arXiv:2302.14546v2 [cs.LO] 3 Mar 2023

# 通信混合程序动态逻辑

Marvin Brieger[1[0000−0001−9656−2830]]、Stefan Mitsch[2[0000−0002−3194−9759]]、Andr´e Platzer[2,3[0000−0001−7238−5710]]

[1] 德国慕尼黑大学[2] 美国匹兹堡卡内基梅隆大学[3] 德国卡尔斯鲁厄理工学院
marvin.brieger@sosy.ifi.lmu.de smitsch@cs.cmu.edu platzer@kit.edu

摘要。本文提出一种动态逻辑 $d\mathcal{L}_{\text{CHP}}$，用于对通信混合程序（CHP）进行组合式演绎验证。CHP通过添加用于通信和并行性的CSP风格算子，超越了混合系统传统的离散与连续混合动力学。本文提出一种组合证明演算，通过假设—承诺推理，在动态逻辑中模块化地验证CHP（包括其并行组合），并依据其子程序的证明进行验证。与霍尔风格的假设—承诺不同，$d\mathcal{L}_{\text{CHP}}$ 通过为通信原语显式引入记录器变量，支持直观的符号执行。由于 $d\mathcal{L}_{\text{CHP}}$ 是微分动态逻辑 $d\mathcal{L}$的保守扩展，因此可以与 $d\mathcal{L}$证明演算以及 $d\mathcal{L}$关于微分方程不变式的完备公理化可靠地结合使用。

关键词：组合式验证 · 混合系统 · 并行程序 · 微分动态逻辑 · 假设—承诺推理 · CSP

## 1 引言

信息物理系统（CPS）验证 [1, 2, 12, 30] 和并行程序验证 [3, 20, 27, 38] 在安全关键型应用中十分普遍，且涉及诸多技术细节，因此都面临着重要挑战。CPS 验证的复杂性源于其离散控制决策与微分方程之间微妙的相互作用。并行程序验证的复杂性则来自并行组件之间因状态或通信依赖关系而产生的同步，这种同步会引发错综复杂的交互。然而，将二者结合起来会带来本质上的复杂性，因为并行 CPS 总是相互依赖的：它们始终通过共享同一全局时间而隐式同步。此外，许多现实世界中的 CPS 包含异构子系统，其控制器并非以锁步方式运行，且其通信可能不可靠（见图 1）。不同于混合系统模型检验 [2, 4, 8, 23]——即使缩减子自动机的规模，也仍需计算规模可观的通信并行自动机的乘积——演绎方法能够真正实现组合式处理。然而，现有的演绎验证方法无法妥善应对上述

挑战，因为它们仅适用于齐次子系统 [32], 特定的组件形状和交互模式 [19,22,26], 不支持符号执行 [10,21,41],，或不具备组合性 [10,21,41],；即使明确尝试实现组合性 [10,41]，最终也会再次失去组合性。

无论是通过分别推理离散、连续和通信行为来驾驭复杂性的组合性，还是表达模型的通用性，抑或是提升演绎推理可行性的符号执行，对于实用方法都不可或缺。因此，为了应对这三项挑战，本文提出 $d\mathcal{L}_{\text{CHP}}$，一种用于通信混合程序（CHP）的动态逻辑。它在微分动态逻辑 $d\mathcal{L}$（用于微分方程混合程序 [30, 31, 33, 34] ）的基础上，扩展了 CSP 风格的并行组合和消息传递通信运算符 [14, 15] ，以及假设—承诺（ac）推理 [25,43]。并行 CHP 不能共享状态，但可以通信。它们在全局时间下同步运行，且通信是瞬时的。

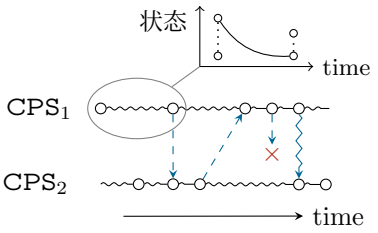


图 1：以下对象之间的交互 $\text{CPS}_1$ 和 $\text{CPS}_2$ 具有（延迟）（）、有损（）以及含噪（）通信。离散变化（）独立于并行中的离散变化，除非发生同步。连续演化（）不会被并行离散行为中断。

关于并行性推理有两种基本方法。并行性既可以通过展开其显式操作语义来理解，也可以通过其指称语义来理解，后者通过匹配各子程序在状态相应部分上的行为，隐式地刻画并行行为。基于操作语义的验证会展开数量呈指数级增长的所有可能交错，例如混合自动机 [2] 或混合 CSP [10,41]。这类方法虽能在表面上缓解状态空间爆炸，但在缩减子自动机的规模后，最终总是诉诸积自动机 [4,8,13],；或者只是推迟了对数量呈指数级增长的轨迹交错进行推理的负担 [10,41] ，因为它揭示了子程序的内部结构 [41]。相比之下，如果语义具有组合性，且与预期的推理方式契合，那么借助假设-承诺推理 [43,44], ，基于指称语义的验证对于离散程序而言便具有组合性。本文将假设-承诺推理推广，以便将其融入组合式混合系统逻辑 [30,31,33,34]。

我们的核心贡献是针对 $d\mathcal{L}_{\text{CHP}}$ 的一种可靠组合证明演算。为了对并行通信进行组合式验证，该演算通过显式的假设—承诺模态 $[\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi$ 将假设-承诺推理嵌入动态逻辑。假设—承诺模态表达的是：对于 $\alpha$ 的所有运行，只要其输入通信满足假设 A，输出通信就满足承诺 C，并且 $\psi$ 在最终状态下成立。公式 A 和 C 描述了 $\alpha$ 的通信行为，而

如果各子程序的契约彼此一致，这些公式便可实现并行组合。关键在于，这些公式通过历史变量直接与通信历史接口相连，因此，正如底层指称语义中那样，通信可以在并行组合公理中保持隐式。由于我们证明了 $d\mathcal{L}_{\text{CHP}}$ 是 $d\mathcal{L}$ 的保守扩展，它继承了 $d\mathcal{L}$ 对微分方程不变式 [35] 的完备公理化。

与基于霍尔逻辑的方法不同，我们的演算支持逐条语句进行符号执行，而不是反向执行语句。由于执行通信原语会扩展已有历史，因此新的历史状态需要一个新名称。因此，直接照搬带有一个专用于通信历史的变量的 Hoare 风格的假设-承诺推理并不可靠。相反， $d\mathcal{L}_{\text{CHP}}$ 通过记录变量协调假设-承诺推理与符号执行，这些记录变量的演化可以像我们的通信公理那样在推理过程中维护。

总之，我们提出了首个真正组合式的通信并行混成系统模型验证方法，并证明了其可靠性。我们的逻辑处理将离散、连续和通信推理的核心内容分别提炼为公理，与以往方法相比，这些公理简单且模块化 [21, 41]。尽管由于前缀闭合的动态语义、由全局时间和记录变量导致的微妙静态语义，以及动态逻辑中公式与程序的相互依赖，技术推导颇具挑战性，但这些细节最终仍可隐藏在底层。我们通过一个自动驾驶示例展示了 $d\mathcal{L}_{\text{CHP}}$ 及其证明演算的灵活性；该示例考虑了有损通信这一挑战，其中一辆follower汽车与 leader 汽车通信以组成车队。

## 2 通信混合程序的动态逻辑

我们介绍 $d\mathcal{L}_{\text{CHP}}$，这是一种用于推理通信混合程序（CHP）的动态逻辑。CHP 将 $d\mathcal{L}$ 的混合程序 [30, 33, 34] 与通信原语以及类似于 CSP [14, 15]的并行算子结合起来。在逻辑方面， $d\mathcal{L}_{\text{CHP}}$ 将假设-承诺推理 [25, 43, 44] 引入 $d\mathcal{L}$的动态逻辑框架 [11] ，从而能够以保留符号执行这一直观推理原则的方式，对通信进行组合推理。

### 2.1 语法

该语法使用信道名称 $\Omega$ 和变量 $V = V_{\mathbb{R}} \cup V_{\mathbb{N}} \cup V_{\mathcal{T}}$，其中实变量 $V_{\mathbb{R}}$、整数变量 $V_{\mathbb{N}}$ 和轨迹变量 $V_{\mathcal{T}}$两两不相交。变量 $\mu \in V_{\mathbb{R}}$ 被指定用于反映全局时间。按照约定， $x$、$y$、$t \in V_{\mathbb{R}}$、 $n$、$n_i \in V_{\mathbb{N}}$、 $h$、$h_i \in V_{\mathcal{T}}$、 $ch$、$ch_i \in \Omega$以及 $z\, z_i \in V$。公式和程序中自由变量 $FV(\cdot)$与约束变量 $BV(\cdot)$的概念，按照语法通过同步归纳以通常方式定义（见附录 B）。 $V(\cdot) = FV(\cdot) \cup BV(\cdot)$是所有变量的集合，无论这些变量是被读取还是被写入。

所有实变量 $V_{\mathbb{R}}$ 都可以在程序中读取和写入，但全局时间 $\mu$ 并不用于手动写入。[4] 相反， $\mu$ 在每种连续行为中内置的演化，使其能够表示全局时间的流。程序在记录通信时会约束轨迹变量。对于程序 $\alpha$，我们将剩余的集合（$BV(\alpha) \cap V_{\mathbb{R}}$） $\setminus \{\mu\}$ 称为 $\alpha$ 的状态，并称 $\alpha$ 在实数状态上运行。在并行组合 $\alpha \parallel \beta$中，程序$\alpha$ 和 $\beta$ 可以显式通信，但不共享状态。

$d\mathcal{L}_{\text{CHP}}$ 的逻辑语言采用迹代数，遵循 Zwiers 等人 [42,44]的方法来推理通信行为。在符号程序执行期间，通信事件会以语法形式收集到逻辑轨迹变量中，这些变量被明确指定用于记录历史。这样，程序的通信行为便可通过用作接口的记录器变量来规约。与专门的历史变量类似，此接口对于获得并行组合的组合式证明规则至关重要 [17, 38, 44]。

定义 1（项）。实数项 $\text{Trm}_{\mathbb{R}}(V,\Omega)$、整数项 $\text{Trm}_{\mathbb{N}}(V,\Omega)$、信道项 $\text{Trm}_{\Omega}(V,\Omega)$ 和迹项 $\text{Trm}_{\mathcal{T}}(V,\Omega)$ 由以下语法定义，其中 $c \in \mathbb{Q}$ 是有理常数，ch $\in \Omega$ 是信道名称， $\theta_1$、$\theta_2 \in \mathbb{Q}[V_{\mathbb{R}}]$ 是 $V_{\mathbb{R}}$ 中的多项式， $C \subseteq \Omega$ 是有限信道名称集合。所有项的集合记作 $\text{Trm}(V,\Omega)$。

$$\text{实数项}_{\mathbb{R}}(V,\Omega) : \eta_1,\eta_2 ::= x \mid c \mid \eta_1+\eta_2 \mid \eta_1 \cdot \eta_2 \mid \text{值}(te[ie]) \mid \text{时间}(te[ie])$$
$$\text{Trm}_{\mathbb{N}}(V,\Omega) : ie_1, ie_2 ::= n \mid 0 \mid 1 \mid ie_1 + ie_2 \mid |te| \text{Trm}_{\Omega}(V,\Omega) : ce_1, ce_2 ::= \text{ch} \mid \text{chan}(te[ie]) \text{Trm}_{\mathcal{T}}(V,\Omega) : te_1, te_2 ::= h \mid \epsilon \mid \langle ch, \theta_1, \theta_2 \rangle \mid te_1 \cdot te_2 \mid te \downarrow C$$

实数项 $\text{Trm}_{\mathbb{R}}(V,\Omega)$ 由算术运算符、变量 $x$ （包括 $\mu$）和有理常数 $c$ 构成。此外，val($te[ie]$) 用于访问轨迹 $te$ 中第 $ie$ 次通信的值，而 time($te[ie]$) 用于访问其时间戳。在 CHP 中，只会出现具有有理系数的多项式 $\theta \in \mathbb{Q}[V_{\mathbb{R}}] \subset \text{Trm}_{\mathbb{R}}(V,\Omega)$ $V_{\mathbb{R}}$ ，即不含迹项的多项式，因为 CHP 在实数状态上运行。按照惯例， $\theta, \theta_i$ 表示来自 $\mathbb{Q}[V_{\mathbb{R}}]$ 的项。

对于整数，我们使用 Presburger算术（不含乘法），因为它是可判定的 [37] ，且足以满足我们的需要。[5] 整数项 $|te|$ 表示轨迹 $te$的长度。类似于 val($te[ie]$)，项 chan($te[ie]$)用于访问轨迹 $te$中第 $ie$次通信的信道名称。迹项 $\epsilon$ 表示空通信， $te_1 \cdot te_2$ 表示迹项 $te_1$ 与 $te_2$的连接，而 $te \downarrow C$ 表示将 $te$ 投影到信道名称集合 $C \subseteq \Omega$上。元组 $\langle$ch $\theta_1, \theta_2\rangle$ 表示在时间 $\theta_2$通过信道 ch 传递 $\theta_1$ ，其中 $\theta_1, \theta_2 \in \mathbb{Q}[V_{\mathbb{R}}]$ ，因为通信发生在具有实数状态的程序之间。

轨迹变量 $h$ 指的是通信事件序列。通过符号执行，证明会在指定用于记录历史的轨迹变量中收集通信项

[4] 手动写入全局时间 $\mu$ 的程序很可能毫无意义，例如$\mu := 0 \parallel \mu := 1$ ，它并行地将 $\mu$ 设为 0 和 1；幸运的是，这种程序没有运行。[5] Presburger算术是 $\text{Trm}_{\mathbb{N}}(V,\Omega)$ 中不包含长度计算 $|te|$的子集。

。然后，使用投影到感兴趣的信道上，对照这些记录器变量来指定通信行为（见下方示例 1）。这使规范能够隐藏程序的内部结构，从而在存在通信 [17,38,44] 的情况下进行组合推理。

记法。我们用 val($te$) 简写 val($te[|te|-1]$)，即访问轨迹 $te$ 上最后一项的值。同样，我们使用 time($te$) 和 chan($te$)。

例1。公式 $|h\downarrow \mathsf{ch}| > 0 \to \mathsf{val}(h\downarrow \mathsf{ch}) > 0$ 表示由 $h$ 记录的沿信道 ch 发送的最后一个值为正。前置条件 $|h\downarrow \mathsf{ch}| > 0$ 确保仅当历史非空时才访问该值。

定义2（通信混合程序）。通信混合程序的集合 CHP($V,\Omega$) 由下述语法定义，其中 $x \in V_{\mathbb{R}}$ 对于 $x$、$x'$ 和 $\theta \in \mathbb{Q}[V_{\mathbb{R}}]$ 是关于 $V_{\mathbb{R}}$ 的多项式，而 $\chi \in \mathsf{FOL}_{\mathbb{R}}(V_{\mathbb{R}})$ 是一阶实数算术公式。在并行组合 $\alpha \parallel \beta$ 中，各组成部分不得共享状态，即 $V(\alpha) \cap BV(\beta) = V(\beta) \cap BV(\alpha) \subseteq \{\mu\} \cup V_{\mathcal{T}}$。

$$\alpha,\beta ::= x := \theta \mid x := * \mid \{x' = \theta \,\&\, \chi\} \mid ?\chi \mid \alpha;\beta \mid \alpha \cup \beta \mid \alpha^* \mid \quad \text{(standard } d\mathcal{L}\text{)}$$
$$ch(h)!\theta \mid ch(h)?x \mid \alpha \parallel \beta \quad \text{(CSP extension)}$$

语句 $x := \theta$ 会立即将 $x$ 更改为 $\theta$，而非确定性赋值 $x := *$ 则将 $x$ 设为任意值。对全局时间 $\mu$ 的赋值仅供公理使用。如 $d\mathcal{L}$ [30]所示，连续演化 $\{x' = \theta \,\&\, \chi\}$会按照微分方程 $x' = \theta$ 持续任意选定的时长，但前提是定义域约束 $\chi$ 始终成立。

在 $d\mathcal{L}_{\text{CHP}}$中，即使全局时间 $\mu$ 没有在语法上出现，它也总会在连续演化期间按照 $\mu' = 1$ 演化。因此，如果 $\theta \neq 1$ 不成立，则演化$\mu' = \theta$ 会被视为格式错误；正如微分方程 $x' = 1, x' = 2$ 也会被视为格式错误一样。由于程序在实数状态上运行，项 $\theta \in \mathbb{Q}[V_{\mathbb{R}}]$ 是关于 $V_{\mathbb{R}}$ 的多项式，而 $\chi \in$FOL$_{\mathbb{R}}(V_{\mathbb{R}})$ 是一阶实数算术公式。

测试 $?\chi$ 在公式 $\chi$ 满足时通过。否则，执行将中止。顺序组合 $\alpha;\beta$ 在 $\alpha$之后执行 $\beta$。选择 $\alpha \cup \beta$ 以非确定方式执行 $\alpha$或 $\beta$，而 $\alpha^*$ 则将 $\alpha$ 重复执行零次或多次。

通信和并行性的灵感来自 CSP [14]。原语 ch($h$)!$\theta$ 通过信道 ch 发送项 $\theta$ 的值，而 ch($h$)?$x$ 则从 ch 接收一个值，并将其绑定到变量 $x$。对于这两条语句，$h$ 是指定用于记录通信的轨迹变量。在正在进行的符号执行中，可以重命名该变量，以指代保存最新通信历史的变量。在系统模型中，所有记录器变量都应相同。在这种情况下，我们也写作 ch!$\theta$ 和 ch?$x$，而不写 ch($h$)!$\theta$ 和 ch($h$)?$x$。

最后，$\alpha \parallel \beta$ 以相同的持续时间并行执行 $\alpha$ 和 $\beta$，即它们的最终状态在全局时间 $\mu$的值上保持一致。如果不手动操作 $\mu$，其增量就等于连续行为的持续时间。与 CSP 一样，$\alpha$ 和 $\beta$可以执行同步消息传递，但不能共享状态。[6] 所有参与

[6] 全局时间 $\mu$ 和轨迹变量 $V_{\mathcal{T}}$ 不被视为程序状态。

通过信道进行通信的程序都必须在该信道上的所有通信方面达成一致，并在同一时间共享相同的值和记录变量，即消息传递不会消耗时间。由于共享的记录变量使所有子程序在通信方面保持一致，它们提供了能够分解并行行为的接口。如果记录器不像 $\mathsf{ch}(h_0)!\theta \parallel \mathsf{ch}(h_1)?x$ 中那样相同，则不存在运行。并行组合中对匹配记录器的要求，不得与沿程序顺序结构通过符号执行对历史进行重命名相混淆。

与 CSP 中的通常情况一样，[14], 语法并未强制采用单向通信，因此只要多个程序在记录变量和值上达成一致，就可以同时在同一信道上发送和接收。例如，$\mathsf{ch}(h)?x \parallel \mathsf{ch}(h)?y$ 是一个良构程序。其语义包含所有 $x$ 与 $y$ 接收相同值的运行。同样，若所有 $\theta_i$ 的值一致，$\mathsf{ch}(h)!\theta_1 \parallel \ldots \parallel \mathsf{ch}(h)!\theta_n$ 就有终止运行。因此，接收语句 $\mathsf{ch}(h)?x$ 可以替换为与其语义等价的 $x := *;\mathsf{ch}(h)!x$。

记法。与通常一样，$\mathsf{if}\,(\varphi)\,\{\alpha\}$ 是 $(?\varphi;\ \alpha)\ \cup ?\neg\varphi$ 的简写。

例2。图2对车队中的两辆汽车如何安全地调整速度进行了建模。不时地，leader 会将其速度 $v_l$ 调整到 0 至 $V$ 的范围内，并将这一变化通知follower 。然而，通信可能会丢失（$\mathsf{vel}!v_l \cup \mathsf{skip}$）。通过 updt 发送位置更新，至少每 $\epsilon$ 时间单位就能成功一次。收到此类更新后， follower的控制器 dist 便会唤醒。如果距离 $d$ 低于 $\epsilon V$， follower 就会减速，以便在下一次位置更新前避免碰撞。

通常情况下， follower会采用 velo中的速度更新，但关键在于，如果最近已知的距离不安全（$d > \epsilon V$），它会拒绝这样做。若 leader 能够覆盖 follower 的速度，即使当前服从指令完全没有问题，也可能导致未来发生碰撞（见下文图3）。这是因为随后关于前导车减速的通知可能会丢失。

$$
\begin{aligned}
\mathsf{velo} &\equiv \mathrm{vel}?v_{tar}; \mathsf{if}\,(d > \epsilon V)\, v_f := v_{tar} & \chi_{vel} &\equiv 0 \le v_l \le V \\
\mathsf{dist} &\equiv \mathrm{pos}?m; d := m - x_f; & \mathsf{noti} &\equiv v_l := *; ?\chi_{vel}; (\mathrm{vel}!v_l \cup \mathsf{skip}) \\
&\quad \mathsf{if}\,(d \le \epsilon V)\,\{v_f := *; ?0 \le v_f < {}^{d}\!/_{\epsilon}\} & \mathsf{updt} &\equiv \mathrm{pos}!x_l; w := 0 \\
\mathsf{plant}_f &\equiv \{x_f' = v_f\} & \mathsf{plant}_l &\equiv \{w' = 1, x_l' = v_l \,\&\, w \le \epsilon\} \\
\mathsf{follower} &\equiv \big((\mathsf{velo} \cup \mathsf{dist}); \mathsf{plant}_f\big)^* & \mathsf{leader} &\equiv \big((\mathsf{noti} \cup \mathsf{updt}); \mathsf{plant}_l\big)^*
\end{aligned}
$$

图2：两辆正在行驶的汽车（follower 和 leader）的模型，它们旨在通过并行组合形成车队 follower $\parallel$ leader ，并通信目标速度。

定义3（公式）。集合 $d\mathcal{L}_{\mathrm{CHP}}$ 公式 $\mathsf{Fml}(V, \Omega)$ 由以下语法定义，其中 $z \in V$、项 $e_1$, $e_2 \in \mathsf{Trm}(V, \Omega)$ 的类型相同，$\eta_i \in \mathsf{Trm}_{\mathbb{R}}(V, \Omega)$、 $ie_i \in \mathsf{Trm}_{\mathbb{N}}(V, \Omega)$、 $te_i \in \mathsf{Trm}_{\mathcal{T}}(V, \Omega)$, 且假设-承诺公式 A 和 C 不涉及 $\alpha$ 的状态和时间，即 $(FV(\mathsf{A}) \cup FV(\mathsf{C})) \cap BV(\alpha) \subseteq V_{\mathcal{T}}$。

$$
\begin{aligned}
\varphi, \psi, \mathsf{A}, \mathsf{C} ::= {} & e_1 = e_2 \mid \eta_1 \ge \eta_2 \mid ie_1 \ge ie_2 \mid te_1 \preceq te_2 \mid \neg\varphi \mid \varphi \wedge \psi \mid \varphi \vee \psi \mid \\
& \varphi \to \psi \mid \forall z\, \varphi \mid \exists z\, \varphi \mid [\alpha]\psi \mid [\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi
\end{aligned}
$$

为了描述 CHP 的（通信）行为，我们将一阶动态逻辑 [11] 与假设-承诺推理 [43] 结合起来。等式定义在每种类型的项上。对于实数项和整数项，$\geq$ 具有通常的含义。对于迹项，$te_1 \preceq te_2$ 表示 $te_1$ 是 $te_2$的前缀。通道项没有顺序关系。量化变量 $z \in V$ 可以是任意类型。由于我们主要关注安全性，因此省略动态模态 $\langle\alpha\rangle\psi$，并且不为 $[\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi$给出对偶算子$\langle\alpha\rangle_{\{\mathsf{A},\mathsf{C}\}}\psi$。

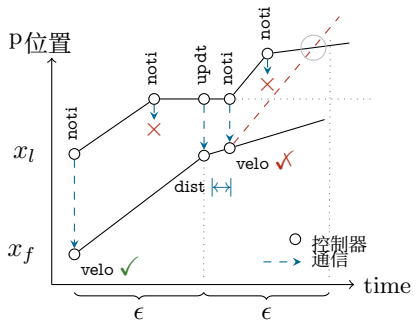


图3：示例位置 $x_f$以及 $x_l$ 随时间变化的汽车情况图。首先，速度更新被接受（✓）。下一次更新丢失（×）。位置更新后（⟷），follower调整其速度。关键在于，当与一辆减速的↙发生碰撞（↯）的可能性存在时，它会保守地拒绝速度更新（leader ），因为速度通信可能会失败（×），直到预期下一次可靠的位置更新为止，见虚线轨迹（）。

除了动态模态 $[\alpha]\psi$，$d\mathcal{L}_{\text{CHP}}$ 还突出引入了 ac-盒$[\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi$ ，将 Hoare 风格的 ac-推理 [43] 改造为动态逻辑的模态方法。在 ac-契约 $\varphi \rightarrow[\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi$中，假设 A 和承诺 C 规定了 $\alpha$沿记录变量接口的通信行为，但无法访问 $\alpha$的状态和时间；而这正是 $(FV(\mathsf{A}) \cup FV(\mathsf{C})) \cap BV(\alpha) \subseteq V_\mathcal{T}$ 所要求的。相比之下，公式 $\varphi$ 和 $\psi$ 则像往常一样充当前置条件和后置条件。

