{obs}} \\ P_{\Sigma_{\text{obs}}}(\omega) & \text{otherwise.} \end{cases}$$

请注意，这一定义在结构上导致了前面提到的后缀盲性，因为投影后的定时词会丢弃最后一个可观测事件之后发生的任何时间流逝。

接下来，我们建立从 LBTO 到 EBTO 的形式化归约。二者的关键区别在于，LBTO 不包含任何状态信息：EBTO 对包含位置和时钟的语义演化进行求值，而 LBTO 仅依赖定时词。为弥合这一结构性差距，我们定义映射 $\mathcal{Y}$，通过将连续延迟累积为全局时间戳，把详细的系统执行投影为可观测的定时序列。

定义 5 (将演化映射为定时词)。 设 $\mathcal{T} = (S, s_0, \Gamma, \delta)$ 是一个动作集为 $\Gamma = \Sigma \cup \mathbb{R}_{\geq 0}$ 的状态图。考虑一个生成演化

$$\rho = s_0 \xrightarrow{\gamma_0} s_1 \xrightarrow{\gamma_1} \cdots \xrightarrow{\gamma_{n-1}} s_n.$$

我们定义映射 $\mathcal{Y}$，它通过将序列投影到$(\Sigma \times \mathbb{R}_{\geq 0})^*$ 上，将 ρ 转换为定时词。令 $0 \leq k_1 < k_2 < \cdots < k_m < n$ 为与离散事件对应的迁移的有序索引，即 $\gamma_{k_j} \in \Sigma$。 ρ 的定时词定义如下：

$$\mathcal{Y}(\rho) = (\gamma_{k_1}, t_{k_1})(\gamma_{k_2}, t_{k_2})\cdots(\gamma_{k_m}, t_{k_m}),$$

其中，每个全局时间戳 t_{k_j} 都是此前所有时间延迟之和：

$$t_{k_j} = \sum_{h=0}^{k_j-1} \text{dur}(\gamma_h), \quad \textit{with} \quad \text{dur}(\gamma) = \begin{cases} \gamma, & \textit{if } \gamma \in \mathbb{R}_{\geq 0}, \\ 0, & \textit{if } \gamma \in \Sigma. \end{cases}$$

逆映射 $\mathcal{Y}^{-1}$ 将定时词 ω 映射到生成该定时词的所有演化组成的集合：

$$\mathcal{Y}^{-1}(\omega) = \{\, \rho \in \text{Gen}^{\mathcal{T}} \mid \mathcal{Y}(\rho) = \omega \,\}. \qquad \blacksquare$$

我们自然地将这些映射扩展到集合。对于演化集合 Evo $\subseteq$ Gen$^{\mathcal{T}}$，其生成语言为 $\mathcal{Y}$(Evo) ={$\mathcal{Y}(\rho)$ | $\rho \in$Evo}。反过来，对于给定的定时语言 $\mathcal{L}$，其原像是生成其中某个词的所有演化组成的集合：

$$\mathcal{Y}^{-1}(\mathcal{L}) = \bigcup_{\omega \in \mathcal{L}} \mathcal{Y}^{-1}(\omega) = \{\, \rho \in \text{Gen}^{\mathcal{T}} \mid \mathcal{Y}(\rho) \in \mathcal{L} \,\}.$$

例如，设 ρ 是一个由下式给出的有效演化：

$$\rho = s_0 \xrightarrow{1.5} s_1 \xrightarrow{a} s_2 \xrightarrow{0.7} s_3 \xrightarrow{0.3} s_4 \xrightarrow{b} s_5 \xrightarrow{0.2} s_6,$$

所得定时词为： $\mathcal{Y}(\rho)$ =$(a,\ 1.5)(b,\ 2.5)$。

这个例子展示了映射如何抽象掉中间状态（s_1， s_3， s_4），并将多个延迟步骤合并为一个全局时间戳。值得注意的是，与前面讨论的投影 $P_{\Sigma_{\text{obs}}}$ 非常相似，该映射会丢弃最终离散事件之后发生的任何时间延迟，例如，通向 s_6 的 0.2 延迟。

在 LBTO 的语境下，关注点在于系统的生成语言。为此，我们通过将映射 $\mathcal{Y}$ 应用于所有生成演化 $\mathcal{L}_{\text{gen}}(\mathcal{A})$ = $\mathcal{Y}$(Gen$^{\mathcal{T}}$)，来定义定时自动机 $\mathcal{A}$的生成语言，记作 $\mathcal{L}_{\text{gen}}(\mathcal{A})$。。接下来，我们回顾 LBTO 的定义。

定义 6 (基于语言的定时不透明性，LBTO [10])。 若定时自动机 $\mathcal{A}$ 相对于 Σ_{obs} 和秘密语言 $\mathcal{L}_s$ 满足以下条件，则称其具有基于语言的定时不透明性： $\forall \omega \in \mathcal{L}_{\text{gen}}(\mathcal{A}) \cap \mathcal{L}_s, \exists \omega' \in \mathcal{L}_{\text{gen}}(\mathcal{A}) \setminus \mathcal{L}_s$ 使得 $P_{\Sigma_{\text{obs}}}(\omega) = P_{\Sigma_{\text{obs}}}(\omega')$。 $\blacksquare$

定义 7 (转换函数，LBTO 到 EBTO)。 给定定时自动机 $\mathcal{A} = (L, l_0, C, \Sigma, E, I)$ 和秘密语言 $\mathcal{L}_s$， 转换函数为 $\mathcal{C}_{\text{LE}}(\mathcal{A}, \mathcal{L}_s) = (\mathcal{A}, \text{Gen}_s^{\mathcal{T}})$，其中秘密演化的集合是秘密语言的精确逆像：

$$\text{Gen}_s^{\mathcal{T}} = \mathcal{Y}^{-1}(\mathcal{L}_s). \qquad \blacksquare$$

此外，有效归约要求两个领域的观测模型在形式上保持一致。由于 LBTO 将观察者限制为只能访问离散事件和时间戳，因此必须限制 EBTO观察者访问位置和时钟数据（例如， $L_{\text{obs}} = \varnothing$ 和 $C_{\text{obs}} = \varnothing$）。在这一特定限制下，状态图中的观测等价可直接推出语言领域中的投影相等。也就是说，对于任意 ρ， $\rho' \in$ Gen$^{\mathcal{T}}$：

$$[\![\mathcal{M}(\rho)]\!]_{\equiv_{\text{obs}}} = [\![\mathcal{M}(\rho')]\!]_{\equiv_{\text{obs}}} \implies P_{\Sigma_{\text{obs}}}(\mathcal{Y}(\rho)) = P_{\Sigma_{\text{obs}}}(\mathcal{Y}(\rho')).$$