公式 $[\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi$ 承诺：假设每次通信事件发生前 A 都成立，那么$\alpha$ 的每次通信事件发生后 C 都成立。此外，如果程序已终止，并且每次通信事件发生前后 A 都成立，那么最终状态满足 $\psi$。

例 3。下面关于 follower和 leader 的安全条件表达的是：如果它们开始行驶时的距离至少为 $d$，且速度为 $\leq d/\epsilon$，足以使 follower无法在 $\epsilon$ 个时间单位内到达 leader，那么这些汽车永远不会相撞。第3节给出了该公式的证明。

$$\epsilon \geq 0 \land 0 \leq v_f \leq d/\epsilon \land v_f \leq V \land x_f + d < x_l \rightarrow [\mathsf{follower} \parallel \mathsf{leader}]\, x_f < x_l$$

通信具有内部伙伴的封闭系统，可以用方框 $[\cdot]\psi$ （见示例3）来描述，因为它们的安全性不依赖于环境。分解这类系统时，就需要用到 Ac-方框 $[\cdot]_{\{\mathsf{A},\mathsf{C}\}}\psi$，因为组成部分 follower和 leader 彼此构成对方的环境。

## 2.2 语义

通信混合程序具有指称线性历史语义，它融合了 $d\mathcal{L}$ [30]和假设-承诺推理 [44] 的思想，并加入了全局时间中的同步。基本论域是轨迹 $\mathcal{T}$和状态 $\mathcal{S}$。轨迹 $\tau \in \mathcal{T}$是通信事件 $\tau_i = \langle \mathsf{ch}_i, a_i, s_i\rangle$ 的有限序列 $(\tau_1, ..., \tau_n)$，其中信道为 $\mathsf{ch}_i \in \Omega$，值为 $a_i \in \mathbb{R}$，

时间戳为 $s_i \in \mathbb{R}$，且按时间顺序排列，即对于所有 $1 \leq i < j \leq n$，都有 $s_i \leq s_j$。空迹记为 $\epsilon$，轨迹 $\tau_1$ 与 $\tau_2$ 的连接记为 $\tau_1 \cdot \tau_2$；对于 $C \subseteq \Omega$，投影 $\tau\downarrow C$ 是 $\tau$ 的子序列，恰好由其中满足 ch $a, s\rangle$ 和 $\langle h,$ ch $a, s\rangle$ 的那些 ⟨组成，且 ch $\in C$.[7]我们用 $\tau' \preceq \tau$和 $\tau' \prec \tau$分别表示 $\tau'$是 $\tau$的前缀或真前缀。记录迹 $\tau \in \mathcal{T}_{\text{rec}}$是带有额外记录器变量 $h_i \in V_{\mathcal{T}}$的轨迹，每个通信事件都对应一个这样的变量，使得 $\tau_i = \langle h_i,$ $\mathsf{ch}_i, a_i, s_i\rangle$。原始迹 $\mathcal{T}$ 表示状态中的迹项，而记录迹则源自程序。

状态是一个映射 $v\colon V \to \mathbb{R} \cup \mathbb{N} \cup \mathcal{T}$，它为每个变量 $z \in V$ 指定一个来自 $type(z)$ 的值，其中 $type(e) = \mathbb{M}$ 当且仅当 $e \in \mathsf{Trm}_{\mathbb{M}}(V, \Omega)$，其中 $\mathbb{M} \in \{\mathbb{R}, \mathbb{N}, \mathcal{T}\}$。更新状态 $v_z^d$ 定义为在 $\{z\}^{\complement}$ 上应用 $v_z^d = v$，且 $v_z^d(z) = d$。状态轨迹的串接 $v \cdot \tau$ 会将记录的通信 $\tau \in \mathcal{T}_{\text{rec}}$ 追加到 $v \in \mathcal{S}$ 中相应的轨迹变量。它定义为在 $V_{\mathcal{T}}^{\complement}$ 上应用 $v \cdot \tau = v$，并且对所有 $h \in V_{\mathcal{T}}$，$(v \cdot \tau)(h) = v(h) \cdot \tau(h)$，其中 $\tau(h)$ 表示 $\tau$ 的子轨迹，该子轨迹由记录在 $\tau$ 中、由 $h$ 记录的通信事件 $\langle h$、ch $a, s\rangle$ 的原始版本⟨ch $a, s\rangle$ 构成。

项语义。项 $e$ 在状态 $v \in \mathcal{S}$ 下的值 $[\![e]\!]v \in type(e)$ 根据其类型 $type(e)$ 确定（见附录A）。实数项和整数项的求值按通常方式进行。此外，val($te[ie]$) 求得其值，time($te[ie]$) 求得其时间戳，而 chan($te[ie]$) 求得 $te$ 中第 $ie$ 个通信事件的信道名称，索引范围为 0 到 $|te| - 1$。此外，$|te|$ 求得 $te$ 的长度。迹项的求值与轨迹上的语义算子 $[42,44]$, 保持一致，例如 $[\![te\downarrow C]\!]v = ([\![te]\!]v)\downarrow C$ 以及 $[\![\langle$ch $\theta_1, \theta_2\rangle]\!]v = \langle$ch $[\![\theta_1]\!]v, [\![\theta_2]\!]v\rangle$。

计算域。CHP $\alpha$ 的指称语义 $[\![\alpha]\!] \subseteq \mathcal{D}$ 的定义域为 $\mathcal{D} = \mathcal{S} \times \mathcal{T}_{\text{rec}} \times \mathcal{S}_{\perp}$，其中包含 $\mathcal{S}_{\perp} = \mathcal{S} \cup \{\perp\}$，即，从某个状态启动的 CHP 的可观测量包括通信和一个最终状态。标记 $\perp$ 表示未完成执行，该执行要么可以继续，要么因失败测试而中止。由于即使在未完成的计算中也可以观测到通信，通信程序的有意义语义是前缀闭合且全的（见下文定义4）。全性表明，每个程序至少都能开始计算，即使它像 ?T 一样立即中止，并且最初没有发出通信。对于定义4，我们将轨迹上的前缀关系 $\preceq$ 从 $\mathcal{T}_{\text{rec}}$ 扩展为可观察行为 $\mathcal{T}_{\text{rec}} \times \mathcal{S}_{\perp}$ 上的偏序 $\preceq$，表示 $(\tau', w')$ 是 $(\tau, w)$ 的前缀，当且仅当 $\big((w = w'$和 $\tau = \tau')$ 或 $(w' = \perp$和 $\tau' \preceq \tau)\big)$。

定义 4（前缀闭合性与全性）。如果 $(v, \tau, w) \in U$且 $(\tau', w') \preceq (\tau, w)$ 蕴含 $(v, \tau', w') \in U$，则集合 $U \subseteq \mathcal{D}$ 是前缀闭合的。如果$\perp_{\mathcal{D}} \subseteq U$满足 $\perp_{\mathcal{D}} = \mathcal{S} \times \{\epsilon\} \times \{\perp\}$，则该集合是全的，即对于每个 $v \in \mathcal{S}$，都有 $(v, \epsilon, \perp) \in U$。

[7] 对于迹项 $te$ 和语义迹 $\tau$，我们分别使用相同的算子表示相应的语法和语义，即 $te\downarrow C$ 和 $\tau\downarrow C$ 分别是它们在 $C$ 上的投影。

程序语义。复合程序的语义通过语义算子以组合方式定义：对于 $U, M \subseteq \mathcal{D}$，我们定义 $U_\perp = \{(v,\tau,\perp) \mid (v,\tau,w) \in U\}$，并且当 $(v,\tau_1,u) \in U$、$u \neq \perp$ 且存在 $\tau = \tau_1 \cdot \tau_2$ 使得 $(u,\tau_2,w) \in M$ 时，$(v,\tau,w) \in U \triangleright M$。算子 $\hat{\circ}$ 用于顺序组合。对于 $U, M \subseteq \mathcal{D}$，我们定义 $U \hat{\circ} M = U_\perp \cup (U \triangleright M)$。语义迭代 $U^m$ 定义为 $U^0 = \mathrm{I}_{\mathcal{D}} = \perp_{\mathcal{D}} \cup (\mathcal{S} \times \{\epsilon\} \times \mathcal{S})$ 和 $U^{n+1} = U \hat{\circ} U^n$，其中 $n > 0$。相应地，$\alpha^0 \equiv ?\mathrm{T}$ 和 $\alpha^{n+1} \equiv \alpha; \alpha^n$ 定义了语法迭代。

并行组合 $\alpha \parallel \beta$ 要求 $\alpha$ 和 $\beta$ 具有互不相交的有界变量（定义 2），但 $\{\mu\} \cup V_{\mathcal{T}}$ 除外；对于 $\{\mu\} \cup V_{\mathcal{T}}$，它们始终取值一致。因此，对于状态 $w_\alpha$、$w_\beta \in \mathcal{S}_\perp$，其合并状态 $w_\alpha \oplus w_\beta \in \mathcal{S}_\perp$ 可以明确地确定如下：$w_\alpha \oplus w_\beta = \perp$ 如果至少有一个状态是 $\perp$。否则，定义 $(w_\alpha \oplus w_\beta)(z) = w_\alpha(z)$ 当且仅当 $z \in BV(\alpha)$，并定义 $(w_\alpha \oplus w_\beta)(z) = w_\beta(z)$ 当且仅当 $z \notin BV(\alpha)$。[8]对于程序 $\alpha$，集合 $CN(\alpha) \subseteq \Omega$ 由 $\alpha$中出现的所有信道名称组成，即发送语句 $\mathsf{ch}(h)!\theta$ 和接收语句 $\mathsf{ch}(h)?x$ 中的信道名称。投影 $\tau \downarrow CN(\alpha)$ 简写为 $\tau \downarrow \alpha$。对于程序 $\alpha, \beta \in \mathsf{CHP}(V, \Omega)$，语义并行算子定义如下：

$$[\![\alpha]\!] \parallel [\![\beta]\!] = \left\{ (v, \tau, w_\alpha \oplus w_\beta) \in \mathcal{D} \;\middle|\; \begin{array}{l} (v, \tau \downarrow \alpha, w_\alpha) \in [\![\alpha]\!], (v, \tau \downarrow \beta, w_\beta) \in [\![\beta]\!], \\ w_\alpha(\mu) = w_\beta(\mu), \tau = \tau \downarrow (\alpha \parallel \beta) \end{array} \right\}$$

与其计算显式交错，并行算子 $\parallel$ 通过子程序能够达成一致的任意顺序，隐式地刻画联合通信 $\tau$。因此，$\tau \in \mathcal{T}_{\mathrm{rec}}$ 排除了 $\tau \downarrow \alpha$ 或 $\tau \downarrow \beta$各自独有的通信事件以非时间顺序排列。此外，根据 $\tau = \tau \downarrow (\alpha \parallel \beta)$，轨迹 $\tau$ 不得包含任何无关通信，即并非由 $\alpha$ 或 $\beta$引起的通信。$\alpha$ 与 $\beta$ 的联合信道上的通信，其记录变量、值和时间戳必须一致，因为它们分别出现在 $\tau \downarrow \alpha$ 和 $\tau \downarrow \beta$中。根据 $w_\alpha(\mu) = w_\beta(\mu)$要求两次计算都必须在全局时间的同一点会合。[9]

定义 5（程序语义）。程序 $\alpha \in \mathsf{CHP}(V, \Omega)$ 的语义 $[\![\alpha]\!] \subseteq \mathcal{D}$ 归纳定义如下，其中 $\perp_{\mathcal{D}} = \mathcal{S} \times \{\epsilon\} \times \{\perp\}$和 $\vDash$ 是公式的满足关系（定义 6）：

$$\begin{aligned}
&[\![x := \theta]\!] = \perp_{\mathcal{D}} \cup \{(v, \epsilon, w) \mid w = v_x^{[\![\theta]\!]v}\} \\
&[\![x := *]\!] = \perp_{\mathcal{D}} \cup \{(v, \epsilon, w) \mid w = v_x^a \ \textit{where}\ a \in \mathbb{R}\} \\
&[\![?\chi]\!] = \perp_{\mathcal{D}} \cup \{(v, \epsilon, v) \mid v \vDash \chi\} \\
&[\![\{x' = \theta \,\&\, \chi\}]\!] = \perp_{\mathcal{D}} \cup \big\{(\varphi(0), \epsilon, \varphi(s)) \mid \varphi(\zeta) \vDash \mu' = 1 \wedge x' = \theta \wedge \chi \ \textit{and} \\
&\qquad \varphi(\zeta) = \varphi(0) \ \textit{on}\ \{x, \mu\}^{\complement} \ \textit{for all}\ \zeta \in [0, s] \ \textit{and a solution} \\
&\qquad \varphi : [0, s] \to \mathcal{S} \ \textit{with}\ \varphi(\zeta)(z') = \frac{d\varphi(t)(z)}{dt}(\zeta) \ \textit{for}\ z \in \{x, \mu\}\big\}
\end{aligned}$$

[8] 当 $w_\alpha = w_\beta$在 $(BV(\alpha) \cup BV(\beta))^{\complement}$上成立时，替代条件 $z \in BV(\beta)$会导出一个等价的定义；并行组合中的最终状态正是这种情况。[9] 如果 $w_\alpha = \perp$ 或 $w_\beta = \perp$，我们就认为 $w_\alpha(\mu) = w_\beta(\mu)$ 成立。

$[\![ch(h)!\theta]\!] = \{(v,\tau,w) \mid (\tau,w) \preceq (\langle h, ch, [\![\theta]\!]v, v(\mu)\rangle, v)\}$
$[\![ch(h)?x]\!] = \{(v,\tau,w) \mid (\tau,w) \preceq (\langle h, ch, a, v(\mu)\rangle, v_x^a) \ \textit{where } a \in \mathbb{R}\}$
$[\![\alpha \cup \beta]\!] = [\![\alpha]\!] \cup [\![\beta]\!]$
$[\![\alpha;\beta]\!] = [\![\alpha]\!] \mathbin{\hat{\circ}} [\![\beta]\!] = [\![\alpha]\!]_\perp \cup ([\![\alpha]\!] \triangleright [\![\beta]\!])$
$[\![\alpha^*]\!] = \bigcup_{n\in\mathbb{N}} [\![\alpha]\!]^n = \bigcup_{n\in\mathbb{N}} [\![\alpha^n]\!]$
$[\![\alpha \parallel \beta]\!] = [\![\alpha]\!] \parallel [\![\beta]\!]$

在连续演化语义中，常微分方程的解为带撇变量 $x'$ 赋予了含义，如 $d\mathcal{L}$ [33]所示。根据 $\mu' = 1$，全局时间 $\mu$在每次连续演化中始终以斜率 1 演化。

对于每个程序 $\alpha$（见附录A），语义 $[\![\alpha]\!] \subseteq \mathcal{D}$ 都是前缀闭合且全的（定义4）。对于原子非通信程序，$\perp_{\mathcal{D}} = \mathcal{S}\times\{\epsilon\}\times\{\perp\}$确保前缀闭合性。若?$\chi$ 或 $\{x' = \theta \& \chi\}$ 中止，$\perp_{\mathcal{D}}$ 还保证全性。保留未完成计算 $[\![\alpha]\!]_\perp$ 可保持 $\alpha$的前缀闭合性；$\beta$。

公式语义。一阶片段的语义与通常相同。如同动态逻辑 [11], 中一样，盒 $[\alpha]\psi$ 表示，在所有已完成的计算之后，$\psi$ 为真，即$(v,\tau,w) \in [\![\alpha]\!]$ 连同 $w \neq \perp$的最终状态和通信。ac-盒 $[\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi$ 还表示，（未）完成计算的通信满足承诺C。在我们对假设-承诺推理 [43],的模态处理中，假设A和程序 $\alpha$ 共同决定可达世界，即只需考虑其输入通信满足A的计算。

定义 6（公式语义）。公式 Fml($V,\Omega$) 的语义 $[\![\varphi]\!] \subseteq \mathcal{S}$ $\varphi \in$ 定义为 $[\![\varphi]\!] = \{v \mid v \vDash \varphi\}$，采用满足关系 $\vDash$。关系 $\vDash$ $\varphi$ 按其结构通过归纳法定义如下:

1. $v \vDash e_1{=}e_2$ 当 $[\![e_1]\!]v = [\![e_2]\!]v$时成立。因此，对于 $\eta_1{\geq}\eta_2$, $ie_1{\geq}ie_2$, $te_1{\preceq}te_2$
2. $v \vDash \varphi \wedge \psi$ 当 $v \vDash \varphi$ 且 $v \vDash \psi$时成立。因此，对于 $\neg, \vee, \rightarrow$3. $v \vDash \forall z\, \varphi$ 当对于所有 $d \in type(z)$ 都有 $v_z^d \vDash \varphi$ 时成立 4. $v \vDash \exists z\, \varphi$ 当存在某个 $d \in type(z)$ 使得 $v_z^d \vDash \varphi$ 时成立 5. $v \vDash [\alpha]\psi$ 当对于所有 $(v,\tau,w)$, $w\cdot\tau \vDash \psi$ 与 $w \neq \perp$满足 $\in [\![\alpha]\!]$ 时成立 6. $v \vDash [\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi$ 当对于所有 $(v,\tau,w)$，以下条件都成立时成立:

$$\{v\cdot\tau' \mid \tau' \prec \tau\} \vDash \mathsf{A} \ \textit{implies}\ v\cdot\tau \vDash \mathsf{C} \qquad \text{(commit)}$$
$$\big(\{v\cdot\tau' \mid \tau' \preceq \tau\} \vDash \mathsf{A} \ \textit{and}\ w \neq \perp\big) \ \textit{implies}\ w\cdot\tau \vDash \psi \qquad \text{(post)}$$

其中，$U \vDash \varphi$ 对于一个状态集合 $U \subseteq \mathcal{S}$，以及任意公式 $\varphi \in$ Fml($V,\Omega$), 若$v \vDash \varphi$ 对所有 $v \in U$均成立。特别地，$\emptyset \vDash \varphi$。

在第 6 项中，(commit) 会在每个通信事件之后进行检查，这正是我们所期望的，因为根据程序语义的前缀闭合性，所有通信前缀都是可达世界 $[\![\alpha]\!]$（定义 4）。通过第 5 项和第 6 项中的状态—迹连接 $v\cdot\tau$和 $w\cdot\tau$，记录在 $\tau$中的通信事件变得可观测。这源于这样一个认识：CHP 的可达世界由最终状态和通信轨迹组成。

注1。在 (commit) 中，只能获得关于严格发生在通信之前的通信的假设，以避免不可靠的循环推理 [17, 43]。如果采用非严格定义，公式 $y = 0 \to [\mathsf{ch}(h)!\, y]_{\{\mathsf{A},\mathsf{C}\}}\mathsf{T}$（其中 $\mathsf{A} \equiv \mathsf{C} \equiv |h\downarrow \mathsf{ch}| > 0 \to \mathsf{val}(h\downarrow \mathsf{ch}) = 1$）将变为有效。在局部范围内，我们能够意识到前置条件 $y = 0$ 与 A 所假设内容之间的矛盾，而环境无法意识到这一点，并会信任承诺 C。

命题 1（保守扩展）。逻辑 $d\mathcal{L}_{\text{CHP}}$ 是 $d\mathcal{L}$的保守扩展。也就是说，公式 $\varphi \in \mathsf{Fml}(V, \Omega) \cap \mathsf{Fml}_{d\mathcal{L}}$ 在 $d\mathcal{L}_{\text{CHP}}$ 中有效，当且仅当它在 $d\mathcal{L}$ 中有效，其中 $\mathsf{Fml}_{d\mathcal{L}}$ 是 $d\mathcal{L}$ 公式的集合（见附录A）。

## 2.3 演算

本节为 $d\mathcal{L}_{\text{CHP}}$构建了一个可靠的证明演算（见定理1），其概要见第13页的图4。第14页的图 5给出了常用的导出规则。由于 $d\mathcal{L}_{\text{CHP}}$ 是 $d\mathcal{L}$ 的保守扩展（命题 1），因此整个 $d\mathcal{L}$ 序列演算 [33, 34, 36] 都可以可靠地用于关于$d\mathcal{L}_{\text{CHP}}$公式的推理。一个带有公式 $\Gamma$、$\Delta$ 有限列表的序列 $\Gamma \vdash \Delta$ 是 $\bigwedge_{\varphi\in\Gamma}\varphi \to \bigvee_{\psi\in\Delta}\psi$的简写。

每条程序语句都由一个动态盒 $[\cdot]\psi$ 或一个 ac-盒$[\cdot]_{\{\mathsf{A},\mathsf{C}\}}\psi$公理化。公理 $[\epsilon]_{\mathsf{AC}}$ 和$[]\top, \top$ 用于在动态盒与 ac-盒之间切换，从而将二者联系起来。动态公理与微分 [33]动态逻辑 [11]中的常规公理相同。ac-公理将 Hoare 风格的 ac 推理 [43] 重新表述为动态逻辑。不过，我们为并行组合和通信设计了更原子的公理，由此可导出并行组合的证明规则 $[\|\ ]_{\mathsf{AC}}\mathrm{R}$ 以及通信的证明规则。

非干扰（定义 7）指出了公式 $[\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi \to [\alpha \,\|\, \beta]_{\{\mathsf{A},\mathsf{C}\}}\psi$ 的有效实例，我们将其作为公理 $[\mathsf{k}\ ]_{\mathsf{AC}}$ 引入，见图4。对于公式 $\chi$，访问通道 $CN(\chi) \subseteq \Omega$ 是指其通信可能影响 $\chi$ 真值的通道，例如 $|h\downarrow\mathsf{ch}| > 0$ 中的 ch。也就是说，$CN(\chi)$ 对通信轨迹 $v|_{V_\mathcal{T}}$（将状态限制在 $V_\mathcal{T}$ 上）所起的作用，与 $v \in \mathcal{S}$ 作为 $FV(\chi)$ 对整体状态 $v$ 所起的作用相似。对于程序 $\alpha$，集合 $CN(\alpha)$ 表示所使用的通信通道。

定义 7（非干扰）。给定一个 ac-盒 $[\alpha \,\|\, \beta]_{\{\mathsf{A},\mathsf{C}\}}\psi$ 若 CHP $\beta$ 满足以下条件，则它不会干扰其周围的契约：[10]

$$FV(\psi) \cap BV(\beta) \subseteq \{\mu\} \cup V_\mathcal{T} \tag{1}$$
$$FV(\chi) \cap BV(\beta) \subseteq V_\mathcal{T} \quad (\text{for } \chi \in \{\mathsf{A}, \mathsf{C}\}) \tag{2}$$
$$CN(\chi) \cap CN(\beta) \subseteq CN(\alpha) \quad (\text{for } \chi \in \{\mathsf{A}, \mathsf{C}, \psi\}) \tag{3}$$

[10] 该定义只限制了 $\beta$ 对公式 A、C 的影响，$\psi$ 但不限制其对程序 $\alpha$ 的影响，因为在并行组合 $\alpha \,\|\, \beta$ 中，子程序本来就不能共享状态。

显然，由 $\beta$绑定且在 $\chi \in$ {A、C $\psi$} 中自由出现的状态变量会影响 $\chi$在 $[\alpha \parallel \beta]_{\{A,C\}}\psi$中的真值。然而，方程 (1) 和方程 (2) 无法捕获轨迹变量 $V_{\mathcal{T}}$，因为它们同时也是 $\alpha$的接口，其通信可能与 $\beta$进行联合通信。不过，方程 (3) 将对 $\chi$ 中轨迹变量的访问限制为这样的信道：其通信要么只能从 $\alpha$ 中观察到，要么是 $\alpha$ 与 $\beta$之间的联合通信，因此防止了 $\beta$对 $\chi$ 产生超出 $\alpha$已造成影响的影响。然而，定义 7 仍允许完全访问 $\alpha$的通信，包括与 $\beta$的联合通信。

动态假设-承诺推理。在 Hoare 风格的假设-承诺推理中，[43], 一个专门的历史变量全局记录通信。假设 $h$ 是 $d\mathcal{L}_{\text{CHP}}$ 中的此类变量，则发送语句的一种看似合理但错误的公理化方式是

$$[\text{ch}!\theta]\psi(h) \leftrightarrow \forall h_0 \left(h_0 = h \cdot \langle \text{ch}, \theta, \mu\rangle \rightarrow \psi(h_0)\right). \qquad (\lightning)$$

将其应用于

$$\vdash [\text{ch}_1!\theta_1][\text{ch}_2!\theta_2]\psi(h) \qquad (4)$$

得到 $h_0 = h \cdot \langle \text{ch}_1, \theta_1, \mu\rangle \vdash [\text{ch}_2!\theta_2]\psi(h_0)$。完成这一步后，当前历史为 $h_0$。然而，再次应用会得到 $h_0 = h \cdot \langle \text{ch}_1, \theta_1, \mu\rangle, h_1 = h \cdot \langle \text{ch}_2, \theta_2, \mu\rangle \vdash \psi(h_0)$。错误的是，通信又被追加到 $h$，而且$\psi(h_0)$仍然指向 $h_0$。问题在于，第一次应用期间的替换（$[\text{ch}_2!\theta_2]\psi(h)$）$\{h \mapsto h_0\}$并不能指引 $\text{ch}_2!\theta_2$ 将其通信追加到 $h_0$。如果 $h$ 没有在语法上出现，却在 $\text{ch}_2!\theta_2$ 中自由出现，那么该替换甚至没有明确的定义。出于类似原因，公理

$$[\text{ch}!\theta]\psi(h) \leftrightarrow \psi(h \cdot \langle \text{ch}, \theta, \mu\rangle) \qquad (\lightning)$$