（形式化描述和证明见 Ap-附录 B。）

这些结构等价和观测等价直接导出了主要归约定理。

定理 1 (EBTO 对 LBTO 的充分性)。 设 $\mathcal{A}$是一个具有状态图 $\mathcal{T} = \mathcal{S}(\mathcal{A})$的定时自动机（*TA*），设 $\Sigma_{\text{obs}} \subseteq \Sigma$ 是给定的可观测事件集合，其中位置和时钟均不可观测（即$L_{\text{obs}} = \varnothing$ 和 $C_{\text{obs}} = \varnothing$），并设 $\mathcal{L}_s$ 是秘密语言。令 $(\mathcal{A}, \text{生成}_s^{\mathcal{T}}) = \mathcal{C}_{\text{LE}}(\mathcal{A}, \mathcal{L}_s)$。

若定时自动机 $\mathcal{A}$相对于 Σ_{obs} 和 $\mathcal{L}_s$ 满足 *EBTO* 条件，则它相对于 $\mathcal{M}$ 和 生成$_s^{\mathcal{T}}$满足 *LBTO* 条件。

证明。 形式化证明见附录 C。

定理 1确立了严格的单向蕴含。由于基于语言的表述存在一种根本性的结构局限，反向蕴含并不成立，我们将这种局限称为后缀盲性。具体而言，LBTO 观测映射会在最后一个可观测事件发生时截断连续时间进展，舍弃所有尾随时间延迟或后续的不可观测状态评估。在 LBTO 下，定时自动机可能仅仅因为语言投影掩盖了终端时序差异，就被判定为安全。相比之下，EBTO 中的观测等价 $\equiv_{\text{obs}}$ 严格保留时间的连续进展，能够识别出仅在尾随延迟方面有所不同的演化。

考虑图 2 所示的定时自动机，其中事件 a 可观测，事件 b 不可观测。该定时自动机生成两个定时词： $\omega_1 = (a, 1)$ 和 $\omega_2 = (a,1)(b, 100)$。设秘密语言为 $\mathcal{L}_s = \{\omega_1\}$，非秘密语言为 $\{\omega_2\}$。在 LBTO 投影下，不可观测事件 b 及其时间戳会被丢弃。因此，$P_{\Sigma_{\text{obs}}}(\omega_1) = P_{\Sigma_{\text{obs}}}(\omega_2) = (a, 1)$，该定时自动机满足 LBTO。

然而，在 EBTO 下，秘密演化集合定义为 Gen$_s^{\mathcal{T}} = \mathcal{Y}^{-1}(\{\omega_1\})$，其中包含总时间延迟为 $t \in [1, 100)$ 的所有演化。非秘密演化集合 $\mathcal{Y}^{-1}(\{\omega_2\})$ 包含满足 $t \geq 100$的演化。由于没有任何秘密演化与非秘密演化在观测上等价，观察者可以识别出秘密。因此，该定时自动机不满足 EBTO。这个例子表明，LBTO 投影会丢弃尾随延迟，因此无法检测到秘密。相比之下，EBTO 会保留这些延迟，并将该系统识别为不透明。

为正式证明这种不对称性，以下命题证明 EBTO 的表达能力严格更强，因为任何 LBTO 设置都无法捕捉仅嵌入于终止延迟中的秘密。

命题 1 (EBTO 相较于 LBTO 的严格表达能力)。 存在一个定时自动机 $\mathcal{A}$ 和一个秘密演化集合Gen$_s^{\mathcal{T}}$，使得任何可观测事件集上的 *LBTO* 秘密语言 $\mathcal{L}_s$ 都无法准确捕捉相同的秘密行为。具体而言，$\text{Gen}_s^{\mathcal{T}} \neq \mathcal{Y}^{-1}(\mathcal{L}_s)$ 对于所有可能的 $\mathcal{L}_s$均成立。

证明。 形式证明见附录 D。

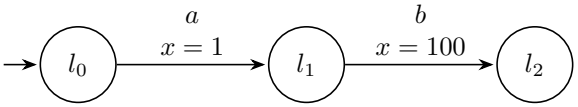


图 2：展示后缀盲性的定时自动机示例。

B. EBTO 与 ETO 之间的转换

与依赖事件序列的 LBTO 不同，ETO [14]是基于<运行 定义的，其中连续的时间延迟会合并（根据时间可加性），并根据其累积时长进行评估。

定义 8 (ETO [14])。 设 $\mathcal{A} = (L, l_0, C, \Sigma, E, I)$ 为一个定时自动机。设 $l_{\text{priv}} \in L$ 为一个私有位置， $l_f \in L$ 为一个最终位置。 $\mathcal{A}$ 的运行 运行 是由具体状态以及延迟和事件对交替组成的序列，并从初始状态 $(l_0, \mathbf{0})$开始：

$$\begin{aligned}\text{Run} = (l_0, \mathbf{0}), (d_0, e_0), (l_1, u_1), \cdots, (d_{m-1}, e_{m-1}), (l_m, u_m),\\ \cdots, (d_{n-1}, e_{n-1}), (l_n, u_n), \quad m, n \in \mathbb{N},\end{aligned}$$

其中， $d_i \in \mathbb{R}_{\geq 0}$ 表示延迟， $e_i \in \Sigma$ 表示离散事件。

运行持续时间定义为延迟之和：

$$\text{Duration}(\text{Run}) = \sum_{0 \leq i \leq n-1} d_i.$$

我们根据是否恰好访问特定位置 l_{priv} 和 l_f，定义两组运行：

1) 私有运行 访问$^{\text{priv}}(\mathcal{A})$：满足以下条件的运行集合

$$l_m = l_{\text{priv}} \wedge l_n = l_f \wedge (\forall 0 \leq i \leq n-1, l_i \neq l_f).$$

这形式化地刻画了在首次出现 l_f之前途经 l_{priv} 的运行。我们用 DVisit$^{\text{priv}}(\mathcal{A})$表示这些运行的所有持续时间构成的集合。

2) 公共运行访问$^{\overline{\text{priv}}}(\mathcal{A})$：满足以下条件的运行集合

$$\begin{aligned}l_n = l_f \wedge (\forall 0 \leq i \leq n-1, l_i \neq l_f) \wedge\\ (\forall 0 \leq j \leq n, l_j \neq l_{\text{priv}}).\end{aligned}$$

这表示到达 l_f 且从未访问过的运行 l_{priv}。我们用 DVisit 表示$^{\overline{\text{priv}}}(\mathcal{A})$ 这些运行的所有持续时间的集合。

若系统 $\mathcal{A}$ 的私有时长集合包含于公开时长集合中，则称其为执行时间不透明[3] （具体而言，即弱执行时间不透明性）：

$$\text{DVisit}^{\text{priv}}(\mathcal{A}) \subseteq \text{DVisit}^{\overline{\text{priv}}}(\mathcal{A}). \quad \blacksquare$$