由于对方程 (4) 应用两次会得到 $\vdash \psi(h \cdot \langle \text{ch}_2, \theta_2, \mu\rangle \langle \text{ch}_1, \theta_1, \mu\rangle)$，其中通信项的顺序错误，因此它不可靠。这里，该公理无法将第二个通信项追加到正确的位置，因为第一次应用后，历史 $h \cdot \langle \text{ch}_1, \theta_1, \mu\rangle$ 的状态没有符号名称。

为了支持符号执行，我们放弃存在一个专用历史变量的假设，并为每个通信语句 $\text{ch}(h)!\theta$ 和 $\text{ch}(h)?x$标注一个显式的记录器变量 $h$。现在，替换 $\alpha\{h \mapsto h_0\}$ 很容易定义：对于 $\alpha \equiv \text{ch}(h)!\theta$，定义为 $\text{ch}(h_0)!\theta$；对于 $\alpha \equiv \text{ch}(h)?x$，定义为 $\text{ch}(h_0)?x$；对于其他原子程序，定义为 $\alpha$；其他情况则通过递归应用来定义。

原子混合程序。对于一个（原子）非通信程序 $\alpha$，我们可以通过公理 $[\epsilon]_{\text{AC}}$ 将 $[\alpha]_{\{A,C\}}\psi$ 展平为动态公式，因为当 $CN(\alpha) = \emptyset$时，A 和 C 只涉及初始状态。随后，我们可以通过该程序的动态公理执行程序（[:=], [:∗], [?], [′]）。注意，根据保守扩展（命题 1），只有当常微分方程$x' = \theta$ 符合底层语义时，公理 $[']$ 才适用于 $[\{x' = \theta \,\&\, \chi\}]\psi$；也就是说，只有在 $\mu \in x$时才适用。对于良构的连续演化 $x' = \theta$，其右端为 1。因此，公理 $[\mu]$ 允许在必要时将全局时间流 $\mu$ 具体化为演化 $\mu' = 1$。

$[:=]$ $[x := \theta]\psi(x) \leftrightarrow \psi(\theta)$ $[;]_{AC}$ $[\alpha;\beta]_{\{A,C\}}\psi \leftrightarrow [\alpha]_{\{A,C\}}[\beta]_{\{A,C\}}\psi$ $[:*]$ $[x := *]\psi \leftrightarrow \forall x\,\psi$ $[\cup]_{AC}$ $[\alpha \cup \beta]_{\{A,C\}}\psi \leftrightarrow [\alpha]_{\{A,C\}}\psi \wedge [\beta]_{\{A,C\}}\psi$ $[?]$ $[?\chi]\psi \leftrightarrow (\chi \to \psi)$ $[^*]_{AC}$ $[\alpha^*]_{\{A,C\}}\psi \leftrightarrow [\alpha^0]_{\{A,C\}}\psi \wedge [\alpha]_{\{A,C\}}[\alpha^*]_{\{A,C\}}\psi$ [a] $[]_{\top}$,$_{\top}$ $[\alpha]\psi \leftrightarrow [\alpha]_{\{T,T\}}\psi$ I$_{AC}$ $[\alpha^*]_{\{A,C\}}\psi \leftrightarrow [\alpha^0]_{\{A,C\}}\psi \wedge [\alpha^*]_{\{A,T\}}(\psi \to [\alpha]_{\{A,C\}}\psi)$ [a] $[\mu]$ $[\{x' = \theta\ \&\ \chi\}]\psi \leftrightarrow [\{\mu' = 1, x' = \theta\ \&\ \chi\}]\psi$ $[']$ $[x' = \theta(x)]\psi(x) \leftrightarrow \forall t{\geq}0\,[x := y(t)]\psi(x)$ $(y'(t) = \theta(y)$ 和 $\mu \in x)$ [b] $[ch!]$ $[ch(h)!\theta]\psi(h) \leftrightarrow \forall h_0\,(h_0 = h \cdot \langle ch\ \theta, \mu\rangle \to \psi(h_0))$ $(h_0$ fresh) $[ch!]_{AC}$ $[ch(h)!\theta]_{\{A,C\}}\psi \leftrightarrow C \wedge \big(A \to [ch(h)!\theta](C \wedge (A \to \psi))\big)$ $[ch?]_{AC}$ $[ch(h)?x]_{\{A,C\}}\psi \leftrightarrow [x := *][ch(h)!x]_{\{A,C\}}\psi$ $[]_K$ $(Cl_\forall K) \wedge [\alpha]_{\{A_1\wedge A2, C_1\wedge C_2\}}\psi \to [\alpha]_{\{A,C_1\wedge C_2\}}\psi$ [c] [d] $[k]_{AC}$ $[\alpha]_{\{A,C\}}\psi \to [\alpha \parallel \beta]_{\{A,C\}}\psi$ ($\beta$ 不会干扰 $[\alpha]_{\{A,C\}}\psi$ （定义 7））

$[\epsilon]_{AC}$ $[\alpha]_{\{A,C\}}\psi \leftrightarrow C \wedge (A \to [\alpha]\psi)$ $(CN(\alpha) = \emptyset)$ [d]

$M[\cdot]_{AC}$ $\dfrac{A_2 \to A_1 \quad C_1 \to C_2 \quad \psi_1 \to \psi_2}{[\alpha]_{\{A_1,C_1\}}\psi_1 \to [\alpha]_{\{A_2,C_2\}}\psi_2}$

$W[]_{AC}$ $[\alpha]_{\{A,C\}}\psi \leftrightarrow C \wedge [\alpha]_{\{A,C\}}(C \wedge (A \to \psi))$

$[]_{AC}\wedge$ $[\alpha]_{\{A,C_1\wedge C_2\}}(\psi_1 \wedge \psi_2) \leftrightarrow \bigwedge_{j=1}^{2}[\alpha]_{\{A,C_j\}}\psi_j$

$G_{AC}$ $\dfrac{C \wedge \psi}{[\alpha]_{\{A,C\}}\psi}$

[a] 注意，$[\alpha^0]_{\{A,C\}}\psi \leftrightarrow C \wedge (A \to \psi)$ 可由 $[\epsilon]_{AC}$ 和 $[?]$ 推出，因为 $\alpha^0 \equiv ?T$. [b] 保守扩展仅在 $\mu' = 1$ 属于 $x' = \theta$ 时适用；当 $\mu \in x$ 时该条件成立，因为在演化中，除 1 以外，$\mu$ 的每个右侧都被视为非良构。[c] K 是组合性条件 $(A \wedge C_1 \to A_2) \wedge (A \wedge C_2 \to A_1)$。$_\forall\varphi$ 的全称闭包 Cl $\varphi$ 定义为 $\forall z_1$、.....、$z_n\,\varphi$，其中 $FV(\varphi) = \{z_1, \ldots, z_n\}$。[d] 例如，当从右向左应用 $[\epsilon]_{AC}$ 时，必须注意所得的 ac-方框是良构的，即 $(FV(A) \cup FV(C)) \cap BV(\alpha) \subseteq V_T$ 对于 $[\alpha]_{\{A,C\}}\psi$。

图4： $d\mathcal{L}_{\mathrm{CHP}}$ 证明演算

复合混合程序。ac-盒中的复合 CHP 若进行通信，则无法通过公理 $[\epsilon]_{AC}$ 处理。相反，它们适用公理 $[;]_{AC}$、$[\cup]_{AC}$、$[^*]_{AC}$ 和 I$_{AC}$。动态盒中的复合程序可以利用公理 $[]_\top$、$_\top$ 重新封装到 ac-盒中。交流归纳公理 I$_{AC}$ 谨慎地将动态逻辑 [11]中的归纳法推广了出来。重要的是，归纳步骤需要成立的可达世界只取决于程序 $\alpha$ 以及关于输入通信的假设 A，而承诺 C 则通过归纳法证明。在图5中，我们给出了有用的派生循环不变式证明规则 ind$_{AC}$。与通常一样，它源自公理 I$_{AC}$ 和 G$_{AC}$ 版 G¨odel- 一般化规则的交流版本，这证实了嵌入动态逻辑的正确性。

如果我们在 $\alpha$；$\beta$的语义中忽略中止运行的通信，公理 $[;]_{AC}$ 就不可靠。要证明 $[\alpha]_{\{A,C\}}[\beta]_{\{A,C\}}\psi$，需要证明在每次C 通信之后，$\alpha$ 的承诺 $\beta$ 仍然成立，即使 $[\alpha;\ \beta]_{\{A,C\}}\psi$ 中止。要从 $[\![\alpha;\ \beta]\!] = [\![\alpha]\!]_\perp \cup ([\![\alpha]\!] \triangleright [\![\beta]\!]$的语义中得到这一点，该语义包含 $\alpha$ 的所有相应运行，直至 $\beta$，且 $[\![\alpha]\!]_\perp$。

$$\text{CG}\ \frac{\Gamma, h_0 = h \cdot \langle \mathrm{ch}, \theta, \mu\rangle \vdash [\alpha(h_0)]\psi, \Delta}{\Gamma, \vdash [\alpha(h)]\psi, \Delta}\quad (h \notin FV(\psi) \text{ and } h_0 \text{ fresh})$$

$$\text{ind}_{\text{AC}}\ \frac{\Gamma \vdash \mathsf{C} \wedge \mathsf{I}, \Delta \quad \mathsf{C}, \mathsf{I} \vdash [\alpha]_{\{\mathsf{A},\mathsf{C}\}}\mathsf{I} \quad \mathsf{A}, \mathsf{C}, \mathsf{I} \vdash \psi}{\Gamma \vdash [\alpha^*]_{\{\mathsf{A},\mathsf{C}\}}\psi, \Delta} \qquad [\text{if}]\ \frac{\Gamma, \varphi \vdash [\alpha]\psi, \Delta \quad \Gamma, \neg\varphi \vdash \psi, \Delta}{\Gamma \vdash [\text{if}\,(\varphi)\,\{\alpha\}]\psi, \Delta}$$

$$[\|\_]_{\text{AC}}\mathrm{R}\ \frac{\vdash \mathsf{K} \quad \Gamma \vdash [\alpha_j]_{\{\mathsf{A}_j,\mathsf{C}_j\}}\psi_j, \Delta \quad (j = 1,2)}{\Gamma \vdash [\alpha_1 \,\|\, \alpha_2]_{\{\mathsf{A},\mathsf{C}_1\wedge\mathsf{C}_2\}}(\mathsf{C}_1 \wedge \mathsf{C}_2), \Delta}\quad (\alpha_{3-j} \text{ does not interfere with } [\alpha_j]_{\{\mathsf{A}_j,\mathsf{C}_j\}}\psi_j \text{ for } j = 1,2 \text{ (Def. 7)})^a$$

$$[!\boldsymbol{\theta}]_{\text{AC}}\mathrm{R}\ \frac{\Gamma \vdash \mathsf{C}(h), \Delta \quad \Gamma, H_0 \vdash \mathsf{C}(h_0), \Delta \quad \Gamma, H_0, \mathsf{A}(h_0) \vdash \psi(h_0), \Delta}{\Gamma \vdash [\mathrm{ch}(h)!\theta]_{\{\mathsf{A}(h),\mathsf{C}(h)\}}\psi(h), \Delta}\quad (h_0 \text{ fresh})^b$$

[a] $\mathsf{K}$ is the compositionality condition $(\mathsf{A} \wedge \mathsf{C}_1 \to \mathsf{A}_2) \wedge (\mathsf{A} \wedge \mathsf{C}_2 \to \mathsf{A}_1)$.
[b] Formula $H_0$ is short for $h_0 = h, \cdot \langle \mathrm{ch}\ \theta\ \mu\rangle$ recording the global time $\mu$ as timestamp.

图 5：派生的 $d\mathcal{L}_{\text{CHP}}$ 证明规则

通信语句。公理 $[\mathrm{ch}!]_{\text{AC}}$ 将单个发送语句的 ac-盒展开（提交）为动态盒。执行发送 $\mathrm{ch}(h)!\theta$ 对记录变量 $h$ 的影响由公理 $[\mathrm{ch}!]$刻画。它将事件 $\langle \mathrm{ch}\ \theta, \mu\rangle$ 记录下来，以当前全局时间 $\mu$ 作为时间戳，并在后置条件中重命名历史，以供后续证明步骤使用。公理$[\mathrm{ch}?]_{\text{AC}}$ 利用接收语句与发送语句的对偶性来执行接收语句。导出规则 $[!\boldsymbol{\theta}]_{\text{AC}}\mathrm{R}$结合 $[\epsilon]_{\text{AC}}$ 和 $[\mathrm{ch}!]$, ，并将该语句分解为两个关于（提交）的前提和一个关于（后置条件）的前提。规则 CG 很有用，因为它通过在历史前添加额外的幽灵通信，免去了对空历史进行分类讨论的需要。

并行组合。非干扰程序 $\beta$ （定义 7）可以依据公理 $[\alpha \,\|\, \beta]_{\{\mathsf{A},\mathsf{C}\}}\psi \leftrightarrow [\alpha]_{\text{AC}}$ 从并行组合中删除，因为它不会影响周围的契约 $[\alpha \,\|\, \_]_{\{\mathsf{A},\mathsf{C}\}}\psi$。由于 $\|$ 具有结合性和交换性（参见附录 C），公理 $[\|]_{\text{AC}}$ 可以删除并行语句链中的任意子程序。在 $[\alpha_j]_{\{\mathsf{A}_j,\mathsf{C}_j\}}\psi_j$ 的并行组合中，对于 $\overline{j} = 1$、2，承诺会相互贡献于假设。这可以依据公理 $[]_{\mathsf{K}}$ 将 $\alpha_1 \,\|\, \alpha_2$ 关于其环境的假设弱化为 $\mathsf{A}$，前提是组合性条件 $\mathsf{K} \equiv (\mathsf{A} \wedge \mathsf{C}_1 \to \mathsf{A}_2) \wedge (\mathsf{A} \wedge \mathsf{C}_2 \to \mathsf{A}_1)$ 有效。

导出规则 $[\mathrm{k}]_{\text{AC}}\mathrm{R}$ 将公理 $[\mathrm{k}]_{\text{AC}}$ 和 $[]_{\mathsf{K}}$ 结合起来，以完整分解并行性。要对任意 $\mathsf{A}$、$\mathsf{C}$ 和 $\psi$ 的并行 $[\alpha_1 \,\|\, \alpha_2]_{\{\mathsf{A},\mathsf{C}\}}\psi$ 进行推理，任务是为 $j = 1,2$ 构造 $\mathsf{A}_j$、$\mathsf{C}_j$ 和 $\psi_j$，使得 $\mathsf{C}_1 \wedge \mathsf{C}_2 \to \mathsf{C}$ 和 $\psi_1 \wedge \psi_2 \to \psi$ 有效，并且 $[\mathrm{k}]_{\text{AC}}\mathrm{R}$ 可适用。由于 $[\mathrm{k}]_{\text{AC}}\mathrm{R}$ 关于非干扰的侧条件仍允许 $\mathsf{C}_j$ 和 $\psi_j$ 为 $j = 1,2$ 访问 $\overline{\alpha_j}$ 的通信（包括与 $\alpha_{3-j}$ 的联合通信），因此这些公式可以涵盖 $\alpha_1 \,\|\, \alpha_2$ 的完整通信。

其他。根据公理 $[]_{\text{AC}}\wedge$，Ac-方框可对合取进行分配；但与前置条件类似，假设 $\varphi_j$ 不会在 $\varphi_1 \wedge \varphi_2 \to [\alpha]\psi$ 中进行分配。

规则 $\mathrm{M}[\cdot]_{\mathsf{AC}}$ 将单调性从动态方框推广到 ac-方框。ac-弱化$\mathrm{W}[]_{\mathsf{AC}}$ 利用程序语义的全性 $[\![\alpha]\!]$，在初始状态中添加或删除 C 。此外，通过 $\mathrm{W}[]_{\mathsf{AC}}$，在最终状态中添加或删除 C 和 A $\rightarrow \psi$，分别归因于（提交）和（后置条件）。规则 $\mathrm{G}_{\mathsf{AC}}$ 是 G¨odel-广义规则的交流版本。

不含长度计算 $|te|$ 的 $\mathrm{Trm}_{\mathbb{N}}(V,\Omega)$ 上的一阶公式 $\mathrm{FOL}_{\mathbb{N}}(V_{\mathbb{N}})$，可以通过有效的预言机证明规则（称为 $\mathbb{N}$）处理，因为 Presburger 算术是可判定的 [37]。同样，一阶实数算术 $\mathrm{FOL}_{\mathbb{R}}(V_{\mathbb{R}})$ 是可判定的 [40]，，我们也像 $d\mathcal{L}$ [30] 中那样为其使用预言机规则（称为 $\mathbb{R}$）。然而，$d\mathcal{L}_{\mathrm{CHP}}$ 的完整一阶片段 $\mathrm{FOL}(V,\Omega)$ 是不可判定的，因为存在迹变量和整数变量的交替量词 [5]。

相反，关于迹项的推理依靠简单的代数定律进行连续化简（见附录 C） [42]。为了应用规则 $\mathbb{R}$ 和 $\mathbb{N}$，迹子项可以用新变量重写。例如，$\mathrm{val}(te_1[ie])$ <$\mathrm{val}(te_2[ie]) \rightarrow \mathrm{val}(te_1[ie])+\theta < \mathrm{val}(te_2[ie])+\theta$ 是有效的，因为 $x<y \rightarrow x+\theta < y+\theta$ 在 $\mathrm{FOL}_{\mathbb{R}}(V_{\mathbb{R}})$ 中有效。最终，我们在迹项模下使用 $\mathbb{N}$ 和 $\mathbb{R}$，即不显式地执行重写。

我们的核心贡献是关于组合式$d\mathcal{L}_{\mathrm{CHP}}$ 证明演算的可靠性定理。图 5 中给出的证明规则可推导出（见附录 C）。

定理 1。 $d\mathcal{L}_{\mathrm{CHP}}$ 演算（见图4）是可靠的（见附录 C）。

## 3 dLCHP 的演示

我们通过概述一个证明来演示我们的演算，该证明针对的是第 7 页示例 3 中关于第 6 页图 2 所示车队的安全条件。将并行语句分解后，证明便可通过逐条语句进行符号执行，以纯机械的方式推进。证明从图 7 开始，采用一种标准模式来分解并行语句：首先，通过公理 $[]\top$, $\top$ 和规则 $\mathrm{M}[\cdot]_{\mathsf{AC}}$，引入承诺和后置条件（见图6），以关联各子程序；其次，规则 $[\![\ \|\ ]\!]_{\mathsf{AC}}\mathrm{R}$ 因此变得适用。后者还使这些承诺成为相互假设。–

图 6 中联系各子程序的公式清晰地将其复杂的内部结构化简，并且只依赖于简洁的通信接口和局部变量，因此无需了解另一辆车的内部结构。添加初始幽灵通信（规则 CG）利用显式历史变量和动态逻辑的灵活性，避免了针对空历史进行繁琐的分类讨论。

图 7 将 $x_f < x_l$ 分解为 $\psi_f$ 和 $\psi_l$，因为 follower 始终位于 leader 的最后已知位置 $\mathrm{val}(h_{\mathrm{pos}})$ 之后，而 leader 根据 $\psi_l$ 从不向后行驶。事实上，follower 在 $d$ 中存储了最后已知的距离 $\mathrm{val}(h_{\mathrm{pos}}) - x_f$，而 $\epsilon - \Delta(\mu, h_{\mathrm{pos}})$ 则界定了沿 pos 信道进行下一次位置更新前的等待时间。因此，以速度 $d/\epsilon$ 行驶时，follower 始终位于 leader 之后。

图 8 接续图 7，展示了沿着 follower的一条执行路径进行推理的过程。用于归纳法 $\mathrm{ind}_{\mathsf{AC}}$ 的不变式 F 对 follower 的

$$\varphi \equiv \epsilon \geq 0 \land 0 \leq v_f \leq {}^{d}/_{\epsilon} \land v_f \leq V \land x_f + d < x_l \qquad \text{（前置条件：车队）}$$
$$\psi_f \equiv 0 \leq {}^{d}/_{\epsilon} \land x_f + (\epsilon - \Delta(\mu, h\downarrow \text{pos}))^{d}/_{\epsilon} < \text{值}(h\downarrow \text{pos}) \qquad \text{（后置条件 follower）}$$
$$\psi_l \equiv \text{值}(h\downarrow \text{位置}) \leq x_l \land \Delta(\mu, h\downarrow \text{位置}) \leq \epsilon \qquad \text{（后置条件 leader）}$$
$$\mathsf{A} \equiv \mathsf{C} \equiv 0 \leq \text{值}(h\downarrow \text{速度}) \leq V \qquad \text{(ac-公式)}$$

图 6：对于通道 $\in \{$速度、位置$\}$，项 $\Delta(\mu, h\downarrow$通道$)$ 是 $\mu -$时间$(h\downarrow$通道$)$ 的简写，即沿通道自上次通信以来经过的时间，由 $h$记录。 leader给出的承诺 C、 follower作出的假设 A，以及后置条件 $\psi_f$ 和 $\psi_l$ 用于图 7 中的证明。

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{\vdash \mathsf{C} \to \mathsf{A}} \quad \dfrac{\triangleright \text{ Fig. 8}}{\Gamma \vdash [\text{follower}(h)]_{\{\mathsf{A},\mathsf{T}\}}\psi_f} \quad \dfrac{\triangleright \text{ Fig. 21}}{\Gamma \vdash [\text{leader}(h)]_{\{\mathsf{T},\mathsf{C}\}}\psi_l}}{\Gamma \vdash [\text{follower}(h) \parallel \text{leader}(h)]_{\{\mathsf{T},\mathsf{C}\}}(\psi_f \land \psi_l)}\,[\|\_\|_{\mathsf{AC}}\mathrm{R}}{\Gamma \vdash [\text{follower}(h) \parallel \text{leader}(h)]_{\{\mathsf{T},\mathsf{C}\}}x_f < x_l}\,\mathrm{M}[\cdot]_{\mathsf{AC}}}{\Gamma \vdash [\text{follower}(h) \parallel \text{leader}(h)]_{\{\mathsf{T},\mathsf{T}\}}x_f < x_l}\,\mathrm{M}[\cdot]_{\mathsf{AC}}}{\Gamma \vdash [\text{follower}(h) \parallel \text{leader}(h)]x_f < x_l}\,[]_{\top,\top}}{\varphi \vdash [\text{follower}(h_0) \parallel \text{leader}(h_0)]x_f < x_l}\,2{\times}\mathrm{CG}}{\vdash \varphi \to [\text{follower}(h_0) \parallel \text{leader}(h_0)]x_f < x_l}\,{\to}\mathrm{R}$$

$\triangleleft_1$ $\top$R　$\triangleleft_2$ $\mathbb{R}$

图 7：示例 2 中车队的安全性证明，其中 $\Gamma$是公式列表$\varphi$， $h_1 = h_0 \cdot \langle$速度$0$， $\mu\rangle$， $h = h_1 \cdot \langle$位置 $x_l$， $\mu\rangle$。开放前提 $\mathsf{C} \vdash \mathsf{T}$ $(\triangleleft_1)$ 和$\psi_f \land \psi_l \vdash x_f < x_l$ $(\triangleleft_2)$ 分别通过规则 $\top$R 和 $\mathbb{R}$闭合。

速度进行界定，使其在下一次位置更新之前始终落后于 leader 。TA 表示轨迹代数推理。其余证明是机械的符号执行。具体而言，组合 $[\epsilon]_{\mathsf{AC}}$ 和 W$[]_{\mathsf{AC}}$ 会吸收合取范式公式{A,T} ，而使用对偶公理 $[\text{ch?}]_{\mathsf{AC}}$ 可以通过规则 $[!\theta]_{\mathsf{AC}}$R 执行通信。公理 $[\mu]$ 将全局时间 $\mu$ 的流具体化，从而使解公理 $[']$ 适用。弱化 WL 会去除无关前提， $\forall$R 为量化变量引入新鲜变量，而 $=$L 和 $=$R 分别在左侧和右侧执行替换。轨迹代数 TA 对假设 A 求值。最后，证明通过模去迹项的实数算术得出。

## 4 相关工作

与 CHP 不同，混合 CSP（HCSP） [18] 在 CSP [14] 的基础上加入了急切连续演化，并在违反演化约束时终止。这种降低了的不确定性几乎不给并行程序留下就持续时间达成一致的余地，因此很容易导致空行为和空洞证明。CHP 中的非急切演化涵盖了急切运行。不同于 $d\mathcal{L}_{\text{CHP}}$ 中利用其组合模型的做法，其他混合进程代数通过转换为模型检测 [6, 24, 39]，以非组合方式进行验证。与 CHP 不同，CHP 已证明无需额外改造即可对通信丢失进行建模和推理，而元级

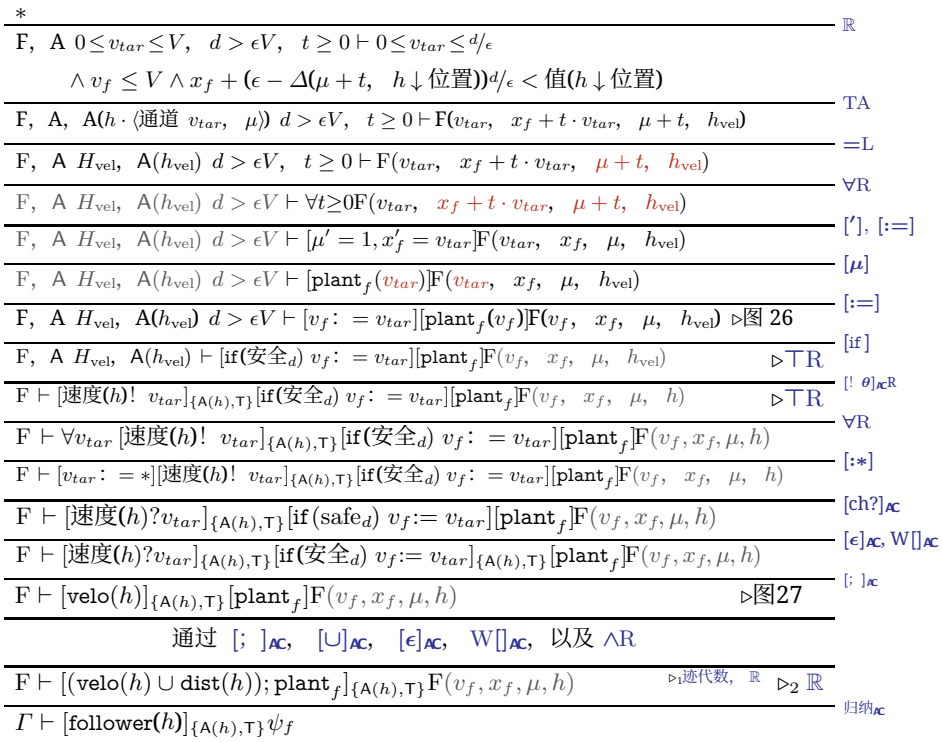


图 8: follower的部分证明。归纳法 indAC使用 F $\equiv 0 \le v_f \le d/\epsilon \wedge v_f \le V \wedge x_f + (\epsilon - \Delta(\mu, h\downarrow\text{pos}))d/\epsilon < \text{val}(h\downarrow\text{pos})$ 作为不变式。公式 $H_{\text{vel}}$ 是 $h_{\text{vel}} = h \cdot \langle \text{vel}\ v_{tar}、\ \mu\rangle$ 的简写，而 $\text{safe}_d$ 是 $d > \epsilon V$ 的简写。归纳基 $\Gamma \vdash$ F $(\triangleright_1)$ 通过轨迹代数 TA 和实数算术 ℝ 得以闭合。后置条件 F $\vdash \psi_f$ $(\triangleright_2)$ 由 ℝ成立。为清晰起见，我们突出显示代换。

组件 [4,7,13,19,22,23,26] 则需要重新设计，才能像应对其他每一种新应用那样，集成有损通信。

HCSP 的混合霍尔逻辑（HHL） [21] 不具组合性 [41]。Wang等人[41] 以假设-保证推理（AGR）扩展了它，但与$d\mathcal{L}_{\text{CHP}}$不同，这种扩展再次变得不具组合性。遗憾的是，他们针对并行组合的规则仍然会在后置条件中显式展开通信轨迹的所有交错，从而反映子程序的结构。HHL 中的假设和保证无法描述通信历史，而是考虑就绪性，并将无死锁性推理留待未来工作 [41]。以这种方式外置完整的可观察行为（以及程序结构），会使组合性的整体意义荡然无存 [38, 第 1.6 节。2]，却只是推迟了对指数级多个交错的推理。同样，Guelev等人将并行组合的语义编码进后置条件中 [10]。

Hoare 风格的假设-承诺推理 [16,43,44] （包括针对 HCSP 的霍尔风格推理） [10,21,41] 缺少作为直观推理原则的符号执行，但通过

引入一个特殊的历史变量来处理，因为无法同时考虑多个 Hoare 三元组。 $d\mathcal{L}_{\text{CHP}}$ 通过显式轨迹变量（它们在证明中指向历史的不同可能状态），使符号执行成为可能，尽管存在通信。由此形成的假设-承诺推理与动态逻辑的结合，可以灵活地在一阶推理、动态逻辑和假设-承诺推理之间切换，同时公理也很简单，能够刻画离散行为、连续行为或通信行为。与 $d\mathcal{L}_{\text{CHP}}$不同，后者因连续演化而具有全局时间流，分布式实时计算的演算 [16, 17] 还需要考虑等待耗时离散语句终止的情况。

不同于其他 $d\mathcal{L}$ 方法 [19, 22, 26]， $d\mathcal{L}_{\text{CHP}}$ 在混合程序中将内置时间同步的并行算子作为一等公民，该算子可与其他程序任意嵌套，而非对具有显式时间模型的元级组件进行并行组合。通过非确定性选择建模并行性，还需要格外谨慎，以确保执行周期性 [22]。与最多只关联相邻输入/输出事件的一阶约束 [19, 22, 26]不同， $d\mathcal{L}_{\text{CHP}}$ 能够推理整个通信历史的不变式。不同于我们对离散行为、混合行为和通信行为进行的集成推理，Kamburjan 等人 [19] 将通信推理与混合系统推理分开处理。

量化微分动态逻辑 Q$d\mathcal{L}$ [32] 允许对无界数量的分布式 CPS 的并行组合进行推理。不同于能够推理完全不同程序之间交互的 $d\mathcal{L}_{\text{CHP}}$，Q$d\mathcal{L}$ 中的并行性仅限于具有同质结构的子程序。

与 CHP 的指称语义不同，混合自动机的并行组合 [4,8,13,23], 就像对 HCSP 进行霍尔风格推理一样 [10,41],总是退回到对并行性的组合式探索。因此，即使是针对混合自动机的假设-保证推理方法 [4, 8, 12, 23] 能够缓解子自动机的状态空间爆炸问题，最终也会转而使用大型积自动机。相比之下， $d\mathcal{L}_{\text{CHP}}$的并行组合证明规则利用了其语义内在的组合性，使子程序的验证真正独立于其环境，通信接口除外。与 $d\mathcal{L}_{\text{CHP}}$ 中能够描述任意通信信道配对的变化、速率、延迟或噪声的 ac 公式不同，基于定时迁移系统的过近似仅限于粗粒度抽象 [8], ，其组件完全舍弃了对连续行为的认知 [13], ，或采用静态全局契约 [4]。$d\mathcal{L}_{\text{CHP}}$ 从$d\mathcal{L}$继承了对微分方程不变式的完整推理能力，而自动机方法通常仅适用于线性连续动态系统 [8,13]。

并发动态逻辑（CDL）没有提供并行程序相互作用的方式 [29]。带通信的 CDL [28] 具有 CSP 风格的 [14] 通信原语，但缺少连续行为和用于验证的证明演算。

## 5 结论

本文提出了一种用于通信混合程序（CHP）的动态逻辑 $d\mathcal{L}_{\text{CHP}}$，支持全局时间下的同步并行组合。该 $d\mathcal{L}_{\text{CHP}}$ 证明

演算是首个真正面向通信并行混合系统的组合式验证方法。为此， $d\mathcal{L}_{\text{CHP}}$ 利用动态逻辑的灵活性，在必要模态和可能模态的基础上补充了假设-承诺（ac）模态。至关重要的是，这种对假设-承诺推理的嵌入支持以一种可控复杂度的方式，对并行混合行为进行组合式规约与验证。由于支持在存在通信的情况下通过直观的符号执行进行推理， $d\mathcal{L}_{\text{CHP}}$ 的实际可行性得以提升。语义构造中的所有技术细节都隐藏在底层，使得实际的演算能够自然地推广动态逻辑推理。

未来的工作包括开发一种一致替换演算 [33] ，以便$d\mathcal{L}_{\text{CHP}}$ 实现精简的定理证明器实现 [9]。

资助声明。本项目部分由德国研究联合会（DFG）——378803395（ConVeY）和亚历山大·冯·洪堡教授职位资助。

## 参考文献

[1] Alur, R.：混合系统形式验证。载于：Chakraborty, S.、Jerraya, A.、Baruah, S.K.、Fischmeister, S.（编），第11届国际嵌入式软件会议（EMSOFT）论文集。第 273 278 2011 10 1145 2038642 2038685 –页。ACM Press [2] （）。doi：。/。Alur, R.、Courcoubetis, C.、Henzinger, T.A.、Ho, P.：混合自动机：混合系统规约与验证的算法方法。载于：Grossman, R.L.、Nerode, A.、Ravn, A.P.、Rischel, H.（编），第1届和第2届国际混合系统研讨会（HS）论文集。LNCS，第736卷，第209–229页。Springer（1993年）。doi： 10 1007 3 540 57318 6_30 。/---Apt, K.R.、de Boer, F.S.、Olderog, E.R.：顺序与并发程序验证。Springer, 3 2010 10 1007 978 1 84882 745 5 版 [3] （）。doi：。/----Benvenuti, L.、Bresolin, D.、Collins, P.、Ferrari, A.、Geretti, L.、Villa, T.：利用 ARIADNE 对非线性混合系统进行假设-保证验证。《鲁棒非线性控制国际期刊》 **24**, 699 724 2014 10 1002 2914 – （）。doi：。/rnc。 [4] Bradley, A.R.、Manna, Z.、Sipma, H.B.：关于数组，有哪些问题是可判定的？载于：Emerson, E.A.、Namjoshi, K.S.（编），验证、模型检测与抽象解释，第7届国际会议，VMCAI 2006，美国南卡罗来纳州查尔斯顿，2006年1月8日至10日，论文集。LNCS，第3855卷，第427–442页。Springer（2006年）。doi： 10 1007 11609773_28 。/Cong, X.、Yu, H.、Xu, X.：使用 Phaver 验证信息物理系统的混合χ模型。载于：Barolli, L.、You, I.、Xhafa, F.、Leu, F.、Chen, H.（编），第七届普适计算领域创新移动与互联网服务国际会议，IMIS 2013，中国台湾台中，2013年7月3日至5日。第122– 128 2013 10 1109 2013 29 页。IEEE计算机学会（）。 [6] doi：。/IMIS。。Frehse, G.：Phaver：超越 Hytech 的混合系统算法验证。《软件工具与技术转移国际期刊》**10**（3），263–279（2008年）。doi：10.1007/s10009-007-0062-x [7] [8] Frehse, G.、Han, Z.、Krogh, B.H.：通过过近似连续交互，对混合输入/输出自动机进行假设-保证推理。载于：第43届IEEE 决策与控制会议（CDC）论文集。第479–484页。IEEE（2004年）。doi： 10 1109 2004 1428676 。/CDC。。Fulton, N.、Mitsch, S.、Quesel, J.D.、V¨olp, M.、Platzer, A.：KeYmaera X：混合系统的公理化策略定理证明器。载于：Felty, A.、Middeldorp, A.（编），CADE。LNCS，第9195卷，第527–538页。Springer，柏林（2015年）。doi： 10.1007/978-3-319-21401-6 36 – [9]

[10] Guelev, D.P.、Wang, S.、Zhan, N.：时长演算中关于混合 CSP 的组合式 Hoare 风格推理。载于：Larsen, K.G.、Sokolsky, O.、Wang, J.（编），可信软件工程：理论、工具与应用——第三届国际研讨会，SETTA 2017，中国长沙，2017年10月23日至25日，论文集。LNCS，第10606卷，第110–127页。Springer（2017年）。doi：10 1007 978 3 319 69483 2_7 。/---- Harel, D.：一阶动态逻辑，[11] LNCS，第68卷。Springer（1979年）。doi：10 1007 3 540 09237 4 。/--- Henzinger, T.A.：混合自动机理论。载于：第11届 IEEE 计算机科学逻辑研讨会（LICS）论文集。第278–292页。IEEE（[12] 1996年）。doi：10 1109 1996 561342 。/LICS。。Henzinger, T.A.、Minea, M.、Prabhu, V.S.：层次化混合系统的假设-保证推理。载于：Benedetto, M.D.D.、[13] Sangiovanni-Vincentelli, A.L.（编），第4届国际混合系统：计算与控制研讨会（HSCC）论文集。LNCS，第 2034， 275 290 2001 10 1007 3 540 45351 2_24 卷，第–页。Springer（[14]）。doi：。/--- Hoare, C.A.R.：通信顺序进程。《美国计算机协会通讯》**21** 8 666 677 1978 10 1145 359576 359585 （），–（）。doi：。/。Hoare, C.A.R.：《通信顺序进程》。普伦蒂斯·霍尔国际出版社（1985年）[15][16] Hooman, J.：实时分布式消息传递的组合式证明理论。载于：de Bakker, J.W.、Nijman, A.J.、Treleaven, P.C.（编），PARLE，欧洲并行体系结构与语言，第II卷：并行语言，荷兰埃因霍温，1987年6月15日至19日，论文集。LNCS，第259卷，第315–332页。Springer（ 1987 10 1007 3 540 17945 3_18 ）。doi：。/---Hooman, J.J.M. 、 de Roever, W.P.：[17] 并发组合方法及其在实时系统中的应用简介。S¯adhan¯a 17(1), 29–73（1992年）。doi：10 1007 02811338 。/BF Jifeng, H.：《古典思想》：纪念 C. A. R. Hoare 的论文集，第“从 CSP[18] 到混合系统”章，第171–189页。普伦蒂斯·霍尔国际出版社（1994年）[19] Kamburjan, E.、Schlatte, R.、Johnsen, E.B.、Tarifa, S.L.T.：利用混合主动对象设计分布式控制。载于：Margaria, T.、Steffen, B.（编），第9届国际形式化方法应用：工具与趋势研讨会（ISoLA）论文集。LNCS，第12479卷，第88–108页。Springer（2020年）。doi：10 1007 978 3 030 83723 5_7 。/---- Levin, G.、Gries, D.：通信顺序进程的证明技术。Acta Informatica[20] **15** 3 281 302 1981 10 1007 00289266 （），–（）。doi：。/BF Liu, J.、Lv, J.、Quan, Z.、Zhan, N.、Zhao, H.、Zhou, C.、Zou, L.：[21] 混合 CSP 演算。载于：Ueda, K.（编），第8届亚洲编程语言与系统研讨会（APLAS）论文集。LNCS，第6461卷，第1–15页。Springer（2010年）。doi：10 1007 978 3 642 17164 2_1 。/---- Lunel, S.、Mitsch, S.、Boyer, B.、Talpin, J.：微分动态逻辑[22]中计算机控制系统的并行组合与模块化验证。载于：ter Beek, M.H.、McIver, A.、Oliveira, J.N.（编），第3届世界形式化方法大会——未来三十年（FM）论文集。LNCS，第11800卷，第354–370页。Springer（ 2019 10 1007 978 3 030 30942 8_22 ）。doi：。/----Lynch, N.A. 、 Segala, R. 、 Vaandrager, F.W.：[23] 混合输入 / 输出自动机。《信息与计算》**185** 1 105 157 2003 10 1016 0890 5401 03 00067 1 （），–（）。doi：。/S-()- Man, K.L.、Reniers, M.A.、Cuijpers, P.J.L.：[24] 混合进程代数 HyPA 的案例研究。《软件工程与知识工程国际期刊》15(2)，299–306（2005年）。doi：10 1142 0218194005002385 。/S Misra, J.、Chandy, K.M.：进程网络证明。《IEEE 软件工程汇刊》[25] **7** 4 417 426 1981 10 1109 1981 230844 （），–（）。doi：。/TSE。。Muller, A.、Mitsch, S.、Retschitzegger, W.、Schwinger, W.、Platzer, A.：[26] 用于混合系统组件验证的战术式契约组合。STTT 20(6)，615–643（2018年）。doi：10.1007/s10009-018-0502-9, FASE'[27] 精选论文专刊 Owicki, S.S.、Gries, D.：并行程序的公理化证明技术 I。

Acta Informatica **6**, 319 340 1976 10 1007 00268134 – ( ). doi: . /BF [28] Peleg, D.：并发动态逻辑中的通信。J. Comput. Syst. Sci. **35** 1 23 58 1987 10 1016 0022 0000 87 90035 3 ( ), – ( ). doi: . / - ( ) - Peleg, D.：并发动态逻辑。[29] J. ACM ( ), 450–479 (1987). doi: 10 1145 23005 23008 . / . Platzer, A.：用于混合系统的微分动态逻辑。J. **34** 2 Autom. Reas. 41(2), 143 189 2008 10 1007 10817 008 9103 8 – ( ). doi: . /s - - - Platzer, A.：[30] 《混合系统的逻辑分析：复杂动力学定理的证明》。Springer, Heidelberg ( [31] 2010 10 1007 978 3 642 14509 4 ). doi: . / - - - - Platzer, A.：分布式混合系统的量化微分动态逻辑。载于：Dawar, A., Veith, H.（编）CSL。LNCS, vol. 6247, pp. 469–483。[32] Springer ( 2010 10 1007 978 3 642 15205 4_36 ). doi: . / - - - - Platzer, A.：微分动态逻辑的完备一致替换演算。J. Autom. Reas. [33] **59** 2 219 265 2017 10 1007 10817 016 9385 1 ( ), – ( ). doi: . /s - - - Platzer, A.：《信息物理系统的逻辑基础》。Springer, Cham ( 2018 10 1007 978 3 319 63588 0 ). [34] doi: . / - - - - Platzer, A., Tan, Y.K.：微分方程公理化：微分幽灵的惊人威力。载于：Dawar, A., Gr¨adel, E. [35] （编）LICS。pp. 819–828。ACM, New York ( 2018 10 1145 3209108 3209147 ). doi: . / . Platzer, A., Tan, Y.K.：微分方程不变性公理化。J. ACM **67** 1 6 1 6 66 2020 10 1145 3380825 [36] ¨ ¨ ( ), : – : ( ). doi: . / Presburger, M.：《关于一种整数算术系统的完备性，该系统中加法是唯一显式出现的运算》。[37] 载于：Comptes Rendus du I congr`es de Math´ematiciens des Pays Slaves (1931) [38] de Roever, W.P., de Boer, F.S., Hannemann, U., Hooman, J.J.M., Lakhnech, Y., Poel, M., Zwiers, J.：《并发验证：组合与非组合方法导论》，Cambridge Tracts in Theoretical Computer Science, vol. 54。Cambridge University Press (2001) [39] Song, H., Compton, K.J., Rounds, W.C.：SPHIN：一种基于 SPIN 的可重配置混合系统模型检查器。载于：Lazic, R., Nagarajan, R.（编）《第 5 届关键系统自动验证国际研讨会论文集》，AVoCS 2005，英国华威大学，2005 年 9 月 12–13 日。ENTCS, vol. 145, 167 183 2005 10 1016 2005 10 011 pp. – 。Elsevier ( ). [40] doi: . /j.entcs. . . Tarski, A.：《初等代数与几何的判定方法》。University of California Press, Berkeley, 2 1951 10 1525 9780520348097 nd edn. ( ). doi: . / Wang, [41] S., Zhan, N., Guelev, D.P.：一种基于假设/保证的混合 CSP 组合演算。载于：Agrawal, M., Cooper, S.B., Li, A.（编）《第 9 届计算模型理论与应用会议（TAMC）论文集》。LNCS, vol. 7287, pp. 72 83 2012 10 1007 978 3 642 29952 0_13 – 。Springer ( ). doi: . / - - - - Zwiers, J.：[42] 《组合性、并发与部分正确性——进程网络的证明理论及其相互关系》，LNCS, vol. 321。Springer ( 1989 10 1007 0020836 ). doi: . /BFb Zwiers, J., de Bruin, A., de Roever, W.P.：动态进程网[43] 络部分正确性的证明系统（扩展摘要）。载于：Clarke, E.M., Kozen, D.（编）《卡内基梅隆大学 1983 年程序逻辑研讨会论文集》。LNCS, vol. 164, pp. 513 527 1983 10 1007 3 540 12896 4_384 – 。Springer ( ). doi: . / - - - Zwiers, J., [44] de Roever, W.P., van Emde Boas, P.：组合性与并发网络：证明系统的可靠性与完备性。载于：Brauer, W.（编）《第 12 届自动机、语言与程序设计国际讨论会（ICALP）论文集》。LNCS, vol. 194, pp. 509–519。Springer (1985). doi: 10.1007/BFb0015776

## A 语义细节

我们为定义 9 中的项给出形式语义，在命题2中证明通信混合程序的语义是前缀闭合且全的，并证明 $d\mathcal{L}_{\mathrm{CHP}}$ 是 $d\mathcal{L}$ 的保守扩展（见命题1）。此外，我们证明第 2.2 节中的算子 $\hat{\circ}$ 是结合的。

我们将项的语义改编自 Zwiers [42, p. 113]，并将实数算术作为基础项融入我们的设定。为了定义项的语义，我们使用以下定义中的轨迹算子：

定义 8（轨迹算子）。设 $\tau = (\tau_1,\ldots,\tau_n) \in \mathcal{T}$为一个包含通信事件 $\tau_i$的轨迹。那么，我们将其长度 $|\tau|$ 定义为 $n$。此外，$|\epsilon| = 0$。对于 $\tau \in \mathcal{T}$和 $k \in \mathbb{N}$，我们将 $at(\tau, k)$ 定义为 $\tau_{k+1}$，其中 $0 \leq k < |\tau|$。否则，我们将 $at(\tau, k)$ 定义为 $= \epsilon$。

对于通信事件 $\rho = \langle \mathrm{ch}\ a, s\rangle$ 或 $\rho = \langle h, \mathrm{ch}\ a, s\rangle$，我们将通道访问 $chan(\rho)$ 定义为 $=$ ch，将值访问 $val(\rho)$ 定义为 $= a$，并将时间戳访问 $time(\rho)$ 定义为 $= s$。此外，对于某个 ch $\in \Omega$，我们将 $chan(\epsilon)$ 定义为 $=$ ch，并将 $val(\epsilon)$ 定义为 $= 0$，以及将 $time(\epsilon)$ 定义为 $= 0$。

定义 9（项的值）。项$e \in \mathrm{Trm}(V, \Omega)$ $[\![e]\!]v \subseteq \mathbb{R} \cup \mathbb{N} \cup \Omega \cup \mathcal{T}$在状态 $v$ 上的值 $[\![e]\!]v \subseteq \mathbb{R} \cup \mathbb{N} \cup \Omega \cup \mathcal{T}$是通过归纳法在图9中定义的。

$[\![x]\!]v = v\ x \quad x \in V_{\mathbb{R}} \cup \{\mu\}$ $\qquad$ $[\![n]\!]v = v$ $[\![\kappa]\!]v = \kappa$ ( ) ( ) $(n)$ (

$[\![c]\!]v = c$

$[\![\eta_1 + \eta_2]\!]v = [\![\eta_1]\!]v + [\![\eta_2]\!]v$

$[\![\eta_1 \cdot \eta_2]\!]v = [\![\eta_1]\!]v \cdot [\![\eta_2]\!]v$

$[\![ie_1 + ie_2]\!]v = [\![ie_1]\!]v + [\![ie_2]\!]v$

$\kappa \in \{0, 1\}$) $\qquad$ $[\![|te|]\!]v = |[\![te]\!]v|$ $\qquad$ $[\![值(te[ie])]\!]v = val(at([\![te]\!]v, [\![ie]\!]v))$ (c)

整数项$[\![时间(te[ie])]\!]v = time(at([\![te]\!]v, [\![ie]\!]v))$ $[\![h]\!]v = v(h)$ (a) 实数项 $[\![\epsilon]\!]v = \epsilon$

$[\![ch]\!]v =$ ch $[\![信道(te[ie])]\!]v = chan(at([\![te]\!]v, [\![ie]\!]v))$ $[\![\langle$ch

$\theta_1\ \theta_2\rangle]\!]v = \langle\ [\![\theta_1]\!]v\ [\![\theta_2]\!]v\rangle$ , ch , ( ) (b)信道项 (d) 迹项

$[\![te_1 \cdot te_2]\!]v = [\![te_1]\!]v \cdot [\![te_2]\!]v$

$[\![te \downarrow C]\!]v = [\![te]\!]v \downarrow C$

图9：在状态 $v \in \mathcal{S}$ [42, p 上，项 $e \in \mathrm{Trm}(V, \Omega)$ 的赋值 $[\![e]\!]v \subseteq \mathbb{R} \cup \mathbb{N} \cup \Omega \cup \mathcal{T}$ 113] 的归纳定义。

命题 2（前缀闭合且全的）。设 $\gamma \in \mathrm{CHP}(V, \Omega)$ 是一个程序。那么，它的语义 $[\![\gamma]\!] \subseteq \mathcal{D}$ 是前缀闭合且全的，即，如果 $(v, \tau, w) \in [\![\gamma]\!]$ 且 $(\tau', w') \preceq (\tau, w)$，那么 $(v, \tau', w') \in [\![\gamma]\!]$，并且 $\perp_{\mathcal{D}} \subseteq [\![\gamma]\!]$。