为在我们提出的框架中分析 ETO，我们定义一个规范化映射。

定义 9 (规范化映射)。 我们定义规范化映射 $\Psi : \text{Gen}^{\mathcal{T}} \to Runs(\mathcal{A})$。对于任意演化 $\rho \in \text{Gen}^{\mathcal{T}}$，令 $0 \leq k_1 < k_2 < \cdots < k_m < n$ 为 ρ 中所有离散事件的索引（即 $\gamma_{k_j} \in \Sigma$）。规范化运行是由 m 步组成的序列：

$$\begin{aligned}\Psi(\rho) = s_0, (d_1, \gamma_{k_1}), s_{k_1+1}, (d_2, \gamma_{k_2}), s_{k_2+1},\\ \ldots, (d_m, \gamma_{k_m}), s_{k_m+1},\end{aligned}$$

其中，对于每个 $j \in \{1, \ldots, m\}$，延迟 d_j是从上一个离散事件 $\gamma_{k_{j-1}}$ （如果 $j = 1$，则从演化开始）到当前事件 γ_{k_j}之间所有延迟的总和。

反向函数定义如下：

$$\Psi^{-1}(\text{Run}) = \{\rho \in \text{Gen}^{\mathcal{T}} \mid \Psi(\rho) = \text{Run}\}. \quad \blacksquare$$

[3]我们关注 [14]中定义的弱执行时间不透明性概念。

请注意，如果 ρ 以时间延迟结尾，即最后一个离散事件 γ_{k_m}之后还有时间延迟，那么这段尾随持续时间不计入 $\Psi(\rho)$。

考虑一个状态图 $\mathcal{T}$ 以及涉及状态 s_0、……、s_6的生成演化 ρ：

$$\rho = s_0 \xrightarrow{0.5} s_1 \xrightarrow{1.5} s_2 \xrightarrow{a} s_3 \xrightarrow{3.0} s_4 \xrightarrow{b} s_5 \xrightarrow{4.5} s_6,$$

由此得到的规范运行是：

$$\Psi(\rho) = s_0, (2.0, a), s_3, (3.0, b), s_5.$$

此运行的总时长为 5.0。请注意， ρ 的语义时长为 9.5。这个差异揭示了结构性差异：状态图中的一般演化可以在任意时间点终止，而 ETO 运行只计算截至最终离散事件所累积的时间。在 ETO 中，运行时长计算截至首次到达最终位置 l_f 所累积的时间。为了在我们的框架中体现这一点，我们定义满足此终止条件的演化集合。令 $\mathrm{Gen}_{l_f}^{\mathcal{T}} \subseteq \mathrm{Gen}^{\mathcal{T}}$ 表示所有在首次进入 l_f时恰好终止的生成演化所构成的集合。由于 TA 中的位置变化严格由离散事件驱动，$\mathrm{Gen}_{l_f}^{\mathcal{T}}$ 中的每个演化自然都以一次离散迁移结束。因此，不存在未记录的尾随延迟，状态图中的总时长与 ETO 框架中的运行时长完全对应：$\forall \rho \in \mathrm{Gen}_{l_f}^{\mathcal{T}}$, $\mathrm{Duration}(\rho) = \mathrm{Duration}(\Psi(\rho))$.

定义10（转换函数，ETO到EBTO）。 给定一个带有 l_{priv} 和 l_f的*TA* $\mathcal{A}$，我们定义转换函数$\mathcal{C}_{\mathrm{ExE}}(\mathcal{A}, l_{\mathrm{priv}}, l_f) = (\mathcal{A}, \mathrm{Gen}_s^{\mathcal{T}})$。秘密演化集合定义为以 l_f 结束且映射到私有运行的演化子集：

$$\mathrm{Gen}_s^{\mathcal{T}} = \{\rho \in \mathrm{Gen}_{l_f}^{\mathcal{T}} \mid \Psi(\rho) \in \mathrm{Visit}^{\mathrm{priv}}(\mathcal{A})\}. \quad \blacksquare$$

有效归约要求两个领域中观察者可获取的信息保持一致。设置$L_{\mathrm{obs}} = \{l_f\}$、 $\Sigma_{\mathrm{obs}} = \varnothing$和 $C_{\mathrm{obs}} = \varnothing$ ，可确保EBTO观察者无法获知任何中间状态和离散事件，从而与ETO以持续时间为中心的关注点相匹配。在这一严格的观测模型下，观察者只能感知连续时间流，直至到达最终位置 l_f。因此，对于任意两个生成演化 $\rho, \rho' \in \mathrm{Gen}_{l_f}^{\mathcal{T}}$，它们观测等价当且仅当其总时长相等：

$$[\![\mathcal{M}(\rho)]\!]_{\equiv_{\mathrm{obs}}} = [\![\mathcal{M}(\rho')]\!]_{\equiv_{\mathrm{obs}}} \iff \mathrm{Duration}(\rho) = \mathrm{Duration}(\rho').$$

（形式化描述和证明见附录E）。

定理 2. 设 $\mathcal{A}$ 是一个定时自动机，其私有位置为 l_{priv} ，最终位置为 l_f。设 $L_{\mathrm{obs}} = \{l_f\}$、 $\Sigma_{\mathrm{obs}} = \varnothing$和 $C_{\mathrm{obs}} = \varnothing$。令 $(\mathcal{A}, \text{生成}_s^{\mathcal{T}}) = \mathcal{C}_{\mathrm{ExE}}(\mathcal{A}, l_{\mathrm{priv}}, l_f)$ 为转换后的系统。

当且仅当定时自动机 $\mathcal{A}$ 相对于观测映射 l_{priv}, l_f 具有 *ETO* 性质时，它相对于观测映射 $\mathcal{M}$ 和秘密演化 生成$_s^{\mathcal{T}}$具有 *EBTO* 性质。

证明。形式化证明见附录F。

定理 2 证明，在极简观测模型下，ETO 与 EBTO 在结构上等价，其中所有离散组件、位置、时钟和事件均不可观测（即 $\Sigma_{\mathrm{obs}} = L_{\mathrm{obs}} = C_{\mathrm{obs}} = \varnothing$）。

命题 2 (EBTO 相对于 ETO 的严格表达能力)。 存在一个 *EBTO* 实例 $(\mathcal{A}, \text{生成}_s^{\mathcal{T}})$，使得对于任意定时自动机 $\mathcal{A}'$、 l_{priv}和 l_f，($\mathcal{A}', l_{\mathrm{priv}}$和 l_f) 的 *ETO* 性质与($\mathcal{A}$, 生成$_s^{\mathcal{T}}$)的 *EBTO* 性质并不等价。