证明。我们对程序 $\gamma$的结构进行归纳法。对于所有程序 $\alpha$ 和所有 $n \in \mathbb{N}$，我们认为 $\alpha^n$在结构上小于 $\alpha^*$ 。不失一般性。

在证明前缀闭合性时，我们假设$(\tau', w') \prec (\tau, w)$，因为如果$(v, \tau, w) \in [\![\gamma]\!]$且$(\tau', w') = (\tau, w)$，则$(v, \tau', w') \in [\![\gamma]\!]$显然成立。

1. $\gamma \in \{x := \theta, x := *, ?\chi, \{x' = \theta \,\&\, \chi\}\}$，则带有 $U \subseteq \mathcal{D}$ 的 $[\![\gamma]\!] = \bot_{\mathcal{D}} \cup U$。现在，令 $(v, \tau, w) \in [\![\gamma]\!]$，且 $(\tau', w') \prec (\tau, w)$。则由于 $\tau = \epsilon$，有 $\tau' = \epsilon$，并且 $w' = \bot$。因此，$(v, \tau', w') \in \bot_{\mathcal{D}} \subseteq [\![\gamma]\!]$。最后，$[\![\gamma]\!]$ 是全的，因为 $\bot_{\mathcal{D}} \subseteq [\![\gamma]\!]$。2. $\gamma \in \{\mathsf{ch}(h)!\theta, \mathsf{ch}(h)?x\}$，则令 $(v, \tau, w) \in [\![\gamma]\!]$，且 $(\tau', w') \prec (\tau, w)$。由于对某个 $(\tilde{\tau}, \tilde{w})$，$(v, \tau, w) \in [\![\gamma]\!]$ 当且仅当 $(\tau, w) \preceq (\tilde{\tau}, \tilde{w})$，我们得到 $(v, \tau', w') \in [\![\gamma]\!]$，因为 $(\tau', w') \prec (\tau, w) \preceq (\tilde{\tau}, \tilde{w})$。由于对任意 $(\tilde{\tau}, \tilde{w})$，$(\epsilon, \bot) \preceq (\tilde{\tau}, \tilde{w})$，对于每个使得 $[\![\gamma]\!]$ 为全的 $v \in \mathcal{S}$，有 $(v, \epsilon, \bot) \in [\![\gamma]\!]$。3. $\gamma \equiv \alpha \cup \beta$，则根据归纳假设，$[\![\alpha]\!]$ 和 $[\![\beta]\!]$ 均为前缀闭合且全的。由 $[\![\gamma]\!] = [\![\alpha]\!] \cup [\![\beta]\!]$ 可容易地得出 $[\![\gamma]\!]$ 的前缀闭合性和全性。4. $\gamma \equiv \alpha; \beta$，则令 $(v, \tau, w) \in [\![\gamma]\!] = [\![\alpha]\!]_{\bot} \cup [\![\alpha]\!] \triangleright [\![\beta]\!]$，且 $(\tau', w') \prec (\tau, w)$。因此，$w' = \bot$ 和 $\tau' \preceq \tau$。注意到，$[\![\alpha]\!]_{\bot}$ 是前缀闭合的，因为根据归纳假设，$[\![\alpha]\!]$ 是前缀闭合的。因此，若 $(v, \tau, w) \in [\![\alpha]\!]_{\bot}$，则 $(v, \tau', w') \in [\![\alpha]\!]_{\bot} \subseteq [\![\gamma]\!]$。若 $(v, \tau, w) \in [\![\alpha]\!] \triangleright [\![\beta]\!]$，则存在 $u \neq \bot$，使得 $(v, \tau_1, u) \in [\![\alpha]\!]$，$(u, \tau_2, w) \in [\![\beta]\!]$，且 $\tau = \tau_1 \cdot \tau_2$。若 $\tau_1$ 完全包含于 $\tau'$ 中，即对某个 $\tau_2'$ 有 $\tau' = \tau_1 \cdot \tau_2'$，则 $\tau_2' \preceq \tau_2$ 且 $(\tau_2', w') \preceq (\tau_2, w)$。由于根据归纳假设，$[\![\beta]\!]$ 是前缀闭合的，我们得到 $(u, \tau_2', w') \in [\![\beta]\!]$，这蕴含 $(v, \tau', w') \in [\![\alpha]\!] \triangleright [\![\beta]\!] \subseteq [\![\gamma]\!]$。否则，若 $\tau' \prec \tau_1 \preceq \tau$，其中 $\tau_1$ 未完全包含于 $\tau'$ 中，则由于 $w' = \bot$，有 $(\tau', w') \preceq (\tau_1, u)$。因此，$(v, \tau', w') \in [\![\alpha]\!]$，因为根据归纳假设，$[\![\alpha]\!]$ 是前缀闭合的。最后，$(v, \tau', w') \in [\![\alpha]\!]_{\bot} \subseteq [\![\gamma]\!]$。由于根据归纳假设，$[\![\alpha]\!]$ 是全的，$\bot_{\mathcal{D}} \subseteq [\![\alpha]\!]$，这蕴含 $\bot_{\mathcal{D}} [\![\alpha]\!]_{\bot} \subseteq [\![\alpha; \beta]\!]$。5. $\gamma \equiv \alpha^*$，则根据归纳假设，对于所有 $n \in \mathbb{N}$，$[\![\alpha^n]\!]$ 都是前缀闭合的，因为我们认为 $\alpha^n$ 在结构上小于 $\alpha^*$。这很容易蕴含 $[\![\alpha^*]\!] = \bigcup_{n \in \mathbb{N}} [\![\alpha^n]\!]$ 是前缀闭合的。最后，$[\![\gamma]\!]$ 是全的，因为 $[\![\alpha]\!] \subseteq [\![\gamma]\!]$，且根据归纳假设，$[\![\alpha]\!]$ 是全的。6. $\gamma \equiv \alpha_1 \parallel \alpha_2$，则令 $(v, \tau, w) \in [\![\gamma]\!]$，且 $(\tau', w') \prec (\tau, w)$。因此，$w' = \bot$ 和 $\tau' \preceq \tau$。此外，对于 $j = 1, 2$，$(v, \tau \downarrow \alpha_j, w_{\alpha_j}) \in [\![\alpha_j]\!]$，且 $w_{\alpha_1}(\mu) = w_{\alpha_2}(\mu)$，并且 $\tau = \tau \downarrow \gamma$，以及 $w = w_{\alpha_1} \oplus w_{\alpha_2}$。现在，注意到 $\tau' \downarrow \alpha_j \preceq \tau \downarrow \alpha_j$，这蕴含对于 , 有 ( $\tau' \downarrow \alpha_j$ $w'_{\alpha_j}$ $\preceq$ $\tau \downarrow \alpha_j$ $w_{\alpha_j}$ $w'_{\alpha_j} = \bot$ $v$ $\tau' \downarrow$, ) ( , )。因此，( , $\alpha_j$ $w'_{\alpha_j} \in [\![\alpha_j]\!]$ $[\![\alpha_j]\!]$ $\bot = \bot \oplus \bot$ , )，因为根据归纳假设 是前缀闭合的。由于 , 有 $w' = w'_{\alpha_1} \oplus w'_{\alpha_2}$。此外，$\tau' = \tau' \downarrow \gamma$，且 $\tau'$ 是按时间顺序的，因为它是按时间顺序的轨迹 $\tau$ 的前缀 $\tau' \preceq \tau$。最后，$(v, \tau', w') \in [\![\gamma]\!]$。对于每个 $v \in \mathcal{S}$ 和 $j = 1, 2$，由于根据归纳假设，$[\![\alpha_j]\!]$ 是全的，存在某个 $(v, \epsilon, \bot) \in [\![\alpha_j]\!]$。于是 $[\![\gamma]\!]$ 是全的，因为对于每个 $v \in \mathcal{S}$，$(v, \epsilon, \bot) \in [\![\gamma]\!]$，因为 $\bot(\mu) = \bot(\mu)$，且 $\epsilon = \epsilon \downarrow \gamma$，以及 $\bot = \bot \oplus \bot$。□

为证明保守扩展（命题1），我们在以下 [30]中粗略回顾 $d\mathcal{L}$：

注2（$d\mathcal{L}$）。${}_{d\mathcal{L}} = \mathbb{Q}[V_{\mathbb{R}}] \subset \mathsf{Trm}V\mathsf{Trm}(\Omega, d\mathcal{L})$中的项是 $V_{\mathbb{R}}$ 上关于 $\mathbb{Q}$的多项式。此外，${}_{d\mathcal{L}} \subset \mathsf{HP}V\mathsf{CHP}(\Omega, d\mathcal{L})$中的混合程序由以下语法生成：$\alpha, \beta ::= x := \theta \mid x := * \mid ?\chi \mid \{x' = \theta \,\&\, \chi\} \mid \alpha; \beta \mid \alpha \cup \beta \mid \alpha^*$，其中 $\theta \in \mathsf{Trm}_{d\mathcal{L}}$，而 $\chi \in \mathsf{FOL}_{\mathbb{R}}(V_{\mathbb{R}})$是一阶实数算术的公式。最后，$\mathsf{Fml}_{d\mathcal{L}}$ 表示 $d\mathcal{L}$ 中由语法 $\varphi, \psi ::= \theta_1 \sim \theta_2 \mid \neg\varphi \mid \varphi \wedge \psi \mid \varphi \vee \psi \mid \varphi \to \psi \mid \forall x\, \varphi \mid \exists x\, \varphi \mid [\alpha]\psi \mid \langle\alpha\rangle\psi$生成的所有公式的集合，其中 $\sim \in \{=, \geq\}$。注意，$\mathsf{FOL}_{\mathbb{R}}(V_{\mathbb{R}}) \subset \mathsf{Fml}_{d\mathcal{L}}$。

实数状态是从 $V_{\mathbb{R}}$ 到 $\mathbb{R}$ 的映射，且 $\mathcal{R}$ 表示所有实数状态的集合。我们用 $[\![\cdot]\!]_{d\mathcal{L}} \subseteq \mathcal{R}$ 表示项的语义，用 $\vDash_{d\mathcal{L}} \subseteq \mathcal{R} \times \mathsf{Fml}_{d\mathcal{L}}$ 表示 $d\mathcal{L}$中的满足关系。混合程序 $[\![\alpha]\!]_{d\mathcal{L}} \subseteq \mathcal{R}\times\mathcal{R}$ HP $\alpha \in$的语义$_{d\mathcal{L}}$ 归纳定义如下:

$$
\begin{aligned}
&[\![x := \theta]\!]_{d\mathcal{L}} = \{(v,w) \in \mathcal{R}\times\mathcal{R} \mid w = v_x^{[\![\theta]\!]_{d\mathcal{L}} v}\}\\
&[\![x := *]\!]_{d\mathcal{L}} = \{(v,w) \in \mathcal{R}\times\mathcal{R} \mid w(y) = v(y) \text{ for all } y \neq x\}\\
&[\![\{x' = \theta \,\&\, \chi\}]\!]_{d\mathcal{L}} = \{(\varphi(0),\varphi(r)) \in \mathcal{R}\times\mathcal{R} \mid\\
&\qquad \varphi(\zeta) \vDash_{d\mathcal{L}} x' = \theta \wedge \chi \text{ and } \varphi(\zeta) = \varphi(0) \text{ on } \{x\}^{\complement} \text{ for all } \zeta \in [0,r]\\
&\qquad \text{for a solution } \varphi : [0,r] \to \mathcal{R} \text{ with } \varphi(\zeta)(x') = \frac{d\varphi(t)(x)}{dt}(\zeta)\}\\
&[\![?\chi]\!]_{d\mathcal{L}} = \{(v,v) \in \mathcal{R}\times\mathcal{R} \mid v \vDash_{d\mathcal{L}} \chi\}\\
&[\![\alpha \cup \beta]\!]_{d\mathcal{L}} = [\![\alpha]\!]_{d\mathcal{L}} \cup [\![\beta]\!]_{d\mathcal{L}}\\
&[\![\alpha;\beta]\!]_{d\mathcal{L}} = [\![\alpha]\!]_{d\mathcal{L}} \circ [\![\beta]\!]_{d\mathcal{L}} \quad (\circ \text{ is composition of relations})\\
&[\![\alpha^*]\!]_{d\mathcal{L}} = \bigcup_{n\in\mathbb{N}} [\![\alpha^n]\!]_{d\mathcal{L}}
\end{aligned}
$$

对于状态 $v \in \mathcal{S}$，实数状态 $v|_{V_{\mathbb{R}}} \in \mathcal{R}$ 是 $v$ 在 $V_{\mathbb{R}}$上的限制。集合 $U \subseteq \mathcal{S} \times \mathcal{T}_{\text{rec}} \times \mathcal{S}_{\perp}$ 在 $\mathcal{R}\times\mathcal{R}$ 上的限制 $U|_{\mathcal{R}\times\mathcal{R}}$ 定义如下:

$$U|_{\mathcal{R}\times\mathcal{R}} = \{(v|_{V_{\mathbb{R}}}, w|_{V_{\mathbb{R}}}) \in \mathcal{R}\times\mathcal{R} \mid (v,\tau,w) \in U \text{ with } w \neq \perp\}.$$

为命题 1 的证明做准备，引理 1 指出， $d\mathcal{L}_{\text{CHP}}$ 相对于混合程序 $\mathsf{HP}_{d\mathcal{L}}$中的项和公式，是 $d\mathcal{L}$ 的保守扩展。基于这一点，引理 2 表明，CHP 的语义是 $d\mathcal{L}$ 中程序语义的保守扩展。我们继续用 $[\![\cdot]\!]$ 表示 $d\mathcal{L}_{\text{CHP}}$ 中项和程序的语义，并用 $\vDash$表示满足关系。

引理 1（程序部分的保守扩展）。设 $\theta \in \mathsf{Trm}_{d\mathcal{L}}$ 是一个 $d\mathcal{L}$-项，且 $\chi \in \mathsf{FOL}_{\mathbb{R}}(V_{\mathbb{R}})$ 是一阶实数算术的公式。那么对于所有状态 $v \in \mathcal{S}$，以下结论成立:

1. $[\![\theta]\!]_{d\mathcal{L}} v|_{V_{\mathbb{R}}} = [\![\theta]\!]v$2.
   $v|_{V_{\mathbb{R}}} \vDash_{d\mathcal{L}} \chi$ 当且仅当 $v \vDash \chi$

证明。证明分别对 $\theta$ 和 $\chi$ 的结构进行归纳。 □

引理 2（保守的程序语义）。$d\mathcal{L}_{\text{CHP}}$ 的程序语义是 $d\mathcal{L}$ 中程序语义的保守扩展。也就是说,

$$[\![\gamma]\!]_{d\mathcal{L}} = [\![\gamma]\!]|_{\mathcal{R}\times\mathcal{R}} = \{(v|_{V_{\mathbb{R}}}, w|_{V_{\mathbb{R}}}) \mid (v,\tau,w) \in [\![\gamma]\!] \; with \; w \neq \perp\}$$

对于混合程序 $\gamma \in \mathsf{HP}_{d\mathcal{L}} \subset \mathsf{CHP}(V,\Omega)$。

证明。证明采用对程序 $\gamma$的结构进行归纳法。对于所有程序 $\alpha$ 以及所有 $n \in \mathbb{N}$，我们认为 $\alpha^n$在结构上小于 $\alpha^*$ 。

1. 对于 $\gamma \in \{x := \theta, x := *, ?\chi, \{x' = \theta \,\&\, \chi\}\}$，我们有 $[\![\gamma]\!] = \bot_{\mathcal{D}} \cup M_\gamma$，其中某个 $M_\gamma \subseteq \mathcal{S} \times \{\epsilon\} \times \mathcal{S}$。注意到 $[\![\gamma]\!]|_{\mathcal{R}\times\mathcal{R}} = M_\gamma|_{\mathcal{R}\times\mathcal{R}}$，因为$\bot_{\mathcal{D}} = \mathcal{S} \times \{\epsilon\} \times \{\bot\}$。最后，根据 $[\![\gamma]\!]_{d\mathcal{L}}$和 $M_\gamma$的定义可得 $[\![\gamma]\!]_{d\mathcal{L}} = M_\gamma|_{\mathcal{R}\times\mathcal{R}}$。例如，在 $\gamma \equiv x := \theta$的情况下，我们得到 $M_\gamma|_{\mathcal{R}\times\mathcal{R}} = \{(v, \epsilon, w) \mid w = v_x^{[\![\theta]\!]v}\}|_{\mathcal{R}\times\mathcal{R}} = \{(v|_{V_{\mathbb{R}}}, w|_{V_{\mathbb{R}}}) \mid w = v_x^{[\![\theta]\!]v}\} = \{(v|_{V_{\mathbb{R}}}, w|_{V_{\mathbb{R}}}) \mid w|_{V_{\mathbb{R}}} = (v|_{V_{\mathbb{R}}})_x^{[\![\theta]\!]_{d\mathcal{L}} v|_{V_{\mathbb{R}}}}\} = [\![x := \theta]\!]_{d\mathcal{L}}$，因为根据引理 1，$[\![\theta]\!]v = [\![\theta]\!]_{d\mathcal{L}} v|_{V_{\mathbb{R}}}$。2. 对于 $\gamma \equiv \alpha \cup \beta$，注意到 $[\![\alpha]\!]|_{\mathcal{R}\times\mathcal{R}} \cup [\![\beta]\!]|_{\mathcal{R}\times\mathcal{R}} = ([\![\alpha]\!] \cup [\![\beta]\!])|_{\mathcal{R}\times\mathcal{R}}$。然后根据归纳假设，$[\![\gamma]\!]_{d\mathcal{L}} = [\![\alpha]\!]_{d\mathcal{L}} \cup [\![\beta]\!]_{d\mathcal{L}}$ 归纳假设$= [\![\alpha]\!]|_{\mathcal{R}\times\mathcal{R}} \cup [\![\beta]\!]|_{\mathcal{R}\times\mathcal{R}} = [\![\gamma]\!]|_{\mathcal{R}\times\mathcal{R}}$。3. 对于 $\gamma \equiv \alpha;\beta$，我们有 $[\![\gamma]\!]|_{\mathcal{R}\times\mathcal{R}} = [\![\alpha]\!]_\bot|_{\mathcal{R}\times\mathcal{R}} \cup ([\![\alpha]\!] \triangleright [\![\beta]\!])|_{\mathcal{R}\times\mathcal{R}}$，因为限制 $\cdot|_{\mathcal{R}\times\mathcal{R}}$ 对并集 $\cup$满足分配律。注意到 $[\![\alpha]\!]_\bot|_{\mathcal{R}\times\mathcal{R}} = \emptyset$ 和$([\![\alpha]\!] \triangleright [\![\beta]\!])|_{\mathcal{R}\times\mathcal{R}} = [\![\alpha]\!]|_{\mathcal{R}\times\mathcal{R}} \circ [\![\beta]\!]|_{\mathcal{R}\times\mathcal{R}}$，其中 $\circ$是关系复合。因此，根据归纳假设，$[\![\gamma]\!]_{d\mathcal{L}} = [\![\alpha]\!]_{d\mathcal{L}} \circ [\![\beta]\!]_{d\mathcal{L}}$ 归纳假设 $= [\![\alpha]\!]|_{\mathcal{R}\times\mathcal{R}} \circ [\![\beta]\!]|_{\mathcal{R}\times\mathcal{R}} = [\![\gamma]\!]|_{\mathcal{R}\times\mathcal{R}}$。4. $\gamma \equiv \alpha^*$，那么对于某个 $n \in \mathbb{N}$，$(v, w) \in [\![\alpha^*]\!]_{d\mathcal{L}}$ 当且仅当$(v, w) \in [\![\alpha^n]\!]_{d\mathcal{L}}$；而根据归纳假设，对于某个 $n \in \mathbb{N}$，$(v, w) \in [\![\alpha^n]\!]|_{\mathcal{R}\times\mathcal{R}}$ 当且仅当$(v, w) \in [\![\alpha^*]\!]|_{\mathcal{R}\times\mathcal{R}}$。□

证明（命题 1）。我们需要证明，公式 $\varphi \in \mathrm{Fml}(V, \Omega) \cap \mathrm{Fml}_{d\mathcal{L}}$ 在 $d\mathcal{L}_{\mathrm{CHP}}$ 中有效，当且仅当它在 $d\mathcal{L}$ 中有效；其中，$\varphi$ 在 $d\mathcal{L}$ 中有效，当且仅当 $v|_{V_{\mathbb{R}}} \vDash_{d\mathcal{L}} \varphi$ 对所有 $v \in \mathcal{S}$ 都成立；$\varphi$ 在 $d\mathcal{L}_{\mathrm{CHP}}$ 中有效，当且仅当 $v \vDash \varphi$ 对所有 $v \in \mathcal{S}$ 都成立。证明对 $\varphi$ 的结构进行归纳:

1. $\varphi \equiv \theta_1 \sim \theta_2$，其中 $\sim \in \{=, \geq\}$，则 $v \vDash \theta_1 \sim \theta_2$ 当且仅当 $[\![\theta_1]\!]v \sim [\![\theta_2]\!]v$，根据引理 1，$[\![\theta_1]\!]_{d\mathcal{L}} v|_{V_{\mathbb{R}}} \sim [\![\theta_2]\!]_{d\mathcal{L}} v|_{V_{\mathbb{R}}}$ 当且仅当 $v|_{V_{\mathbb{R}}} \vDash_{d\mathcal{L}} e_1 \sim e_2$。2. 对于命题联结词 $\neg$、$\wedge$、$\vee$、$\rightarrow$ 以及量词 $\forall$、$\exists$，由归纳假设可直接得证。3. 对于 $\varphi \equiv [\alpha]\psi$，注意到 $(v|_{V_{\mathbb{R}}}, w|_{V_{\mathbb{R}}}) \in [\![\alpha]\!]_{d\mathcal{L}}$ 当且仅当 $(v, \tau, w) \in [\![\alpha]\!]$，其中 $w \neq \bot$ 由引理 2 得出，且 $\tau = \epsilon$ 是因为 $\alpha \in \mathrm{CHP}(V, \Omega)$。因此，$v \vDash [\alpha]\psi$ 当且仅当 $w \cdot \tau \vDash \psi$ 对所有 $(v, \tau, w) \in [\![\alpha]\!]$ 都成立；由归纳假设，$w \cdot \tau = w \neq \bot$ 当且仅当 $w|_{V_{\mathbb{R}}} \vDash_{d\mathcal{L}} \psi$ 对所有 $(v, \tau, w) \in [\![\alpha]\!]$都成立；$w \neq \bot$ 当且仅当 $w|_{V_{\mathbb{R}}} \vDash_{d\mathcal{L}} \psi$ 对所有 $(v|_{V_{\mathbb{R}}}, w|_{V_{\mathbb{R}}}) \in [\![\alpha]\!]_{d\mathcal{L}}$ 都成立；$v|_{V_{\mathbb{R}}} \vDash_{d\mathcal{L}} [\alpha]\psi$。□

引理3表明，复合算子$\hat{\circ}$是结合的。相关算子的定义见第 2.2 节。

引理 3（复合是结合的）。设 $U, M, L \subseteq \mathcal{S} \times \mathcal{T}_{rec} \times \mathcal{S}_\bot$。则$U \hat{\circ} (M \hat{\circ} L) = (U \hat{\circ} M) \hat{\circ} L$。

证明。设 $(v, \tau, w) \in U \hat{\circ} (M \hat{\circ} L)$。若 $(v, \tau, w) \in U_\bot$，则 $(v, \tau, w) \in U_\bot \cup (U \triangleright M)_\bot \subseteq (U \hat{\circ} M)_\bot \subseteq (U \hat{\circ} M) \hat{\circ} L$。若 $(v, \tau, w) \in U \triangleright (M \hat{\circ} L)$，则存在满足 $\tau = \tau_1 \cdot \tau_2$ 的计算 $(v, \tau_1, u) \in U$和 $(u, \tau_2, w) \in (M \hat{\circ} L)$。现在，若 $(u, \tau_2, w) \in M_\bot$，则有 $(v, \tau, w) \in U \triangleright M_\bot = (U \triangleright M)_\bot \subseteq (U \hat{\circ} M)_\bot$。若 $(u, \tau_2, w) \in M \triangleright L$，则 $(v, \tau, w) \in U \triangleright (M \triangleright L)$。由于 $\triangleright$是结合的，$(v, \tau, w) \in (U \triangleright M) \triangleright L \subseteq (U \hat{\circ} M) \triangleright L \subseteq (U \hat{\circ} M) \hat{\circ} L$。

反之，设 $(v, \tau, w) \in (U \hat{\circ} M) \hat{\circ} L$。若 $(v, \tau, w) \in (U \hat{\circ} M)_\bot$，则 $(v, \tau, w) \in U_\bot$或 $(v, \tau, w) \in (U \triangleright M)_\bot$。若 $(v, \tau, w) \in U_\bot$，则可得 $U_\bot \subseteq U \hat{\circ} (M \hat{\circ} L)$。若 $(v, \tau, w) \in (U \triangleright M)_\bot$，则存在计算 $(v, \tau_1, u) \in U$和 $(u, \tau_2, w) \in M_\bot \subseteq M \hat{\circ} L$，满足 $\tau = \tau_1 \cdot \tau_2$。因此，$(v, \tau, w) \in U \triangleright (M \hat{\circ} L) \subseteq U \hat{\circ} (M \hat{\circ} L)$。最后，若 $(v, \tau, w) \in (U \hat{\circ} M) \triangleright L$，则存在计算 $(v, \tau_1, u) \in U \hat{\circ} M$和 $(u, \tau_2, w) \in L$，满足

$\tau = \tau_1 \cdot \tau_2$。由于 $u \neq \bot$，存在 $(v, \tau_1, u) \in U \triangleright M$，使得 $(v, \tau, w) \in (U \triangleright M) \triangleright L$。因此，$(v, \tau, w) \in U \triangleright (M \triangleright L) \subseteq U \triangleright (M \hat{\circ} L) \subseteq U \hat{\circ} (M \hat{\circ} L)$，因为 $\triangleright$ 是结合的。

□

## B 静态语义

静态语义通过自由变量 $FV(\cdot)$ 描述哪些变量可能影响项、程序或公式，并通过约束变量 $BV(\cdot)$ 描述程序会写入哪些变量。遵循$d\mathcal{L}$ [33] 的一般静态语义，我们给出更精确的一致性性质，并将通信历史纳入考量。因此，我们调整了 Zwiers [42] 提出的项的访问通道和通信感知一致性概念，并将其推广到 CHP 和动态逻辑公式。

备注 3（通信感知性）。通信感知一致性反映了这样一点：公式对迹变量 $h$ 的依赖所涉及的通信轨迹 $v(h)$ 部分，会随着 $h$ 的投影而缩小。例如，$|h| > 0$ 依赖于完整轨迹 $v(h)$，而 $|h{\downarrow}\mathsf{ch}| > 0$ 仅依赖于 $v(h){\downarrow}\mathsf{ch}$。项 $e$ 和公式 $\varphi$ 中的访问通道集合$CN(e)$ 和 $CN(\varphi)$，汇集了所有带有 $h \in V_{\mathcal{T}}$ 的通信轨迹 $v(h)$ 中相关的通道。

定义 10（约束变量）。程序 $\gamma \in \mathsf{CHP}(V, \Omega)$ 的约束变量集 $BV(\gamma)$ 由图 10 中的归纳定义给出。

$$
\begin{aligned}
BV(x := e) = BV(x := *) &= \{x\} \\
BV(\{x' = \theta \,\&\, \chi\}) &= \{x, \mu\} \\
BV(?\chi) &= \emptyset \\
BV(\mathrm{ch}(h)!\theta) &= \{h\} \\
BV(\mathrm{ch}(h)?x) &= \{h, x\} \\
BV(\alpha \cup \beta) = BV(\alpha; \beta) = BV(\alpha \parallel \beta) &= BV(\alpha) \cup BV(\beta) \\
BV(\alpha^*) &= BV(\alpha)
\end{aligned}
$$

图 10：程序 $\gamma \in \mathsf{CHP}(V, \Omega)$ 的约束变量集 $BV(\gamma)$ 的归纳定义。

定义 10 与通常情况相同，但连续演化会隐式地（没有语法上的出现）约束全局时间 $\mu$，因为它随每个常微分方程一起演化。引理 4 中的有界效应性质考虑到程序可达的世界由最终状态和通信组成，而不只是最终状态。

引理 4（有界效应性质）。约束变量集合 $BV(\gamma)$ 对程序 $\gamma \in \mathsf{CHP}(V, \Omega)$ 具有有界效应性质。也就是说，对于所有满足 $w \neq \bot$ 的 $(v, \tau, w)$，$v = w$ 在 $BV(\gamma)^{\complement} \cup V_{\mathcal{T}}$ 上，且 $v = w \cdot \tau$ 在 $BV(\gamma)^{\complement}$ 上。

证明。令 $REC(\gamma)$ 为 $\gamma$ 中记录变量的集合。于是，通过对 $\gamma$ 的结构进行归纳可得，对于所有 $h \notin REC(\gamma)$，$\tau(h) = \epsilon$，其中 $\tau(h)$ 是 $\tau$ 中由 $h$ 记录的通信子轨迹。因此，$w = w \cdot \tau$ 在 $REC(\gamma)^{\complement}$ 上。由于 $REC(\gamma) \subseteq BV(\gamma)$，我们得到 $v = w = w \cdot \tau$ 在 $BV(\gamma)^{\complement} \cap REC(\gamma)^{\complement} = (BV(\gamma) \cup REC(\gamma))^{\complement} = BV(\gamma)^{\complement}$，前提仅为 $v = w$ 在 $BV(\gamma)^{\complement}$ 上。后者还表明 $v = w$ 在 $BV(\alpha)^{\complement} \cup V_{\mathcal{T}}$ 上，因为通过对 $\gamma$ 进行另一次归纳可得 $v = w$ 在 $V_{\mathcal{T}}$ 上。现在，我们通过对 $\gamma$ 的结构进行归纳，证明 $v = w$ 在 $BV(\gamma)^{\complement}$ 上。对于所有程序 $\alpha$ 和所有 $n \in \mathbb{N}$，我们认为 $\alpha^n$ 在结构上小于 $\alpha^*$。

1. $\gamma \in \{x := \theta, x := *, \mathsf{ch}(h)?x\}$ 和 $(v, \tau, w) \in [\![\gamma]\!]$，则对某个 $a \in \mathbb{R}$，$w = v^a_x$。因此，$v = w$ 在 $\{x\}^{\complement} = BV(\gamma)^{\complement}$ 上。2. $\gamma \equiv \{x' = \theta \,\&\, \chi\}$ 和 $(v, \tau, w) \in [\![\gamma]\!]$，则存在一个解 $\varphi$：对于所有 $\zeta \in [0, s]$，$[0, s] \to \mathcal{S}$ 都成立，且 $\varphi(\zeta) = v$ 在 $\{x, \mu\}^{\complement}$ 上，并且 $w = \varphi(s)$。因此，$v = w$ 在 $\{x, \mu\}^{\complement} = BV(\gamma)^{\complement}$ 上。3. $\gamma \in \{?\chi, \mathsf{ch}(h)!\theta\}$ 和 $(v, \tau, w) \in [\![\gamma]\!]$，则 $v = w$。因此，$v = w$ 在 $BV(\gamma)^{\complement}$ 上。4. $\gamma \equiv \alpha; \beta$ 和 $(v, \tau, w) \in [\![\gamma]\!]$，则 $(v, \tau, w) \in [\![\alpha]\!] \triangleright [\![\beta]\!] \subseteq [\![\gamma]\!]$。因此，存在 $u \neq \bot$ 使得 $(v, \tau_1, u) \in [\![\alpha]\!]$，$(u, \tau_2, w) \in [\![\beta]\!]$，且 $\tau = \tau_1 \cdot \tau_2$。根据归纳假设，$v = u$ 在 $BV(\alpha)^{\complement}$ 上，且 $u = w$ 在 $BV(\beta)^{\complement}$ 上。因此，$v = w$ 在 $BV(\alpha)^{\complement} \cap BV(\beta)^{\complement} = (BV(\alpha) \cup BV(\beta))^{\complement} = BV(\alpha; \beta)^{\complement}$ 上。5. $\gamma \equiv \alpha \cup \beta$ 和 $(v, \tau, w) \in [\![\gamma]\!]$，则 $(v, \tau, w) \in [\![\alpha]\!]$ 或 $(v, \tau, w) \in [\![\beta]\!]$。根据归纳假设，分别有 $v = w$ $BV\ \alpha\ ^{\complement}$ $BV\ \beta\ ^{\complement}$ $v = w$ $BV\ \alpha\ ^{\complement}$ 在 ( ) 上或 $BV\ \beta\ ^{\complement} = BV\ \alpha\ \cup BV\ \beta\ ^{\complement} = BV\ \alpha \cup \beta\ ^{\complement}$ 在 ( ) 上。始终有，在 ( ) ( ) ( ( ) ( )) ( ) 上。6. $\gamma \equiv \alpha^*$ 和 $(v, \tau, w) \in [\![\gamma]\!]$，则对某个 $n \in \mathbb{N}$，$(v, \tau, w) \in [\![\alpha^n]\!]$。由于 $\alpha^n$ 在结构上小于 $\alpha^*$，根据归纳假设，我们得到 $v = w$ 在 $BV(\alpha^n)^{\complement}$ 上。最后，$BV(\alpha^n)^{\complement} \supseteq BV(\alpha)^{\complement} = BV(\alpha^*)^{\complement}$（注意 $\alpha^0 \equiv ?\mathrm{T}$）。7. $\gamma \equiv \alpha \parallel \beta$ 和 $(v, \tau, w) \in [\![\gamma]\!]$，则 $(v, \tau \downarrow \alpha, w_\alpha) \in [\![\alpha]\!]$，$(v, \tau \downarrow \beta, w_\beta) \in [\![\beta]\!]$，且 $w = w_\alpha \oplus w_\beta$。根据归纳假设，$v = w_\beta$ 在 $BV(\beta)^{\complement}$ 上。此外，根据第 2.2 节中 $\oplus$ 的定义，$w_\beta = w$ 在 $BV(\alpha)^{\complement}$ 上。因此，$v = w$ 在 $BV(\alpha)^{\complement} \cap BV(\beta)^{\complement} = (BV(\alpha) \cup BV(\beta))^{\complement} = BV(\alpha \parallel \beta)^{\complement}$ 上。□

定义 11（项的参数）。项 $e \in \mathrm{Trm}(V, \Omega)$ 的自由变量集合 $FV(e)$ 和访问通道集合 $CN(e)$ 归纳定义于图 11。

不出所料，根据定义 11，轨迹变量 $h$ 可能会访问所有通道 $\Omega$；而对 $C$ 进行投影后，访问通道会减少 $C$。通信项 $\langle \mathsf{ch}\ \theta_1, \theta_2 \rangle$ 不访问任何通道，因为 $\theta_1, \theta_2 \in \mathrm{FOL}_{\mathbb{R}}(V_{\mathbb{R}})$。

为了用于一致性性质，我们将轨迹上的投影扩展到状态，定义为：对于所有 $h \in V_{\mathcal{T}}$ 和 $C \subseteq \Omega$，$v \downarrow C = v$ on $V_{\mathbb{R}} \cup V_{\mathbb{N}}$ 以及 $(v \downarrow C)(h) = v(h) \downarrow C$。与轨迹的情况一样，我们通常用 $v \downarrow e$ 代替 $v \downarrow CN(e)$。

引理 5（项的一致性）。自由变量对 $FV(e)$ 和访问通道 $CN(e)$ 对项 $e \in \mathrm{Trm}(V, \Omega)$ 具有通信感知一致性性质。也就是说，如果 $v \downarrow e = \tilde{v} \downarrow e$ on $FV(e)$，那么 $[\![e]\!]v = [\![e]\!]\tilde{v}$。特别地，若 $v = \tilde{v}$ on $FV(e)$，则 $[\![e]\!]v = [\![e]\!]v$。

证明。不失一般性，我们通过从左到右应用公理 $e$，尽可能将投影向下推 $\epsilon\downarrow$、$\cdot\downarrow$ 和 $\downarrow\cap$、$\downarrow\in$ 和 $\downarrow\notin$（见图 15）。

$$
\begin{aligned}
FV(z) &= \{z\} \quad (z \in V) & CN(h) &= \Omega \quad (h \in V_{\mathcal{T}}) \\
FV(\kappa) &= \emptyset & CN(z) = CN(\kappa) &= \emptyset \quad (z \notin V_{\mathcal{T}}) \\
FV(e_1 \bowtie e_2) &= FV(e_1) \cup FV(e_2) & CN(e_1 \bowtie e_2) &= CN(e_1) \cup CN(e_2) \\
FV(f(te, ie)) &= FV(te) \cup FV(ie) & CN(f(te, ie)) &= CN(te) \cup CN(ie) \\
FV(|te|) &= FV(te) & CN(|te|) &= CN(te) \\
FV(\langle \mathrm{ch}, \theta_1, \theta_2 \rangle) &= FV(\theta_1) \cup FV(\theta_2) & CN(\langle \mathrm{ch}, \theta_1, \theta_2 \rangle) &= \emptyset \\
FV(te \downarrow C) &= FV(te) & CN(te \downarrow C) &= CN(te) \cap C
\end{aligned}
$$

图 11：项 $e \in \mathsf{Trm}(V, \Omega)$ 的自由变量 $FV(e)$ 和访问通道 $CN(e)$ 的归纳定义，其中 $z \in V$, $\kappa$ 是任意类型的常量，$\bowtie \in \{+, \cdot\}$ 是任意算子，而 $f(te, ie) \in \{\mathsf{chan}(te[ie]), \mathsf{val}(te[ie]), \mathsf{time}(te[ie])\}$ 是 $te$ 和 $ie$ 上的项。

这是合理的，因为赋值 $[\![e]\!]$、自由变量 $FV(e)$ 和访问通道$CN(e)$ 在这些重写下保持不变。在得到的范式中，投影的作用域内只出现原始轨迹变量。关键的是，通信项 $\langle \mathsf{ch}\ \theta_1, \theta_2 \rangle$ 不包含其他轨迹变量，因为 $\theta_1, \theta_2 \in \mathsf{FOL}_{\mathbb{R}}(V_{\mathbb{R}})$。现在，对项 $e$ 的结构作归纳证明：

1. 若 $e \equiv z$ 满足 $z \in V$，则 $FV(e) = \{z\}$。若 $z \in V_{\mathbb{R}\cup\mathbb{N}} \cup \{\mu\}$，则由前提可得 $v(z) = \tilde{v}(z)$。若 $z \in V_{\mathcal{T}}$，则由于根据前提，$v(z) = v(z)\downarrow e = \tilde{v}(z) \downarrow e = \tilde{v}(z)$，而且 $CN(e) = \Omega$ 和 $v \downarrow e = \tilde{v} \downarrow e$ 在 $\{z\}$ 上，可得 $[\![e]\!]v = v(z) = \tilde{v}(z) = [\![e]\!]\tilde{v}$。2. 若 $e \equiv \kappa$，其中 $\kappa$ 是任意类型的常量，则 $[\![e]\!]v = \kappa = [\![e]\!]\tilde{v}$。3. 若 $e \equiv e_1 \bowtie e_2$ 满足 $\bowtie \in \{+, \cdot\}$，则由于 $FV(e_j) \subseteq FV(e)$，可得 $v \downarrow e = \tilde{v} \downarrow e$ 在 $FV(e_j)$ 上。对于 $h \in V_{\mathcal{T}}$，注意到 $v(h) \downarrow D = \tilde{v}(h) \downarrow D$ 蕴含 $v(h) \downarrow E = \tilde{v}(h) \downarrow E$，条件是 $E \subseteq D \subseteq \Omega$。因此，我们从$CN(e_j) \subseteq CN(e)$ 得到 $v \downarrow e_j = \tilde{v} \downarrow e_j$ 在 $FV(e_j)$ 上。根据归纳假设，我们得出如下结论：

$$[\![e]\!]v = [\![e_1]\!]v \bowtie [\![e_2]\!]v \overset{\text{IH}}{=} [\![e_1]\!]\tilde{v} \bowtie [\![e_2]\!]\tilde{v} = [\![e]\!]\tilde{v}$$

4. $e \in \{\mathsf{chan}(te[ie]), \mathsf{val}(te[ie]), \mathsf{time}(te[ie])\ \langle \mathsf{ch}\ \theta_1, \theta_2 \rangle, |te|\}$，然后根据归纳假设，我们可以像上一个情况那样得出结论。5. $e \equiv te \downarrow C$，那么对于某个 $h \in V_{\mathcal{T}}$，$te \equiv h$，因为根据假设，$e$ 处于范式。从 $CN(e) = C$ 和 $FV(e) = \{h\}$，我们根据前提得到 $v(h)\downarrow C = \tilde{v}(h)\downarrow C$，使得 $[\![e]\!]v = v(h) \downarrow C = \tilde{v}(h) \downarrow C = [\![e]\!]\tilde{v}$。□

我们调整了 $d\mathcal{L}$ [33] 中的必绑定变量，从而对公式和程序中的自由变量给出更精细的定义。将 $FV([\alpha]\psi)$ 定义为 $FV(\alpha) \cup FV(\psi)$，对于公式的一致性性质而言是可靠的，但不够精确，因为 $[x := 0]x \geq 0$ 不依赖于 $x$。然而，将 $FV([\alpha]\psi)$ 定义为 $FV(\alpha) \cup (FV(\psi) \setminus BV(\alpha))$ 则不可靠，因为 $[x := 0 \cup y := 0]x \geq 0$ 依赖于 $x$，而 $x$ 并未在所有执行路径上都受到约束。必绑定变量是指在程序的所有执行路径上都受到约束的变量。因此，在 $FV([\alpha]\psi) = FV(\alpha) \cup (FV(\psi) \setminus MBV(\alpha))$ 中，可以可靠地从 $FV(\psi)$ 中移除它们。

定义 12（必绑定变量）。程序 $\gamma \in \mathsf{CHP}(V, \Omega)$ 的必绑定变量集合 $MBV(\gamma)$ 在图 12 中以归纳方式定义。

$$\begin{aligned} MBV(\alpha) &= BV(\alpha) \quad (\alpha \text{ is any atomic program}) \\ MBV(\alpha \cup \beta) &= MBV(\alpha) \cap MBV(\beta) \\ MBV(\alpha;\beta) = MBV(\alpha \parallel \beta) &= MBV(\alpha) \cup MBV(\beta) \\ MBV(\alpha^*) &= \emptyset \end{aligned}$$

图 12：程序 $\gamma \in \mathsf{CHP}(V,\Omega)$ 的必绑定变量 $MBV(\gamma)$ 的归纳定义。

定义 13（程序的自由变量）。程序 $\gamma \in \mathsf{CHP}(V,\Omega)$ 的自由变量集合 $FV(\gamma)$ 在图 13 中归纳定义。

$$\begin{aligned} FV(x := \theta) &= FV(\theta) \\ FV(x := *) &= \emptyset \\ FV(?\chi) &= FV(\chi) \\ FV(\{x' = \theta \,\&\, \chi\}) &= \{x,\mu\} \cup FV(\theta) \cup FV(\chi) \\ FV(\mathrm{ch}(h)!\theta) &= \{h,\mu\} \cup FV(\theta) \\ FV(\mathrm{ch}(h)?x) &= \{h,\mu\} \\ FV(\alpha;\beta) &= FV(\alpha) \cup (FV(\beta) \setminus MBV(\alpha)) \\ FV(\alpha \cup \beta) = FV(\alpha \parallel \beta) &= FV(\alpha) \cup FV(\beta) \\ FV(\alpha^*) &= FV(\alpha) \end{aligned}$$

图 13：程序 $\gamma \in \mathsf{CHP}(V,\Omega)$ 的自由变量 $FV(\gamma)$ 的归纳定义。

定义 13 与通常情况相同，只是连续演化在其按照 $x$ 和常微分方程演化时，会静默地（不存在语法上的出现）依赖于全局时间 $\mu$。此外，$\mu$ 在 $\mathsf{ch}(h)!\theta$ 和 $\mathsf{ch}(h)?x$ 中是自由的，因为当前时间会被记录为每个通信事件的时间戳。

定义 14（公式的自由参数）。公式 $\phi \in \mathsf{Fml}(V,\Omega)$ 的自由变量集合 $FV(\phi)$ 和访问通道 $CN(\phi)$ 在图 14 中归纳定义。

引理 6（公式的重合性）。自由变量 $FV(\phi)$ 与访问通道 $CN(\phi)$ 的二元组对于公式 $\phi \in \mathsf{Fml}(V,\Omega)$ 具有通信感知一致性性质：如果 $v\downarrow\phi = \tilde{v}\downarrow\phi$ 在 $FV(\phi)$ 上，则：$v \in [\![\phi]\!]$ 当且仅当 $\tilde{v} \in [\![\phi]\!]$。

引理 7（程序的重合性）。对于程序 $\gamma \in \mathsf{CHP}(V,\Omega)$，自由变量集合 $FV(\gamma)$ 具有通信感知一致性性质：若$v\downarrow C = \tilde{v}\downarrow C$在 $X \supseteq FV(\gamma)$ 上满足 $C \subseteq \Omega$，且 $(v,\tau,w) \in [\![\gamma]\!]$，则存在 $(\tilde{v},\tilde{\tau},\tilde{w}) \in [\![\gamma]\!]$，使得 $w\downarrow C = \tilde{w}\downarrow C$在 $X \cup MBV(\gamma)$ 上成立，且 $\tau = \tilde{\tau}$，并且 $(w = \bot$当且仅当 $\tilde{w} = \bot)$。

证明（引理 6 和引理 7）。我们将 $d\mathcal{L}$ [33, 引理 17] 中关于一致性性质的证明推广到通信混合程序和包含原子通信模态的公式。证明采用对公式和程序结构的同步归纳法。

$FV(e_1 \sim e_2) = FV(e_1) \cup FV(e_2)$ $CN(e_1 \sim e_2) = CN(e_1) \cup CN(e_2)$$FV(\neg\varphi) = FV(\varphi)$ $CN(\neg\varphi) = CN(\varphi)$$FV(\varphi \rightleftharpoons \psi) = FV(\varphi) \cup FV(\psi)$ $CN(\varphi \rightleftharpoons \psi) = CN(\varphi) \cup CN(\psi)$$FV(\mathcal{Q}z.\,\varphi) = FV(\varphi) \setminus \{z\}$ $CN(\mathcal{Q}z.\,\varphi) = CN(\varphi)$$FV([\alpha]\psi) = FV(\alpha) \cup (FV(\psi) \setminus MBV(\alpha))$ $CN([\alpha]\psi) = CN(\psi)$$FV([\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi) = FV([\alpha]\psi) \cup FV(\mathsf{A}) \cup FV(\mathsf{C})$ $CN([\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi) = CN([\alpha]\psi) \cup CN(\mathsf{A}) \cup CN(\mathsf{C})$

图 14：公式 $\phi \in \mathsf{Fml}(V, \Omega)$ 的自由变量 $FV(\phi)$ 和访问通道 $CN(\phi)$ 的归纳定义，其中 $\sim \in \{=, \geq, \preceq\}$，且 $\rightleftharpoons \in \{\wedge, \vee, \rightarrow\}$，以及$\mathcal{Q} \in \{\forall, \exists\}$。

我们先对公式 $\phi$ 使用归纳法。根据前提， $v\downarrow\phi = \tilde{v}\downarrow\phi$ on $FV(\phi)$。然后证明 $v \in [\![\phi]\!]$ 蕴含 $\tilde{v} \in [\![\phi]\!]$。反过来，将 $v$ 和 $\tilde{v}$互换。对于任意公式 $\varphi$，我们认为 $\forall z\,\neg\varphi$ 在结构上小于 $\exists z\,\varphi$。注意，如果 $E \subseteq D \subseteq \Omega$，则$v\downarrow D = \tilde{v}\downarrow D$ 蕴含 $v\downarrow E = \tilde{v}\downarrow E$。在整个证明中，我们都会用到这一事实，不再另行说明。