证明。 形式化证明见附录 G。

这种归约的根本障碍在于 ETO 测量机制固有的信息损失。ETO 通过一个单一的标量值——已完成运行的累积时长——来刻画系统行为。相比之下，EBTO 保留了演化的完整时间轨迹。

在本节中，我们建立了定时不透明性类别的形式层级。我们证明，EBTO 可作为统一的语义基准，同时涵盖基于语言的观测（LBTO）和基于时长的观测（ETO）。尤为重要的是，我们给出了构造性变换，表明在严格受限的观测模型下，以事件为中心和以时长为中心的表述都是所提出的基于演化的框架的严格实例。如图 3所示，这一系统性的统一证实，多种安全要求都可以在单一且连贯的方法论中得到严格分析。

六、结论

本文通过建立统一的语义框架，解决了定时不透明性领域理论碎片化的问题。我们针对定时自动机提出了一种通用观测模型，涵盖对位置、时钟和事件的部分观测。基于这一模型，我们形式化定义了 EBTO 的概念。我们通过建立不透明性类别的形式层级，证明了 EBTO 的表达能力。具体而言，我们证明 EBTO 严格蕴含 LBTO。它通过涵盖尾随时间延迟，提供了更强的验证基准；由于后缀盲性，LBTO 无法观测到这一方面。此外，我们证明，在受限观测条件下，EBTO 与 ETO 形式等价。未来的工作将利用这一框架，探究定时不透明性的可判定性边界，并确定验证所需的系统架构和观察者能力的最小限制。

人工智能使用声明

Google Gemini 仅用于语言润色和语法修正，以提高可读性。所有技术概念和分析均为作者原创。作者审阅了所有经 AI 辅助的文本，并对最终稿件承担全部责任。

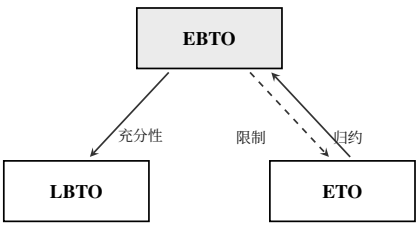


图 3：定时不透明性类别的形式层级。

参考文献

[1] H. Harkat、L. M. Camarinha-Matos、J. Goes 和 H. F. Ahmed，《网络物理系统安全：系统综述》，Comput. Ind. Eng.，第 188 卷，第 109891 页，2024 年。[2] A. Saboori 和 C. N. Hadjicostis，《通过状态估计器构造实现不透明性的监督策略》，IEEE Trans. Autom. Control，第 57 卷，第 1155–1165 页，2011 年 5 月。[3] F. Lin，《离散事件系统的不透明性及其应用》，Automatica，第 47 卷，第 496–503 页，2011 年 3 月。[4] A. Wintenberg、M. Blischke、S. Lafortune 和 N. Ozay，《用于描述和验证不透明性概念的通用基于语言的框架》，Discrete Event Dyn. Syst.，第 32 卷，第 253–289 页，2022 年 6 月。[5] Y. Xie、X. Yin 和 S. Li，《使用非确定性监督器实现不透明性的监督控制》，IEEE Trans. Autom. Control，第 67 卷，第 6567–6582 页，2021 年 12 月。[6] F. Cassez，《定时不透明性的阴暗面》，载于《国际信息安全保障会议论文集》，第 21–30 页，Springer，2009 年。[7] R. Alur 和 D. L. Dill，《定时自动机理论》，Theor. Comput. Sci.，第 126 卷，第 2 期，第 183–235 页，1994 年。[8] ´E. Andr´e、S. D´epernet 和 E. Lefaucheux，《定时不透明性的光明面》，载于《国际形式化工程方法会议论文集》，第 51–69 页，Springer，2024 年。[9] J. Klein、P. Kogel 和 S. Glesner，《离散定时自动机的不透明性验证》，载于《IEEE/ACM 第 12 届软件工程形式化方法国际会议（FormaliSE）论文集》，第 55–65 页，ACM，2024 年 4 月。[10] J. An、Q. Gao、L. Wang、N. Zhan 和 I. Hasuo，《定时自动机的不透明性》，载于《国际形式化方法研讨会论文集》，第 14933 卷，第 620–637 页，Springer，2024 年。[11] W. Deng、D. Qiu 和 J. Yang，《具有整数重置的定时自动机的初始位置不透明性和无限步不透明性》，IEEE Control Syst. Lett.，2025 年。[12] K. Zhang，《带标记实时自动机的基于状态的不透明性》，Theor. Comput. Sci.，第 987 卷，第 114373 页，2024 年 3 月。[13] M. G. Marques、R. J. Barcelos 和 J. C. Basilio，《时间区间自动机在定时离散事件系统建模中的应用及其在不透明性方面的应用》，载于 IFAC-PapersOnLine，第 56 卷，第 8654–8659 页，2023 年 7 月。[14] ´E. Andr´e、E. Lefaucheux、D. Lime、D. Marinho 和 J. Sun，《配置时序参数以确保定时自动机中的执行时间不透明性》，载于 Electron. Proc. Theor. Comput. Sci. (EPTCS)，第 392 卷，26，2023 年 10 月，1 页。–。[15] I. Ammar、Y. E. Touati、M. Yeddes 和 J. Mullins，《定时系统的有界不透明性》，J. Inf. Secur. Appl.，第 61 卷，第 102926 页，2021 年 9 月。[16] A. Rashidinejad、M. Reniers 和 M. Fabian，《使用强制事件进行定时自动机的监督控制综合》，IEEE Trans. Autom. Control，第 69 卷，第 1074–1080 页，2023 年 2 月。[17] E. Fares、J.-P. Bodeveix、M. Filali-Amine 和 M. Garnacho，《一种检查定时系统模拟的自动化技术》，载于《第 11 届自动化验证与分析技术国际研讨会（ATVA）论文集》，第 71–86 页，Springer，2013 年 10 月。[18] A. Saboori 和 C. N. Hadjicostis，《离散事件系统中的安全性和不透明性概念》，载于《第 46 届 IEEE 决策与控制会议（CDC）论文集》，第 5056–5061 页，IEEE，2007 年。[19] Y. Ru 和 C. N. Hadjicostis，《由部分可观测佩特里网建模的离散事件系统中的故障诊断》，Discrete Event Dyn. Syst.，第 551–575 页，2009 年。[20] S. Shu、F. Lin 和 H. Ying，《离散事件系统的可检测性》，IEEE Trans. Autom. Control，第 2356–2359 页，2007 年。

附录

A. 引理 1 的证明

引理 1. 设 $\mathcal{M}$ 为演化上的观测映射，且 $\mathcal{Y}$ 为从演化到定时词的映射（定义 5）。对于任意演化 ρ，以下结论成立：

$$\mathcal{Y}\big(\mathcal{M}(\rho)\big) \;=\; P_{\Sigma_{\text{obs}}}\big(\mathcal{Y}(\rho)\big).$$

证明。 考虑任意演化 $\rho = s_0 \xrightarrow{\gamma_0} s_1 \xrightarrow{\gamma_1} \cdots \xrightarrow{\gamma_{n-1}} s_n$。

首先，我们注意到， $\mathcal{Y}$计算出的全局时间戳对于 ρ 和 $\mathcal{M}$ 是相同的（ρ）。观测映射 $\mathcal{M}$将不可观测事件映射为 σ_ϵ ，但保持时间延迟 $\tau \in \mathbb{R}_{\geq 0}$ 不变。由于对于任意离散事件$\sigma \in \Sigma$，$\text{dur}(\sigma) = 0$，且自然有 $\text{dur}(\sigma_\epsilon) = 0$，因此在任意步骤 k，累积持续时间$t_k = \sum_{h=0}^{k-1} \text{dur}(\gamma_h)$保持不变。

这意味着我们只需比较事件-时间戳对的序列。令 $K = \{k \mid \gamma_k \in \Sigma\}$ 为 ρ 中发生离散事件的索引集合。

- 右侧：项 $\mathcal{Y}(\rho)$ 生成所有 $k \in K$ 对应的序列，包含配对 $(\gamma_k,\ t_k)$。投影函数 $P_{\Sigma\text{ 观测}}$ 仅保留满足 $\gamma_k \in \Sigma\text{ 观测}$ 的配对。

- 左侧：映射 $\mathcal{M}$ 在满足$\gamma_k \in \Sigma_{\text{不可观测}}$时将 γ_k 转换为 σ_ϵ，在满足$\gamma_k \in \Sigma_{\text{可观测}}$时则保持 γ_k 不变。根据定义 5， $\mathcal{Y}$ 通过收集严格处于 Σ 中的动作来构造定时词。由于 $\sigma_\epsilon \notin \Sigma$，对应于 $\Sigma_{\text{不可观测}}$ 的索引不会包含在结果中。因此， $\mathcal{Y}(\mathcal{M}(\rho))$ 恰好由满足 $k \in K$ 且 $\gamma_k \in \Sigma_{\text{可观测}}$ 的配对 $(\gamma_k,\ t_k)$ 组成。

■

B. 引理 2 的证明

引理 2 (定时词的观测对应)。设 $\mathcal{A}$ 是一个位置和时钟不可观测的定时自动机（$L_{\text{obs}} = \varnothing$且 $C_{\text{obs}} = \varnothing$）。对于任意两个演化$\rho$，$\rho' \in \text{Gen}^{\mathcal{T}}$，若它们在 *EBTO* 框架中的观测等价，则它们生成的定时词的投影相同：

$$\begin{aligned}&[\![\mathcal{M}(\rho)]\!]_{\equiv_{\text{obs}}} = [\![\mathcal{M}(\rho')]\!]_{\equiv_{\text{obs}}}\\ &\implies P_{\Sigma_{\text{obs}}}(\mathcal{Y}(\rho)) = P_{\Sigma_{\text{obs}}}(\mathcal{Y}(\rho')).\end{aligned}$$

证明。设 ρ 和 ρ' 是任意两个演化。根据引理1，我们有以下恒等式 $P_{\Sigma_{\text{obs}}}(\mathcal{Y}(\rho)) = \mathcal{Y}(\mathcal{M}(\rho))$。因此，要证明的蕴含关系可归结为证明：

$$[\![\mathcal{M}(\rho)]\!]_{\equiv_{\text{obs}}} = [\![\mathcal{M}(\rho')]\!]_{\equiv_{\text{obs}}} \implies \mathcal{Y}(\mathcal{M}(\rho)) = \mathcal{Y}(\mathcal{M}(\rho')).$$

观测等价 $\equiv_{\text{obs}}$ 定义为静默步等价（$\equiv_\epsilon$）以及时间可加性、连续性和自反等价（$\equiv_\tau$）的闭包。我们证明，映射 $\mathcal{Y}$ 在对观测序列 $\mathcal{M}$（ρ）应用两种基本操作时保持不变。

1) 在 $\equiv_\epsilon$下的不变性：假设 $\mathcal{M}$（ρ'）是通过插入或删除不可观测事件（映射为 σ_ϵ）从$\mathcal{M}$（ρ）推导而来。回顾一下， $\mathcal{Y}$ 通过收集满足 $\sigma_k \in \Sigma_{\text{obs}}$的数对（$\sigma_k$，$t_k$）来构造定时词。

- 事件序列：由于$\sigma_\epsilon \notin \Sigma_{\text{obs}}$，插入或删除 σ_ϵ 不会改变记录的离散事件序列。

- 时间戳：全局时间戳 t_k 是此前所有持续时间之和。由于 $\text{dur}(\sigma_\epsilon) = 0$，累积持续时间始终保持不变。

Thus, $\mathcal{Y}(\mathcal{M}(\rho)) = \mathcal{Y}(\mathcal{M}(\rho'))$.

2) 在 $\equiv_\tau$ 下的不变性：假设 $\mathcal{M}(\rho')$ 是通过合并两个连续的延迟 d_1，d_2 得到的，$\mathcal{M}(\rho)$ 被转换为 $d = d_1 + d_2$（或将它们拆分），或者插入或移除零延迟（$d = 0$）。考虑在这些时间相关修改之后发生的任意可观测事件 σ_k。其时间戳 t_k 计算为此前所有持续时间之和

。根据 $\mathbb{R}_{\geq 0}$ 中加法的结合律和加法单位元性质：

$$\cdots + d_1 + d_2 + \cdots = \cdots + (d_1 + d_2) + \cdots,$$
$$\text{and} \quad \cdots + d + 0 + \cdots = \cdots + d + \cdots.$$

因此，在 $\mathcal{M}(\rho)$中，所有后续事件的计算所得全局时间戳均相同，而 $\mathcal{M}(\rho')$. Thus, $\mathcal{Y}(\mathcal{M}(\rho)) = \mathcal{Y}(\mathcal{M}(\rho'))$.