1. $v \vDash e_1 \sim e_2$，其中 $\sim \in \{=, \geq, \preceq\}$，当且仅当 $[\![e_1]\!]v \sim [\![e_2]\!]v$ 成立。对于 $j = 1, 2$，$FV(e_j) \subseteq FV(e_1 \sim e_2)$ 且 $CN(e_j) \subseteq CN(e_1 \sim e_2)$，使得 $v\downarrow e_j = \tilde{v}\downarrow e_j$在$FV(e_j)$上。因此，根据项的一致性（引理 5），$[\![e_j]\!]v = [\![e_j]\!]\tilde{v}$ 对于 $j = 1, 2$ 成立，这意味着 $[\![e_1]\!]\tilde{v} \sim [\![e_2]\!]\tilde{v}$。于是， $\tilde{v} \vDash e_1 \sim e_2$。2. $v \vDash \neg\varphi$意味着 $v \notin [\![\varphi]\!]$。根据归纳假设，由于 $FV(\neg\varphi) = FV(\varphi)$ 且$CN(\neg\varphi) = CN(\varphi)$，所以 $\tilde{v} \notin [\![\varphi]\!]$。因此， $\tilde{v} \vDash \neg\varphi$。3. $v \vDash \varphi \wedge \psi$ 当且仅当 $v \vDash \varphi$ 且 $v \vDash \psi$。由于对于 $\chi \in \{\varphi, \psi\}$， $FV(\chi) \subseteq FV(\varphi \wedge \psi)$ 且 $CN(\chi) \subseteq$$CN(\varphi \wedge \psi)$，我们有 $v\downarrow\chi = \tilde{v}\downarrow\chi$ 在 $FV(\chi)$ 上。于是，根据归纳假设， $\tilde{v} \vDash \varphi$ 且$\tilde{v} \vDash \psi$。最后， $\tilde{v} \vDash \varphi \wedge \psi$。4. $\varphi \vee \psi$ 和 $\varphi \rightarrow \psi$ 这两种情况可用与 $\varphi \wedge \psi$类似的方法处理。5. $v \vDash \forall z\,\varphi$ 当且仅当对于所有 $a \in type(z)$， $v_z^a \vDash \varphi$。由于$v\downarrow\varphi = \tilde{v}\downarrow\varphi$ 在 $FV(\forall z\,\varphi) = FV(\varphi) \setminus \{z\}$ 上，且 $CN(\forall z\,\varphi) = CN(\varphi)$，因此 $v_z^a\downarrow\varphi = \tilde{v}_z^a\downarrow\varphi$ 在 $FV(\varphi)$上成立。因此，根据归纳假设，对于所有 $a \in type(z)$， $\tilde{v}_z^a \vDash \varphi$ 成立，这意味着 $\tilde{v} \vDash \forall z\,\varphi$。6. $v \vDash \exists z\,\varphi$ 当且仅当 $v \nvDash \forall z\,\neg\varphi$，由此根据归纳假设可得 $\tilde{v} \nvDash \forall z\,\neg\varphi$，因为 $FV(\forall z\,\neg\varphi) =$$FV(\exists z\,\varphi)$，且 $CN(\forall z\,\neg\varphi) = CN(\exists z\,\varphi)$，并且我们将 $\forall z\,\neg\varphi$ 视为在结构上小于 $\exists z\,\varphi$。因此， $\tilde{v} \vDash \exists z\,\varphi$。7. $\phi \equiv [\alpha]\psi$，然后令 $v \vDash \phi$。为证明 $\tilde{v} \vDash \phi$，令 $(\tilde{v}, \tilde{\tau}, \tilde{w}) \in [\![\alpha]\!]$，其中 $\tilde{w} \neq \bot$。由于$v\downarrow\phi = \tilde{v}\downarrow\phi$在 $FV(\phi) \supseteq FV(\alpha)$上，一个计算 $(v, \tau, w) \in [\![\alpha]\!]$ 满足 $w \neq \bot$，且 $w\downarrow\phi = \tilde{w}\downarrow\phi$ 在 $FV(\phi) \cup MBV(\alpha)$ 上，并且根据同步归纳假设， $\tau = \tilde{\tau}$存在。现在， $w\cdot\tau \vDash \psi$，因为 $v \vDash \phi$。根据 $FV(\phi) = FV(\alpha)\cup(FV(\psi)\setminus MBV(\alpha))$，我们得到 $w\downarrow\phi = \tilde{w}\downarrow\phi$在 $FV(\psi) \subseteq FV(\phi)\cup MBV(\alpha)$上成立，这意味着根据 $CN(\phi) = CN(\psi)$， $w\downarrow\psi = \tilde{w}\downarrow\psi$在 $FV(\psi)$上成立。此外，$(w\cdot\tau)\downarrow\psi = (\tilde{w}\cdot\tilde{\tau})\downarrow\psi$，因为 $\tau = \tilde{\tau}$。因此，可在 $w\cdot\tau \vDash \psi$ 上应用归纳假设，从而根据归纳假设， $\tilde{w}\cdot\tilde{\tau} \vDash \psi$ 成立。8. $\phi \equiv [\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi$，然后令 $v \vDash \phi$。为证明 $\tilde{v} \vDash \phi$，令 $(\tilde{v}, \tilde{\tau}, \tilde{w}) \in [\![\alpha]\!]$。由于 $v\downarrow\phi = \tilde{v}\downarrow\phi$在 $FV(\phi) \supseteq FV(\alpha)$上，一个计算 $(v, \tau, w) \in [\![\alpha]\!]$ 满足$w\downarrow\phi = \tilde{w}\downarrow\phi$在 $FV(\phi) \cup MBV(\alpha)$上，且 $\tau = \tilde{\tau}$，并且根据同步归纳假设，$(w = \bot$当且仅当 $\tilde{w} = \bot)$ 存在。

对于（提交），假设 $\{\tilde{v}\cdot\tau' \mid \tau' \prec \tilde{\tau}\} \vDash \mathsf{A}$。则根据归纳假设，$\{v\cdot\tau' \mid \tau' \prec \tau\} \vDash \mathsf{A}$，因为 $\tilde{\tau}=\tau$ 且 $v\downarrow\phi=\tilde{v}\downarrow\phi$ 在 $FV(\phi)$ 上意味着，根据 $FV(\mathsf{A}) \subseteq FV(\phi)$ 和 $CN(\mathsf{A}) \subseteq CN(\phi)$，$v\downarrow\mathsf{A}=\tilde{v}\downarrow\mathsf{A}$ 在 $FV(\mathsf{A})$ 上成立。因此，$v\cdot\tau \vDash \mathsf{C}$，因为 $v \vDash \phi$；这进而意味着根据归纳假设，$\tilde{v}\cdot\tilde{\tau} \vDash \mathsf{C}$，因为 $(v\cdot\tau)\downarrow\mathsf{C}=(\tilde{v}\cdot\tilde{\tau})\downarrow\mathsf{C}$ 在 $FV(\mathsf{C})$ 上成立。

对于（后置条件），假设 $\tilde{w}\neq\bot$ 和 $\{\tilde{v}\cdot\tau' \mid \tau' \preceq \tilde{\tau}\} \vDash \mathsf{A}$。由于 $v\downarrow\phi=\tilde{v}\downarrow\phi$ 在 $FV(\phi)$ 上有 $\supseteq FV(\mathsf{A})$，且 $CN(\phi) \supseteq CN(\mathsf{A})$，根据归纳假设可得 $\{v\cdot\tau' \mid \tau' \preceq \tau\} \vDash \mathsf{A}$。因此，根据 $v \vDash \phi$ 得出 $w\cdot\tau \vDash \psi$。此外，$w\downarrow\psi=\tilde{w}\downarrow\psi$ 在 $FV(\psi)$ 上成立，因为 $FV(\psi) \subseteq FV(\phi)\cup MBV(\alpha)$，且 $CN(\psi) \subseteq CN(\phi)$。最后，根据归纳假设可得 $\tilde{w}\cdot\tau \vDash \psi$。

现在，我们对程序 $\alpha$ 进行归纳。根据前提，$v\downarrow C=\tilde{v}\downarrow C$ 在 $X \supseteq FV(\gamma)$ 上成立。不失一般性，$X\cap V_{\mathcal{T}}=\emptyset$，因为根据有界效应性质（引理 4），$v=w$ 和 $\tilde{v}=\tilde{w}$ 都在 $(BV(\alpha)\backslash V_{\mathcal{T}})^{\complement}$ 上成立，使得 $\tilde{w}\downarrow C=\tilde{v}\downarrow C=v\downarrow C=w\downarrow C$ 在 $X\cap V_{\mathcal{T}}$ 上成立。因此，$v=v\downarrow C=\tilde{v}\downarrow C=\tilde{v}$ 在 $X$ 上成立。此外，对于所有程序 $\alpha$ 和所有 $n\in\mathbb{N}$，我们认为 $\alpha^n$ 在结构上小于 $\alpha^*$，并且 $x:=*;\mathsf{ch}(h)!x$ 小于 $\mathsf{ch}(h)?x$。

如果 $\gamma$ 是原子非通信程序，我们可以统一如下处理 $(v,\tau,w)\in[\![\gamma]\!]$与 $w=\bot$：令 $(v,\tau,\bot)\in[\![\gamma]\!]$。于是 $\tau=\epsilon$，并定义 $\tilde{\tau}=\epsilon$ 和 $\tilde{w}=\bot$。根据全性和前缀闭合性（命题 2），$(\tilde{v},\tilde{\tau},\tilde{w})\in[\![\gamma]\!]$。此外，$w=\tilde{w}$在 $X\cup MBV(\gamma)$ 上成立，因为 $\bot=\bot$对任意变量集都成立。因此，在下文前四种情形中，不失一般性，我们假设 $w\neq\bot$。

1. $(v,\tau,w)\in[\![x:=\theta]\!]$，则 $\tau=\epsilon$ 且 $w=v_x^{[\![\theta]\!]v}$。我们定义 $\tilde{\tau}=\epsilon$和 $\tilde{w}=\tilde{v}_x^{[\![\theta]\!]\tilde{v}}$，使得 $(\tilde{v},\tilde{\tau},\tilde{w})\in[\![x:=\theta]\!]$。根据一致性（引理 5），$w(x)=[\![\theta]\!]v=[\![\theta]\!]\tilde{v}=\tilde{w}(x)$，因为 $v=\tilde{v}$在 $X\supseteq FV(x:=\theta)=FV(\theta)$ 上成立。此外，$w=\tilde{w}$在 $X\setminus\{x\}$ 上成立，因为 $v=\tilde{v}$在 $X$上成立，并且 $v=w$和 $\tilde{v}=\tilde{w}$在 $\{x\}^{\complement}$上成立。因此，$w=\tilde{w}$在 $X\cup MBV(x:=\theta)$ 上成立，因为 $MBV(x:=\theta)=\{x\}$，且 $\tau=\tilde{\tau}$和 $\tilde{w}\neq\bot$。

2. $(v,\tau,w)\in[\![x:=*]\!]$，则对于某个 $a\in\mathbb{R}$，$\tau=\epsilon$且 $w=v_x^a$。我们定义$\tilde{\tau}=\epsilon$和 $\tilde{w}=\tilde{v}_x^a$。显然，在 $\{x\}^{\complement}$上，$v=w$且 $\tilde{v}=\tilde{w}$。因此，在 $X$上，$v=\tilde{v}$蕴含在 $X\setminus\{x\}$上 $w=\tilde{w}$。此外，$w(x)=v_x^a(x)=\tilde{v}_x^a(x)=\tilde{w}(x)$。总体而言，$(\tilde{v},\tilde{\tau},\tilde{w})\in[\![\alpha]\!]$存在，并且在 $X\cup MBV(x:=*)$上 $w=\tilde{w}$，因为 $MBV(x:=*)=\{x\}$。最后，$\tau=\tilde{\tau}$且 $\tilde{w}\neq\bot$。

3. $\gamma\equiv\{x'=\theta\,\&\,\chi\}$且 $(v,\tau,w)\in[\![\gamma]\!]$，则 $\tau=\epsilon$且存在一个解 $\varphi$：存在 $[0,s]\to\mathcal{S}$，满足 $v=\varphi(0)$，且 $w=\varphi(s)$，以及 $\varphi(\zeta)\vDash x'=\theta\wedge\chi$ 且 $\varphi(\zeta)(\mu)=v(\mu)+\zeta$对所有 $\zeta\in[0,s]$均成立，其中 $\varphi(\zeta)(x')=\frac{d\varphi(t)(x)}{dt}(\zeta)$，且 $\varphi(\zeta)(y)=v(y)$对于 $y\notin\{x,\mu\}$成立。我们定义一个解 $\tilde{\varphi}$：通过 $\tilde{\varphi}(\zeta)=\varphi(\zeta)$在 $\{x,\mu\}$上，并且若 $y\notin\{x,\mu\}$，则由 $\tilde{\varphi}(\zeta)(y)=\tilde{v}(y)$，定义一个持续时间相等的 $s$ for$\zeta\in[0,s]$的 $[0,s]\to\mathcal{S}$。

由于对于所有 $\zeta\in[0,s]$，$\varphi(\zeta)(x)=\tilde{\varphi}(\zeta)(x)$，因此我们有 $\varphi(\zeta)(x')=\tilde{\varphi}(\zeta)(x')$。此外，$\tilde{\varphi}(\zeta)=\varphi(\zeta)$在 $\{x,\mu\}$ 上，且 $\varphi(\zeta)=v=\tilde{v}=\tilde{\varphi}(\zeta)$在 $X\setminus\{x,\mu\}$上，这意味着 $\varphi(\zeta)=\tilde{\varphi}(\zeta)$在 $X\cup MBV(\gamma)$上，因为 $MBV(\gamma)=\{x,\mu\}$。由于根据前提，$X\supseteq FV(\gamma)\supseteq FV(\theta)\cup FV(\chi)$，因此根据项的一致性（引理 5），$[\![\theta]\!]\varphi(\zeta)=[\![\theta]\!]\tilde{\varphi}(\zeta)$。此外，根据同步归纳假设，$\varphi(\zeta)\vDash\chi$ 当且仅当 $\tilde{\varphi}(\zeta)\vDash\chi$。因此，对于所有 $\zeta\in[0,s]$，$\tilde{\varphi}(\zeta)\vDash x'=\theta\wedge\chi$。此外，根据 $\tilde{\varphi}$的定义，对于$y\notin\{x,\mu\}$，$\tilde{\varphi}(\zeta)(y)=\tilde{v}(y)$。若定义 $\tilde{v}=\tilde{\varphi}(0)$、$\tilde{\tau}=\epsilon$和 $\tilde{w}=\tilde{\varphi}(s)$，则 $(\tilde{v},\tilde{\tau},\tilde{w})\in[\![\alpha]\!]$。最后，$\tilde{w}=\tilde{\varphi}(s)=\varphi(s)=w$ 在 $X\cup MBV(\gamma)$ 上，且$\tau=\tilde{\tau}$和 $\tilde{w}\neq\bot$。

4. $(v,\tau,w) \in [\![?\chi]\!]$，则 $\tau=\epsilon$、 $w=v$和 $v\vDash\chi$。我们定义 $\tilde{\tau}=\epsilon$ 和 $\tilde{w}=\tilde{v}$。由于在 $X\supseteq FV(?\chi)$ 上， $v\vDash\chi$ 和 $v=\tilde{v}$ $=FV(\chi)$，因此根据同步归纳假设可得 $\tilde{v}\vDash\chi$。因此，$(\tilde{v},\tilde{\tau},\tilde{w}) \in [\![?\chi]\!]$。此外，在$X\cup MBV$上， $w=v=\tilde{v}=\tilde{w}$，因为 $MBV(?\chi)=\emptyset$。最后， $\tau=\tilde{\tau}$ 和 $\tilde{w}\neq\bot$。

5. $\gamma\equiv \mathsf{ch}(h)!\theta$ 且 $(v,\tau,w) \in [\![\gamma]\!]$，则 $(\tau,w) \preceq(\langle h,\mathsf{ch}\ [\![\theta]\!]v,v(\mu)\rangle,v)$。我们定义 $\tilde{\tau}=\tau$，并且当 $w=\bot$ 时为 $\tilde{w}=\bot$，否则为 $\tilde{w}=\tilde{v}$。由于 $v=\tilde{v}$在 $X\supseteq FV(\gamma)$ 上 $=\{h,\mu\}\cup FV(\theta)$，故有 $[\![\theta]\!]v=[\![\theta]\!]\tilde{v}$，且 $v(\mu)=\tilde{v}(\mu)$。因此，$(\tilde{\tau},\tilde{w}) \preceq(\langle h,\mathsf{ch}\ [\![\theta]\!]\tilde{v},\tilde{v}(\mu)\rangle,\tilde{v})$，这蕴含 $(\tilde{v},\tilde{\tau},\tilde{w}) \in [\![\gamma]\!]$。最后，若 $w\neq\bot$，则 $w=\tilde{w}$ 在 $X\cup MBV(\gamma)$ 上 $=X\cup\{h\}$，因为 $w=v=\tilde{v}=\tilde{w}$在 $X$ 上，且由于 $v=\tilde{v}$ 在 $X\subseteq FV(\gamma)$上 $\supseteq\{h\}$。此外， $\tau=\tilde{\tau}$，且 $(w=\bot$ 当且仅当$\tilde{w}=\bot)$。6. $(v,\tau,w) \in [\![\mathsf{ch}(h)?x]\!]$，则 $(v,\tau,w) \in [\![\alpha]\!]$，其中 $\alpha\equiv x:=*$；$\mathsf{ch}(h)!x$。由于 $FV(\mathsf{ch}(h)?x)=FV(\alpha)$，故 $v=\tilde{v}$ 在 $X\supseteq FV(\alpha)$ 上。于是，由归纳假设，存在 $(\tilde{v},\tilde{\tau},\tilde{w}) \in [\![\alpha]\!]$，使得 $\tau=\tilde{\tau}$，且 $w=\tilde{w}$ 在 $X\cup MBV()$ 上，并且 $(w=\bot$当且仅当 $\tilde{w}=\bot)$，因为我们认为 $\alpha$ 在结构上小于 $\mathsf{ch}(h)?x$。最后，$(\tilde{v},\tilde{\tau},\tilde{w}) \in [\![\mathsf{ch}(h)?x]\!]$，并注意到 $MBV(\mathsf{ch}(h)?x)=MBV(\alpha)$。7. $(v,\tau,w) \in [\![\alpha_1\cup\alpha_2]\!]$，则对某个 $j\in\{1,2\}$，有 $(v,\tau,w) \in [\![\alpha_j]\!]$。由于 $X\supseteq FV(\alpha_1\cup\alpha_2)\supseteq FV(\alpha_j)$，故 $v=\tilde{v}$ 在 $X\supseteq FV(\alpha_j)$ 上。因此，由归纳假设，存在 $(\tilde{v},\tilde{\tau},\tilde{w}) \in [\![\alpha_j]\!]\subseteq[\![\alpha_1\cup\alpha_2]\!]$，使得 $w=\tilde{w}$ 在 $X\cup MBV(\alpha_j)$ 上，且 $\tau=\tilde{\tau}$，并且 $(w=\bot$ 当且仅当 $\tilde{w}=\bot)$。最后， $w=\tilde{w}$ 在 $X\cup MBV(\alpha_1\cup\alpha_2)$ 上，因为$MBV(\alpha_1\cup\alpha_2)=MBV(\alpha_1)\cap MBV(\beta_2)$。8. $(v,\tau,w) \in [\![\alpha;\ \beta]\!]$，则 $(v,\tau,w) \in [\![\alpha]\!]_\bot$，或者 $(v,\tau,w) \in [\![\alpha]\!]\triangleright[\![\beta]\!]$。若 $(v,\tau,w) \in [\![\alpha]\!]_\bot\subseteq[\![\alpha]\!]$，则由归纳假设，存在计算 $(\tilde{v},\tilde{\tau},\tilde{w}) \in [\![\alpha]\!]$，使得 $\tau=\tilde{\tau}$ 且 $\tilde{w}=\bot$。由于 $w=\tilde{w}=\bot$，故有 $(\tilde{v},\tilde{\tau},\tilde{w}) \in [\![\alpha]\!]_\bot\subseteq[\![\alpha;\ \beta]\!]$，其中 $w=\tilde{w}$ 在 $X\cup MBV(\alpha;\ \beta)$ 上，且 $\tau=\tilde{\tau}$，并且 $(w'=\bot$当且仅当 $\tilde{w}=\bot)$。若 $(v,\tau,w) \in [\![\alpha]\!]\triangleright[\![\beta]\!]$，则存在计算 $(v,\tau_1,u) \in [\![\alpha]\!]$ 和 $(u,\tau_2,w) \in [\![\beta]\!]$，其中$\tau=\tau_1\cdot\tau_2$。由于 $X\supseteq FV(\alpha;\ \beta)\supseteq FV(\alpha)$，由归纳假设，存在 $(\tilde{v},\tilde{\tau}_1,\tilde{u}) \in [\![\alpha]\!]$，使得 $u=\tilde{u}$ 在 $X\cup MBV(\alpha)$ 上，且 $\tau_1=\tilde{\tau}_1$，并且 $\tilde{u}\neq\bot$，因为 $u\neq\bot$。注意， $X\cup MBV(\alpha)\supseteq FV(\alpha;\ \beta)\cup MBV(\alpha)=FV(\alpha)\cup(FV(\beta)\setminus MBV(\alpha))\cup MBV(\alpha)\supseteq FV(\beta)$。因此，再次由归纳假设，存在 $(\tilde{u},\tilde{\tau}_2,\tilde{w}) \in [\![\beta]\!]$，使得 $w=\tilde{w}$ 在 $X\cup MBV(\alpha)\cup MBV(\beta)=X\cup MBV(\alpha;\ \beta)$ 上，且 $\tau_2=\tilde{\tau}_2$，并且 $(w=\bot$当且仅当 $\tilde{w}=\bot)$。重新组装后得到 $(\tilde{v},\tilde{\tau},\tilde{w}) \in [\![\alpha]\!]\triangleright[\![\beta]\!]\subseteq[\![\alpha;\ \beta]\!]$，其中 $\tilde{\tau}=\tilde{\tau}_1\cdot\tilde{\tau}_2$。最后，$w=\tilde{w}$ 在 $X\cup MBV(\alpha;\ \beta)$ 上，且 $\tau=\tilde{\tau}$，并且 $(w=\bot$当且仅当 $\tilde{w}=\bot)$。9. $(v,\tau,w) \in [\![\alpha^*]\!]$，则对某个 $n\in\mathbb{N}$，有 $(v,\tau,w) \in [\![\alpha^n]\!]$。对 $n$进行归纳法，我们证明存在 $(\tilde{v},\tilde{\tau},\tilde{w}) \in [\![\alpha^n]\!]$，使得 $w=\tilde{w}$ 在 $X$ 上，且 $\tau=\tilde{\tau}$，并且 $(w=\bot$当且仅当 $\tilde{w}=\bot)$。最后，我们由 $[\![\alpha^n]\!]\subseteq[\![\alpha^*]\!]$ 和 $MBV(\alpha^*)=\emptyset$ 得出结论。(a) $n=0$: $(v,\tau,w) \in [\![\alpha^0]\!]=[\![?\mathrm{T}]\!],$ ，则 $\tau=\epsilon$，且 $w=\bot$ 或 $w=v$。我们定义 $\tilde{\tau}=\epsilon$，并且当 $w=\bot$ 时为 $\tilde{w}=\bot$，否则为 $\tilde{w}=\tilde{v}$。因此，$(\tilde{v},\tilde{\tau},\tilde{w}) \in [\![\alpha^0]\!]$，且 $w=\tilde{w}$ 在 $X$ 上，因为若 $w\neq\bot$，则 $v=\tilde{v}$ 在 $X$ 上蕴含 $w=v=\tilde{v}=\tilde{w}$ 在 $X$ 上。此外， $\tau=\tilde{\tau}$，且 $(w=\bot$ 当且仅当 $\tilde{w}=\bot)$。(b) $n>0$: $(v,\tau,w) \in [\![\alpha^n]\!]$，则 $(v,\tau,w) \in [\![\alpha;\ \alpha^{n-1}]\!]=[\![\alpha]\!]_\bot\cup([\![\alpha]\!]\triangleright[\![\alpha^{n-1}]\!])$。若 $(v,\tau,w) \in [\![\alpha]\!]_\bot\subseteq[\![\alpha]\!]$，则由归纳假设，存在 $(\tilde{v},\tilde{\tau},\tilde{w}) \in [\![\alpha]\!]$，使得 $\tau=\tilde{\tau}$ 且$\tilde{w}=\bot$。即，$(\tilde{v},\tilde{\tau},\tilde{w}) \in [\![\alpha]\!]_\bot\subseteq[\![\alpha^n]\!]$，其中 $w=\tilde{w}$ 在 $X$ 上，因为 $\bot=\bot$ 在任意变量集合上， $\tau=\tilde{\tau}$，并且 $(w=\bot$ 当且仅当 $\tilde{w}=\bot)$。若 $(v,\tau,w) \in [\![\alpha]\!]\triangleright[\![\alpha^{n-1}]\!]$，则存在计算 $(v,\tau_1,u) \in [\![\alpha]\!]$ 和 $(u,\tau_2,w) \in [\![\alpha^{n-1}]\!]$，其中 $\tau=\tau_1\cdot\tau_2$。由于 $X\supseteq FV(\alpha^*)=FV(\alpha)$，由归纳假设，

存在 $(\tilde{v},\tilde{\tau}_1,\tilde{u}) \in [\![\alpha]\!]$，使得 $u=\tilde{u}$ 在 $X$ 上，且 $\tau_1=\tilde{\tau}_1$，并且 $\tilde{u}\neq\bot$。由于 $X\supseteq FV(\alpha^*)=FV(\alpha^{n-1})$，且 $\alpha^{n-1}$ 在结构上小于 $\alpha^*$，再次由归纳假设，得到 $(\tilde{u},\tilde{\tau}_2,\tilde{w})\in[\![\alpha^{n-1}]\!]$，其中 $w=\tilde{w}$ 在 $X$ 上，且 $\tau_2=\tilde{\tau}_2$，并且 $(w=\bot$当且仅当 $\tilde{w}=\bot)$。重新组装后得到 $(\tilde{v},\tilde{\tau},\tilde{w})\in[\![\alpha]\!]\triangleright[\![\alpha^{n-1}]\!]\subseteq[\![\alpha^n]\!]$，其中$\tilde{\tau}=\tilde{\tau}_1\cdot\tilde{\tau}_2$。最后，$w=\tilde{w}$ 在 $X$ 上，且 $\tau=\tilde{\tau}$，并且 $(w=\bot$ 当且仅当 $\tilde{w}=\bot)$。