由于对于 $\equiv_\epsilon$ 或$\equiv_\tau$的任何单个步骤，$\mathcal{Y}$ 都会得到相同结果，因此根据归纳法，它对于同一等价类中的任意两个观测都会得到相同结果。因此，$\mathcal{Y}(\mathcal{M}(\rho)) =\mathcal{Y}(\mathcal{M}(\rho'))$，这意味着 $P_{\Sigma_{\text{obs}}}(\mathcal{Y}(\rho)) = P_{\Sigma_{\text{obs}}}(\mathcal{Y}(\rho'))$。■

C. 定理 1 的证明

定理 1 (EBTO 对 LBTO 的充分性)。 设 $\mathcal{A}$是一个具有状态图 $\mathcal{T} = \mathcal{S}(\mathcal{A})$ 的定时自动机，设 $\Sigma_{\text{obs}} \subseteq \Sigma$ 是给定的可观测事件集合，位置和时钟均不可观测，即，$L_{\text{obs}} = \varnothing$ 且 $C_{\text{obs}} = \varnothing$，并设 $\mathcal{L}_s$ 是一个秘密语言。令 $(\mathcal{A}, \text{生成}_s^{\mathcal{T}}) = \mathcal{C}_{\text{LE}}(\mathcal{A}, \mathcal{L}_s)$。

若定时自动机 $\mathcal{A}$关于 Σ_{obs} 和 $\mathcal{L}_s$ 是 *LBTO*，则当且仅当它关于 $\mathcal{M}$ 和生成$_s^{\mathcal{T}}$是 *EBTO*。

证明。假设定时自动机 $\mathcal{A}$ 关于秘密演化集合 $\text{Gen}_s^{\mathcal{T}}$ 和观测映射 $\mathcal{M}$ 是 EBTO。令 $\omega \in \mathcal{L}_{\text{gen}}(\mathcal{A}) \cap \mathcal{L}_s$ 为任意生成的秘密定时词。

为证明 $\mathcal{A}$ 是 LBTO，我们必须找到一个非秘密定时词 $\omega' \in \mathcal{L}_{\text{gen}}(\mathcal{A}) \setminus \mathcal{L}_s$，使得 $P_{\Sigma_{\text{obs}}}(\omega) = P_{\Sigma_{\text{obs}}}(\omega')$。

由于 $\omega \in \mathcal{L}_{\text{gen}}(\mathcal{A})$，存在一个生成演化 $\rho \in \text{Gen}_s^{\mathcal{T}}(\mathcal{Y}^{-1}\mathcal{L}_s)$，使得 $\mathcal{Y}\rho = \omega$。因为 $\omega \in \mathcal{L}_s$ 和 $\rho \in \text{Gen}_s^{\mathcal{T}}(\mathcal{Y}^{-1}\mathcal{L}_s)$，所以有 ρ。因此，这是一个秘密演化。

根据 $\mathcal{A}$ 是 EBTO 这一假设，存在一个演化$\rho' \in \text{Gen}_s^{\mathcal{T}}$，使得 $\rho' \notin \text{Gen}_s^{\mathcal{T}}$，且 $[\![\mathcal{M}(\rho)]\!]_{\equiv_{\text{obs}}} = [\![\mathcal{M}(\rho')]\!]_{\equiv_{\text{obs}}}$。

令 $\omega' = \mathcal{Y}(\rho')$。由于 $\rho' \notin \text{Gen}_s^{\mathcal{T}}$，可得 $\omega' \notin \mathcal{L}_s$。因此，$\omega'$ 是 $\mathcal{L}_{\text{gen}}(\mathcal{A})$中的非秘密定时词。

应用引理2，演化的观测等价意味着它们的投影定时词相等：

$$P_{\Sigma_{\text{obs}}}(\mathcal{Y}(\rho)) = P_{\Sigma_{\text{obs}}}(\mathcal{Y}(\rho')).$$

代入 $\omega = \mathcal{Y}(\rho)$和 $\omega' = \mathcal{Y}(\rho')$，得到 $P_{\Sigma_{\text{obs}}}(\omega) = P_{\Sigma_{\text{obs}}}(\omega')$。

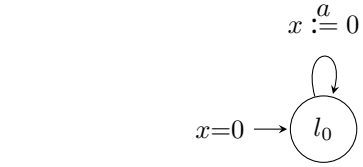
对于每个生成的秘密定时词 ω，都存在一个生成的非秘密定时词 ω'，其投影与之相同。根据定义，定时自动机 $\mathcal{A}$ 是 LBTO。■

D. 命题 1 的证明

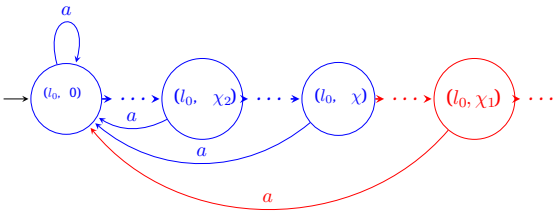
命题 1 (EBTO 相较于 LBTO 的严格表达能力)。 存在一个定时自动机 $\mathcal{A}$ 以及一个秘密演化集合$\text{Gen}_s^{\mathcal{T}}$，使得任何 *LBTO* 秘密语言 $\mathcal{L}_s$ 都无法在任何可观测事件集上精确刻画相同的秘密行为。具体而言，$\text{Gen}_s^{\mathcal{T}} \neq \mathcal{Y}^{-1}(\mathcal{L}_s)$ 对于所有可能的 $\mathcal{L}_s$。

证明。 我们构造一个反例，利用定时词的后缀盲性。

考虑一个定时自动机 $\mathcal{A}$，如图 4a所示，其中包含 $L = \{l_0\}$，$\Sigma = \{a\}$，以及一个时钟 x。唯一的边为 $(l_0, a, \text{true}, \{x\}, l_0)$，其上带有 $I(l_0) = \text{true}$。令 $\mathcal{T} = \mathcal{S}(\mathcal{A})$ 为其语义图。图 $\mathcal{T}$展示了其一部分，见图 4b。



(a) 定时自动机 $\mathcal{A}$



(b) 语义图片段 $\mathcal{T}$

图4：后缀盲性的反例：（a）展示了定时自动机的结构，（b）展示了语义图中的状态。蓝色状态表示非秘密行为（$\tau \leq \chi$），红色状态表示秘密行为（$\tau > \chi$）。

我们将 EBTO 秘密演化 $\text{Gen}_s^{\mathcal{T}}$ 定义为以事件 a 结束，且其后跟有大于常数 $\chi \in \mathbb{R}_{>0}$ 的尾随延迟的演化集合：

$$\text{Gen}_s^{\mathcal{T}} = \bigcup \left\{ [\![\rho]\!]_{\equiv_\tau} \;\middle|\; \rho = \rho_{\text{pre}} \xrightarrow{a} (l_0, 0) \xrightarrow{\tau} (l_0, \tau) \wedge \tau > \chi \right\}.$$

考虑由 $\mathcal{T}$生成的两个演化 ρ_1 和 ρ_2：

- $\rho_1 = (l_0, 0) \xrightarrow{a} (l_0, 0) \xrightarrow{\chi_1} (l_0, \chi_1)$，其中 $\chi_1 > \chi$。根据定义，$\rho_1 \in \text{Gen}_s^{\mathcal{T}}$。
- $\rho_2 = (l_0, 0) \xrightarrow{a} (l_0, 0) \xrightarrow{\chi_2} (l_0, \chi_2)$，其中 $\chi_2 \leq \chi$。根据定义，$\rho_2 \notin \text{Gen}_s^{\mathcal{T}}$。

应用映射 $\mathcal{Y}$后，由于尾随延迟不会产生离散事件，两个演化生成相同的定时词：

$$\mathcal{Y}(\rho_1) = (a, 0) = \mathcal{Y}(\rho_2).$$

令 $\omega = (a, 0)$。反设存在一个秘密语言 $\mathcal{L}_s$，使得 Gen$_s^{\mathcal{T}} = \mathcal{Y}^{-1}(\mathcal{L}_s)$。我们对 $\mathcal{L}_s$评估ω：

- 如果 $\omega \in \mathcal{L}_s$，那么 $\mathcal{Y}^{-1}(\mathcal{L}_s)$必须包含所有映射到 ω的演化。因此，$\rho_2 \in \mathcal{Y}^{-1}(\mathcal{L}_s)$。然而，$\rho_2 \notin \text{Gen}_s^{\mathcal{T}}$，这导致矛盾。
- 如果 $\omega \notin \mathcal{L}_s$，那么 $\mathcal{Y}^{-1}(\mathcal{L}_s)$不能包含任何映射到 ω的演化。因此，$\rho_1 \notin \mathcal{Y}^{-1}(\mathcal{L}_s)$。然而，$\rho_1 \in \text{Gen}_s^{\mathcal{T}}$，这导致矛盾。

因此，不存在这样的 $\mathcal{L}_s$。EBTO 可以指定基于持续时间的后缀秘密，而这类秘密在结构上无法用 LBTO 表示。■

E. 引理3的证明

引理 3 (最终可达性的观测对应关系)。 设 $\mathcal{A}$ 是一个具有最终位置的定时自动机 l_f。在仅最终位置可观测的观测模型（$L_{\text{obs}} = \{l_f\}$）下，所有事件和时钟均不可观测

($\Sigma_{\text{obs}} = \varnothing$, $C_{\text{obs}} = \varnothing$)，对于任意两个演化 $\rho, \rho' \in \text{Gen}_{l_f}^{\mathcal{T}}$，它们观测等价，当且仅当它们的总持续时间相等：

$$[\![\mathcal{M}(\rho)]\!]_{\equiv_{\text{obs}}} = [\![\mathcal{M}(\rho')]\!]_{\equiv_{\text{obs}}} \iff \text{Duration}(\rho) = \text{Duration}(\rho').$$

证明。根据定义，$\rho, \rho' \in \text{Gen}_{l_f}^{\mathcal{T}}$ 在终止前始终处于不可观测位置，并恰好在首次进入 l_f 时终止。它们的映射观测 $\mathcal{M}(\rho)$ 和 $\mathcal{M}(\rho')$ 由一个初始不可观测状态 (l_ϵ, u_ϵ) 构成，其中穿插着不可观测事件 σ_ϵ 和时间延迟，最终以迁移到 (l_f, u_ϵ) 结束。

($\Longrightarrow$) 假设 $[\![\mathcal{M}(\rho)]\!]_{\equiv_{\text{obs}}} = [\![\mathcal{M}(\rho')]\!]_{\equiv_{\text{obs}}}$。等价关系 $\equiv_{\text{obs}}$ 适用 $\equiv_\epsilon$（添加或移除持续时间为 0 的 σ_ϵ）和 $\equiv_\tau$（拆分或合并延迟）。这些操作保持累计时间不变。由于两种观测都以相同的、到达 l_f 的可观测状态变化结束，因此该可观测状态变化之前累计的总时间相等。因此，持续时间(ρ) =持续时间(ρ')。

($\Longleftarrow$) 假设持续时间(ρ) = 持续时间(ρ') = d。对于 $\mathcal{M}(\rho)$ 和 $\mathcal{M}(\rho')$，所有中间离散迁移都发生在不可观测位置之间，从而得到 $(l_\epsilon, u_\epsilon) \xrightarrow{\sigma_\epsilon} (l_\epsilon, u_\epsilon)$。应用 $\equiv_\epsilon$ 后，我们移除所有这些中间 σ_ϵ 符号。应用 $\equiv_\tau$ 后，我们合并所有分段延迟。然而，最终迁移进入 l_f，这意味着可观测状态从 (l_ϵ, u_ϵ) 变化为 (l_f, u_ϵ)。因此，不能应用等价关系 $\equiv_\epsilon$ 来消除这一特定迁移。两个映射观测都严格归约为相同的规范序列：

$$(l_\epsilon, u_\epsilon) \xrightarrow{d} (l_\epsilon, u_\epsilon) \xrightarrow{\sigma_\epsilon} (l_f, u_\epsilon).$$

因此，$[\![\mathcal{M}(\rho)]\!]_{\equiv_{\text{obs}}} = [\![\mathcal{M}(\rho')]\!]_{\equiv_{\text{obs}}}$。 ■

F. 定理 2 的证明

定理 2 (ETO到EBTO的归约)。设 $\mathcal{A}$是一个具有私有位置 l_{priv} 和最终位置 l_f。设 $L_{\text{obs}} = \{l_f\}$，$\Sigma_{\text{obs}} = \varnothing$，以及 $C_{\text{obs}} = \varnothing$。设 $(\mathcal{A}, \text{Gen}_s^{\mathcal{T}}) = \mathcal{C}_{\text{ExE}}(\mathcal{A}, l_{\text{priv}}, l_f)$ 是转换后的系统。

定时自动机 $\mathcal{A}$ 是关于 l_{priv}, l_f 的 *ETO*，当且仅当它关于观测映射 $\mathcal{M}$ 和秘密演化 $\text{Gen}_s^{\mathcal{T}}$ 是 *EBTO*。

证明。($\Longrightarrow$) 假设 $\mathcal{A}$ 是 ETO。设 $\rho \in \text{Gen}_s^{\mathcal{T}}$ 为任意秘密演化。根据定义，$\rho \in \text{Gen}_{l_f}^{\mathcal{T}}$ 并访问 l_{priv}。其持续时间为 $d = \text{Duration}(\rho)$。

根据 ETO 的定义，这一私有运行的存在意味着 $\text{Visit}^{\text{priv}}(\mathcal{A})$ 中存在一个持续时间相同的公共运行 d。设 ρ' 为生成此公共运行的演化。由于 ρ' 在进入 l_f 时终止，$\rho' \in \text{Gen}_{l_f}^{\mathcal{T}}$。由于它没有访问 l_{priv}，$\rho' \notin \text{Gen}_s^{\mathcal{T}}$。

对于 ρ 和 ρ'，我们已证明 $\rho, \rho' \in \text{Gen}_{l_f}^{\mathcal{T}}$ 以及 持续时间(ρ) = 持续时间 (ρ')。由引理 3，可得 $[\![\mathcal{M}(\rho)]\!]_{\equiv_{\text{obs}}} = [\![\mathcal{M}(\rho')]\!]_{\equiv_{\text{obs}}}$。系统 $\mathcal{A}$ 是 EBTO。

($\Longleftarrow$) 假设 $\mathcal{A}$ 是 EBTO。令 $\text{Run}_{\text{priv}} \in \text{Visit}^{\text{priv}}(\mathcal{A})$ 为任意一个持续时间为 d 的私有运行。根据 $\mathcal{C}_{\text{ExE}}$ 的定义，存在相应的秘密演化 $\rho \in \text{Gen}_s^{\mathcal{T}}$，其终止于 l_f，且 $\text{Duration}(\rho) = d$。

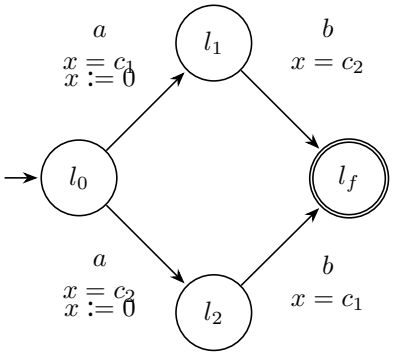


图 5：定时自动机 $\mathcal{A}$ 展示了时钟约束上的路径依赖。

由于 $\mathcal{A}$ 是 EBTO，因此存在一种演化 $\rho' \in \text{Gen}^{\mathcal{T}}$，使得 $\rho' \notin \text{Gen}_s^{\mathcal{T}}$ 且 $[\![\mathcal{M}(\rho)]\!]_{\equiv_{\text{obs}}} = [\![\mathcal{M}(\rho')]\!]_{\equiv_{\text{obs}}}$。

由于 $\rho \in \text{Gen}_{l_f}^{\mathcal{T}}$，其映射观测 $\mathcal{M}(\rho)$记录了一次可观测的位置变化，并且恰好在终止时间进入 l_f d。由于观测等价（$\equiv_{\text{obs}}$）严格保留可观测状态变化的发生及其时间，$\mathcal{M}(\rho')$也必须恰好在时间 d首次且仅一次进入 l_f，之后不再发生延迟。这保证了 ρ' 在进入 l_f时终止，从而得到 $\rho' \in \text{Gen}_{l_f}^{\mathcal{T}}$ 和持续时间（ρ'） $= d$。

由于 $\rho' \in \text{Gen}_{l_f}^{\mathcal{T}} \setminus \text{Gen}_s^{\mathcal{T}}$，这意味着 ρ' 不会访问 l_{priv}。因此，从 ρ' 中提取的运行 $\Psi(\rho')$是 $\text{Visit}^{\text{priv}}(\mathcal{A})$中的有效公共运行，持续时间为 d。因此，$\overline{\text{DVisit}^{\text{priv}}(\mathcal{A})} \subseteq \text{DVisit}^{\text{priv}}(\mathcal{A})$。系统 $\mathcal{A}$ 是 ETO。 ■

G. 命题 2 的证明

命题 2 (EBTO 相对于 ETO 的严格表达能力)。存在一个 *EBTO* 实例 $(\mathcal{A}, \text{Gen}_s^{\mathcal{T}})$ 使得对于任意 *TA* $\mathcal{A}'$、l_{priv}和 l_f，$(\mathcal{A}', l_{\text{priv}}$和 $l_f)$ 的 *ETO* 性质不等价于 $(\mathcal{A}, \text{Gen}_s^{\mathcal{T}})$的 *EBTO* 性质。

证明。我们构造一个反例，其中保密性取决于延迟的非交换时间顺序，而这种顺序会被 ETO 中的求和消除。

考虑图 5 所示的定时自动机，$\mathcal{A} = (L, l_0, C, \Sigma, E, I)$定义如下：

- $L = \{l_0, l_1, l_2, l_f\}$；$C = \{x\}$；$\Sigma = \{a, b\}$；$I(l)$ 对所有 l 均为 true。
- 令 $c_1, c_2 \in \mathbb{R}_{>0}$ 为两个常数，使得 $c_1 \neq c_2$。
- 边的集合 E 构成两条路径：
  - *Path 1:* $l_0 \xrightarrow{a, x=c_1, \{x\}} l_1$ and $l_1 \xrightarrow{b, x=c_2, \varnothing} l_f$.
  - *Path 2:* $l_0 \xrightarrow{a, x=c_2, \{x\}} l_2$ and $l_2 \xrightarrow{b, x=c_1, \varnothing} l_f$.

该定时自动机生成两条严格演化：

- ρ_1 (via l_1):

$$\rho_1 = (l_0, 0) \xrightarrow{c_1} (l_0, c_1) \xrightarrow{a} (l_1, 0) \xrightarrow{c_2} (l_1, c_2) \xrightarrow{b} (l_f, c_2).$$

- ρ_2 (via l_2):

$$\rho_2 = (l_0, 0) \xrightarrow{c_2} (l_0, c_2) \xrightarrow{a} (l_2, 0) \xrightarrow{c_1} (l_2, c_1) \xrightarrow{b} (l_f, c_1).$$

令 $\text{Gen}_s^{\mathcal{T}} = \{\rho_1\}$, $\Sigma_{\text{obs}} = \{a, b\}$，$L_{\text{obs}} = \varnothing$，以及 $C_{\text{obs}} = \varnothing$。由于 $c_1 \neq c_2$，因此 $[\![\mathcal{M}(\rho_1)]\!]_{\equiv_{\text{obs}}} \neq [\![\mathcal{M}(\rho_2)]\!]_{\equiv_{\text{obs}}}$。因此，该定时自动机不是 EBTO。

为了尝试在 ETO 中将 ρ_1 作为秘密，我们将 $l_{\text{priv}} = l_1$ 和最终位置设为 l_f。

- 私有运行 $\Psi(\rho_1)$ 的持续时间为 $c_1 + c_2$。
- 公共运行 $\Psi(\rho_2)$ 的持续时间为 $c_2 + c_1$。由于 $\mathbb{R}_{\geq 0}$ 中加法满足交换律，$c_1 + c_2 = c_2 + c_1$。因此，$\text{DVisit}^{\text{私有}}(\mathcal{A}) \subseteq \text{DVisit}^{\text{私有}}(\mathcal{A})$，且该定时自动机属于 ETO。即使采用严格演化和理想位置标记，ETO 在结构上仍无法识别时间间隔的排列，而 EBTO 则能正确识别信息泄漏。■