10. $(v,\tau,w)\in[\![\alpha_1\parallel\alpha_2]\!]$，则存在 $(v,\tau\downarrow\alpha_j,w_{\alpha_j})\in[\![\alpha]\!]$，使得对于 $j=1$，2 有 $w_{\alpha_1}(\mu)=w_{\alpha_2}(\mu)$，且 $\tau=\tau\downarrow(\alpha_1\parallel\alpha_2)$ 和 $w=w_{\alpha_1}\oplus w_{\alpha_2}$。由于 $X\supseteq FV(\alpha_1\parallel\alpha_2)\supseteq FV(\alpha_j)$，根据归纳假设，存在 $(\tilde{v},\tilde{\tau}_{\alpha_j},\tilde{w}_{\alpha_j})\in[\![\alpha_j]\!]$，其满足 $w_{\alpha_j}=\tilde{w}_{\alpha_j}$关于 $X\cup MBV(\alpha_j)$，且 $\tau\downarrow\alpha=\tilde{\tau}_{\alpha_j}$，并且 $(w_{\alpha_j}=\bot$ 当且仅当 $\tilde{w}_{\alpha_j}=\bot)$。我们定义$\tilde{\tau}=\tau$。因此，$\tilde{\tau}\downarrow\alpha_j=\tilde{\tau}_{\alpha_j}$，且 $\tilde{\tau}=\tilde{\tau}\downarrow(\alpha_1\parallel\alpha_2)$。此外，$\tilde{w}_{\alpha_1}(\mu)=\tilde{w}_{\alpha_2}(\mu)$，这可能是因为若 $\mu$ 未在两个程序中绑定，则根据引理 4，$\tilde{w}_{\alpha_1}=\tilde{v}=\tilde{w}_{\alpha_2}$ 关于 $\mu$；也可能是因为 $\mu\in X$，因为 $\mu\in BV(\alpha_1\parallel\alpha_2)$ 蕴含 $\mu\in FV(\alpha_1\parallel\alpha_2)$，且 $\tilde{w}_{\alpha_1}=w_{\alpha_1}=w_{\alpha_2}=\tilde{w}_{\alpha_2}$关于 $\mu$。总之，$(\tilde{v},\tilde{\tau},\tilde{w})\in[\![\alpha_1\parallel\alpha_2]\!]$，其中 $\tilde{w}=\tilde{w}_{\alpha_1}\oplus\tilde{w}_{\alpha_2}$，使得 $\tau=\tilde{\tau}$，并且 $(w=\bot$ 当且仅当 $\tilde{w}=\bot)$。

最后，我们证明 $w=\tilde{w}$ 在 $X\cup MBV(\alpha_1\parallel\alpha_2)$ 上。令 $z\in X\cup MBV(\alpha_1\parallel\alpha_2)=X\cup MBV(\alpha_1)\cup MBV(\alpha_2)$。若 $z\in BV(\alpha_1)$，则 $z\in X\cup MBV(\alpha_1)\cup\{\mu\}\cup V_{\mathcal{T}}$，因为 $V(\alpha_2)\cap BV(\alpha_1)\subseteq\{\mu\}\cup V_{\mathcal{T}}$(良构性)，且 $MBV(\alpha_2)\subseteq V(\alpha_2)$。此外，$BV(\alpha_1)\cap(\{\mu\}\cup V_{\mathcal{T}})\subseteq MBV(\alpha_1)$。现在，由于 $w_{\alpha_1}=\tilde{w}_{\alpha_1}$ 在 $X\cup MBV(\alpha)$ 上，且根据第 2.2 节中 $\oplus$ 的定义，$w=w_{\alpha_1}$在 $BV(\alpha_1)$ 上并且$\alpha\tilde{w}=\tilde{w}_{\alpha_1}$ 在 $BV(\alpha_1)$ 上，$\alpha_2$故 $w(z)=w_{\alpha_1}(z)=\tilde{w}_{\alpha_1}(z)=\tilde{w}_{\alpha_2}(z)$。若 $z\notin BV(\alpha_1)$ $\complement$ $\tilde{w}_{\alpha_2}$ $z=\tilde{w}$ $z$ $w=w_{\alpha_2}$ $BV$ $\alpha_1$ $\complement$ $\tilde{w}=\tilde{w}_{\alpha_2}$ $BV$ $\alpha_1$ $\complement$ )，则

$z\in X\cup MBV(\,)$。最后，由 $(\,)$ $(\,)$ $(\,)$ $(\,)$ 得出结论，因为根据 $\oplus$ 的定义，再次有在 $(\,)$ 上和在 $(\,)$ 上，且 $w_{\alpha_2}=\tilde{w}_{\alpha_2}$ 在 $X\cup MBV(\alpha_2)$ 上。□

## C 演算的细节

对轨迹项的推理基于简单的代数定律（见图 15）。根据项的语义（见定义 9），这些定律的可靠性显而易见。

$\cdot\downarrow(te_1\cdot te_2)\downarrow C=te_1\downarrow C\cdot te_2\downarrow C$ $\cdot$A $(te_1\cdot te_2)\cdot te_3=te_1\cdot(te_2\cdot te_3)\downarrow\in$ $\langle\mathsf{ch}\ \theta_1,\theta_2\rangle\downarrow C=\langle\mathsf{ch}\ \theta_1,\theta_2\rangle(\mathsf{ch}\ \in C)$ $\cdot$N $te\cdot\epsilon=te=\epsilon\cdot te\downarrow\cap(te\downarrow C')\downarrow C=te\downarrow(C'\cap C)$ $\epsilon\downarrow$ $\epsilon\downarrow C=\epsilon$值$_=$ $|te|=ie\to$值$((te\cdot te_0)[ie])=\theta_1$ $\downarrow\notin$ $\langle\mathsf{ch}\ \theta_1,\theta_2\rangle\downarrow C=\epsilon(\mathsf{ch}\ \notin C)$ 时间$_=$ $|te|=ie\to$时间$((te\cdot te_0)[ie])=\theta_2$ $|\cdot|\geq 0$ $|te|\geq 0$ chan$_=$ $|te|=ie\to\mathsf{chan}((te\cdot te_0)[ie])=\mathsf{ch}\,|\cdot|+1$ $|te\cdot te_0|=|te|+1$值$_>$ $|te|>ie\to$值$((te\cdot te_0)[ie])=$值$(te[ie])$ 时间$_>$ $|te|>ie\to$时间$((te\cdot te_0)[ie])=$时间$(te[ie])$ chan$_>$ $|te|>ie\to\mathsf{chan}((te\cdot te_0)[ie])=\mathsf{chan}(te[ie])$

图 15：迹代数 [42]，其中 $te_0\equiv\langle\mathsf{ch}\ \theta_1,\theta_2\rangle$。

为可靠性证明做准备（见定理 1），引理 8 表明，如果 $\alpha$ if $[\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi$ 良构，那么 A 和 C 不依赖于其状态。此外，引理 9 利用定义 7 表明，在并行组合 $[\alpha \,\|\beta]_{\{\mathsf{A},\mathsf{C}\}}\psi$ 中，程序 $\beta$ 若不干扰 $[\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi$，就不会影响 A 、 C 和 $\psi$ 的有效性。

引理 8。设 $[\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi$ 是良构的，并且 $(v、\ \tau、\ w) \in [\![\alpha]\!]$ 与 $w \neq \perp$。则在 $FV(\mathsf{A}) \cup FV(\mathsf{C})$ 上有 $v = w$。此外，当且仅当 $w \cdot \tilde{\tau} \vDash \chi$ 对于任意 $\tilde{\tau} \in \mathcal{T}_{rec}$ 以及 A、C } 时，$v \cdot \tilde{\tau} \vDash \chi$。

证明。根据有界效应性质（引理 4）， $v = w$ 在 $BV(\alpha)^{\complement} \cup V_{\mathcal{T}}$ 上。由于 $[\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi$ 是良构的，我们有 $(FV(\mathsf{A}) \cup FV(\mathsf{C})) \cap BV(\alpha) \subseteq V_{\mathcal{T}}$，这意味着 $v = w$ 在 $FV(\mathsf{A}) \cup FV(\mathsf{C})$ 上。根据一致性（引理 6）， $v \cdot \tilde{\tau} \vDash \chi$ 当且仅当 $w \cdot \tilde{\tau} \vDash \chi$。□

引理 9（非干扰防止失效）。设 $\beta \in \mathrm{CHP}(V, \Omega)$ 是一个程序，它不与 $[\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi$ （定义 7）发生干扰。此外，设 $(v, \tau, w) \in [\![\alpha \parallel \beta]\!]$，即，除此之外还有 $(v, \tau{\downarrow}\alpha, w_\alpha) \in [\![\alpha]\!]$ 以及 $(v, \tau{\downarrow}\beta, w_\beta) \in [\![\beta]\!]$with $w = w_\alpha \oplus w_\beta$。那么对于 $\chi \in \{\mathsf{A}, \mathsf{C}\}$，以下结论成立：

1. $v \cdot (\tau{\downarrow}\alpha) \vDash \chi$ 当且仅当 $v \cdot \tau \vDash \chi$2. $w \neq \perp$ 蕴含 $\big(w_\alpha \cdot (\tau{\downarrow}\alpha) \vDash \psi$ 当且仅当 $w \cdot \tau \vDash \psi\big)$

证明。首先，我们证明对于 $\lambda \in \{\mathsf{A}, \mathsf{C}\ \psi\}$，$(\tau{\downarrow}\alpha){\downarrow}\lambda = \tau{\downarrow}\lambda$，即 $\lambda$ 仅取决于 $\tau{\downarrow}\alpha$。若某个通信事件 $\rho \in \{\langle \mathsf{ch}\ a, s\rangle, \langle h, \mathsf{ch}\ a, s\rangle\}$ in$\tau$ 未被 $\downarrow\lambda$ 移除，那么它也不会被 $\downarrow\alpha$ 移除。设 $\rho{\downarrow}\lambda = \rho$。那么 $\mathsf{ch} \in CN(\lambda)$。若 $\mathsf{ch} \notin CN(\beta)$，则 $\mathsf{ch} \in CN(\alpha)$，因为 $\mathsf{ch} \in CN(\alpha) \cup CN(\beta)$，而 $\rho$由 $\alpha \parallel \beta$发出。否则，若 $\mathsf{ch} \in CN(\beta)$，则根据非干扰（定义 7），$\mathsf{ch} \in CN(\alpha)$。因此，$\mathsf{ch} \in CN(\alpha)$，使得 $\rho$ 不会被 $\downarrow\alpha$移除。

由于 $(\tau{\downarrow}\alpha){\downarrow}\chi = \tau{\downarrow}\chi$，我们有

$$\big(v \cdot (\tau{\downarrow}\alpha)\big){\downarrow}\chi = (v{\downarrow}\chi) \cdot \big((\tau{\downarrow}\alpha){\downarrow}\chi\big) = (v{\downarrow}\chi) \cdot (\tau{\downarrow}\chi) = (v \cdot \tau){\downarrow}\chi \qquad (5)$$

在 $V \supseteq FV(\chi)$ 上。现在，第1项由一致性（引理 6）得出。

对于第2项，假设 $w \neq \perp$。根据第 2.2 节中 $\oplus$的定义， $w_\alpha \neq \perp$ 且 $w_\beta \neq \perp$。首先，注意到根据 $\oplus$的定义， $w_\alpha = w$ 在 $BV(\alpha)$ 上成立，因此 $w_\alpha = w$ 在 $BV(\alpha) \cap BV(\beta)^{\complement}$ 上成立。其次，根据有界效应性质（引理 4）， $w_\alpha = v$ 在 $BV(\alpha)^{\complement} \cup V_{\mathcal{T}}$ 上成立；同样根据有界效应性质， $v = w_\beta$ 在 $BV(\beta)^{\complement} \cup V_{\mathcal{T}}$ 上成立；根据 $\oplus$的定义，$w_\beta = w$ 在 $BV(\alpha)^{\complement}$ 上成立。将上一句中的等式串联起来可得 $w_\alpha = w$ 在

$$(BV(\alpha)^{\complement} \cup V_{\mathcal{T}}) \cap (BV(\beta)^{\complement} \cup V_{\mathcal{T}}) \cap BV(\alpha)^{\complement} \supseteq BV(\alpha)^{\complement} \cap BV(\beta)^{\complement}.$$

第三， $w_\alpha = v = w_\beta$ 借助 $V_{\mathcal{T}}$ 的有界效应性质，使得 $w_\alpha = w_\alpha \oplus w_\beta = w$ 成立于 $V_{\mathcal{T}}$。总之，当 $w_\alpha$ 等于 $w$时，我们得到 $w_\alpha = w$ 成立于

$$(BV(\alpha) \cap BV(\beta)^{\complement}) \cup (BV(\alpha)^{\complement} \cap BV(\beta)^{\complement}) \cup V_{\mathcal{T}} = BV(\beta)^{\complement} \cup V_{\mathcal{T}}.$$

因此， $w_\alpha = w$在 $FV(\psi)$上成立，因为 $\beta$不会干扰 $[\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi$（定义 7），这意味着 $FV(\psi) \subseteq BV(\beta)^{\complement} \cup V_{\mathcal{T}}$。因此，$(w_\alpha \cdot (\tau{\downarrow}\alpha)){\downarrow}\chi = (w \cdot \tau){\downarrow}\chi$在$FV(\psi)$上成立，因为$(w_\alpha \cdot (\tau{\downarrow}\alpha)){\downarrow}\chi = (w_\alpha \cdot \tau){\downarrow}\chi$类似于方程（5）成立。最后，第2项根据一致性成立。□

命题 3. 并行算子 ||是结合的且可交换的。

证明（命题 3）。我们证明并行算子 $\parallel$ 是结合的且可交换的:

1. 令 $\alpha\beta$ 表示 $\alpha \parallel \beta$。现在，$(v,\tau,w) \in [\![\alpha \parallel \beta\gamma]\!]$ 当且仅当 $(v,\tau\downarrow\pi,w_\pi) \in [\![\pi]\!]$，对于$\pi \in \{\alpha,\beta\gamma\}$，且 $w_\alpha(\mu) = w_{\beta\gamma}(\mu)$，并且 $\tau\downarrow(\alpha \parallel \beta\gamma) = \tau$，以及 $w = w_\alpha \oplus w_{\beta\gamma}$。此外，$(v,\tau\downarrow\beta\gamma,w_{\beta\gamma}) \in [\![\beta\gamma]\!]$ 当且仅当 $(v,\tau\downarrow\pi,w_\pi) \in [\![\pi]\!]$，因为 $(\tau\downarrow\beta\gamma)\downarrow\pi = \tau\downarrow\pi$，对于 $\pi \in \{\beta,\gamma\}$，且 $(\tau\downarrow\beta\gamma)\downarrow\beta\gamma = \tau\downarrow\beta\gamma$，并且 $w_\beta(\mu) = w_\gamma(\mu)$，以及 $w_{\beta\gamma} = w_\beta \oplus w_\gamma$。同理，$(v,\tau,w) \in [\![\alpha\beta \parallel \gamma]\!]$ 当且仅当 $(v,\tau\downarrow\pi,w_\pi) \in [\![\pi]\!]$，对于 $\pi \in \{\alpha,\beta,\gamma\}$，且 $w_{\alpha\beta}(\mu) = w_\gamma(\mu)$，并且 $w_\alpha(\mu) = w_\beta(\mu)$，以及 $\tau\downarrow(\alpha\beta \parallel \gamma) = \tau$，且 $(\tau\downarrow\alpha\beta)\downarrow\alpha\beta = \tau\downarrow\alpha\beta$，并且 $w = w_{\alpha\beta} \oplus w_\gamma$，以及 $w_{\alpha\beta} = w_\alpha \oplus w_\beta$。这两种分解可以重新组合成对方的形式，因为对于任意 $C$，$\tau\downarrow C$都是按时间顺序的，正如 $\tau$ 也是按时间顺序的一样。此外，所有满足 $\pi \in \{\alpha,\beta,\gamma\}$ 的 $w_\pi(\mu)$ 都相等，因为 $w_{\beta\gamma}(\mu) = w_\beta(\mu)$，且 $w_{\alpha\beta}(\mu) = w_\alpha(\mu)$。最后，$w_\alpha \oplus (w_\beta \oplus w_\gamma) = (w_\alpha \oplus w_\beta) \oplus w_\gamma$：若对于某个 $\pi \in \{\alpha,\beta,\gamma\}$，有 $w_\pi = \bot$，则两边都等于 $\bot$。否则，若对于所有 $\pi \in \{\alpha,\beta,\gamma\}$，都有$w_\pi \neq \bot$，则等式成立，因为每个变量至多由 $\alpha$、$\beta$ 或 $\gamma$ 中的一个写入。2. 令 $(v,\tau,w) \in [\![\alpha \parallel \beta]\!]$。则 $(v,\tau\downarrow\alpha,w_\alpha) \in [\![\alpha]\!]$，且 $(v,\tau\downarrow\beta,w_\beta) \in [\![\beta]\!]$，并且 $\tau\downarrow(\alpha \parallel \beta) = \tau$，且 $w_\alpha(\mu) = w_\beta(\mu)$，以及 $w = w_\alpha \oplus w_\beta$。首先，由于 $CN(\alpha \parallel \beta) = CN(\alpha) \cup CN(\beta)$，因此 $\tau\downarrow(\alpha \parallel \beta) = \tau\downarrow(\beta \parallel \alpha)$。根据有界效应性质（引理 4），$w_\alpha \oplus w_\beta = v = w_\beta \oplus w_\alpha$作用于 $(BV(\alpha) \cup BV(\beta))^{\complement}$。此外，$w_\alpha \oplus w_\beta = w_\alpha = w_\beta \oplus w_\alpha$ 作用于 $BV(\alpha)$，因为 $BV(\alpha) \subseteq BV(\beta)^{\complement}$，这是因为 $\alpha$ 和$\beta$ 不共享状态。因此，$w_\alpha \oplus w_\beta = w_\beta \oplus w_\alpha$ 作用于 $BV(\beta)$，从而整体上 $w_\alpha \oplus w_\beta = w_\beta \oplus w_\alpha$。最后，$(v,\tau,w) \in [\![\beta \parallel \alpha]\!]$。□

证明（定理 1）。我们证明新颖的 ac-公理和规则的可靠性。由于$d\mathcal{L}_{\text{CHP}}$ 是 $d\mathcal{L}$ 的保守扩展（命题1），我们可以可靠地使用$d\mathcal{L}$ 证明演算来推理 $d\mathcal{L}_{\text{CHP}}$ 公式。因此，关于从 $d\mathcal{L}$ [30, 33, 34]中采用的公理和规则的可靠性，请参阅相关文献。

$[\epsilon]_{\text{AC}}$：令 $v \vDash [\alpha]_{\{\text{A,C}\}}\psi$。根据公理 W$[]_{\text{AC}}$，则 $v \vDash$ C。现在，令（$v$、$\tau$、$w$）$\in [\![\alpha]\!]$，并假设 $w \neq \bot$ 和 $v \vDash$A。则 $\tau = \epsilon$，因为 $CN(\alpha) = \emptyset$。因此，（post）的前置条件 $\{v\cdot\tau' \mid \tau' \preceq \tau\} \vDash$A得到满足，我们得出 $w \vDash \psi$。反过来，令 $v \vDash$ C $\wedge$（A $\rightarrow [\alpha]\psi$），且（$v$、$\tau$、$w$）$\in [\![\alpha]\!]$。条件（commit）成立，因为根据前置条件，$\tau = \epsilon$ 且 $v \vDash$C。对于（post），假设 $w \neq \bot$ 和$\{v\cdot\tau' \mid \tau' \preceq \tau\} \vDash$ A，其中包含 $v \vDash$ A。则 $v \vDash$ A $\rightarrow [\alpha]\psi$ 蕴含 $w \vDash \psi$。

W$[]_{\text{AC}}$：设 $v \vDash [\alpha]_{\{\text{A,C}\}}\psi$。则由（提交）可得 $v \vDash$ C，因为根据全性（命题 2），$(v,\epsilon,\bot) \in [\![\alpha]\!]$，且 $\{v\cdot\tau' \mid \tau' \prec \epsilon\} \vDash$A 显然成立，因为 $\{v\cdot\tau' \mid \tau' \prec \epsilon\} = \emptyset$。对于 $[\alpha]_{\{\text{A,C}\}}$(C $\wedge$ (A $\rightarrow \psi$))，（提交）由假设成立。对于（后置条件），设 $(v,\tau,w) \in [\![\alpha]\!]$，并假设 $w \neq \bot$且 $\{v\cdot\tau' \mid \tau' \preceq \tau\} \vDash$A。根据（提交），存在 $v\cdot\tau \vDash$ C，使得根据引理 8 有 $w\cdot\tau \vDash$ C。由（后置条件）可得 $w\cdot\tau \vDash \psi$，这蕴含 $w\cdot\tau \vDash$ A $\rightarrow \psi$。反方向可由规则 M$[\cdot]_{\text{AC}}$ 推出。

$[]_K$：设 $v \vDash \mathrm{Cl}_\forall K$，其中 $K \equiv (A \wedge C_1 \to A_2) \wedge (A \wedge C_2 \to A_1)$，且 $\mathrm{Cl}_\forall K$ 表示 K 的全称闭包。此外，设 $v \vDash \Phi$ 对于 $\Phi \equiv [\alpha]_{\{A_1 \wedge A_2, C_1 \wedge C_2\}}\psi$ 以及 $(v, \tau, w) \in [\![\alpha]\!]$。通过对 $\tau$ 的长度进行归纳法，我们同时证明 $v \vDash [\alpha]_{\{A, C_1 \wedge C_2\}}\psi$，且 $\{v \cdot \tau' \mid \tau' \prec \tau\} \vDash A$ 蕴含 $\{v \cdot \tau' \mid \tau' \prec \tau\} \vDash A_1 \wedge A_2$：

1. $|\tau| = 0$，那么 $v \vDash \Phi$ 蕴含 $v \vDash C_1 \wedge C_2$，由公理 W$[]_{AC}$ 得出。因此，(提交)成立，因为 $\tau = \epsilon$。对于（后置条件），假设 $w \neq \bot$ 和 $\{v \cdot \tau' \mid \tau' \preceq \tau\} \vDash A$。那么 $\{v \cdot \tau' \mid \tau' \preceq \tau\} \vDash A_1 \wedge A_2$，因为 $v \vDash C_1 \wedge C_2$ 成立，K 有效，并且 $\tau = \epsilon$。因此，根据假设，$w \cdot \tau \vDash \psi$。请注意，$\{v \cdot \tau' \mid \tau' \prec \tau\} \vDash A_1 \wedge A_2$ 显然满足，因为 $\{v \cdot \tau' \mid \tau' \prec \tau\} = \emptyset$。

2. $|\tau| > 0$，然后 $\tau = \tau_0 \cdot \rho$ 使用 $|\rho| = 1$。对于（commit），假设 $\{v \cdot \tau' \mid \tau' \prec \tau\} \vDash A$。于是 $\{v \cdot \tau' \mid \tau' \preceq \tau_0\} \vDash A$，这根据归纳假设意味着 $\{v \cdot \tau' \mid \tau' \prec \tau_0\} \vDash A_1 \wedge A_2$。由于（$v$、$\tau_0$、$\bot$）根据前缀闭合性（命题 2）$\in [\![\alpha]\!]$，我们通过 $v \vDash \Phi$ 得到 $v \cdot \tau_0 \vDash C_1 \wedge C_2$。因此，由于 K 有效且存在 $v \cdot \tau_0 \vDash A$ 使得 $\{v \cdot \tau' \mid \tau' \prec \tau\} \vDash A_1 \wedge A_2$，有 $v \cdot \tau_0 \vDash A_1 \wedge A_2$。最后，再次通过 $v \vDash \Phi$ 得到 $v \cdot \tau \vDash C_1 \wedge C_2$。对于（post），假设 $w \neq \bot$ 且 $\{v \cdot \tau' \mid \tau' \preceq \tau\} \vDash A$。于是 $\{v \cdot \tau' \mid \tau' \prec \tau\} \vDash A$，这如同（commit）情形一样意味着 $\{v \cdot \tau' \mid \tau' \prec \tau\} \vDash A_1 \wedge A_2$ 和 $v \cdot \tau \vDash C_1 \wedge C_2$。根据 K 的有效性以及 $v \cdot \tau \vDash A$，我们得到 $v \cdot \tau \vDash A_1 \wedge A_2$。总之，$\{v \cdot \tau' \mid \tau' \preceq \tau\} \vDash A_1 \wedge A_2$，，这通过 $v \vDash \Phi$ 意味着 $w \cdot \tau \vDash \psi$。

$[;\,]_{AC}$ 令 $v \vDash [\alpha;\ \beta]_{\{A,C\}}\psi$。为证明 $v \vDash [\alpha]_{\{A,C\}}[\beta]_{\{A,C\}}\psi$，令 $(v, \tau_1, u) \in [\![\alpha]\!]$。对于（提交），假设 $\{v \cdot \tau' \mid \tau' \prec \tau_1\} \vDash A$，并注意到 $(v, \tau_1, \bot) \in [\![\alpha]\!]_\bot \subseteq [\![\alpha;\ \beta]\!]$。于是根据假设可得 $v \cdot \tau_1 \vDash C$。对于（后置条件），假设 $u \neq \bot$ 且 $\{v \cdot \tau' \mid \tau' \preceq \tau_1\} \vDash A$。为证明 $u \cdot \tau_1 \vDash [\beta]_{\{A,C\}}\psi$，令 $(u, \tau_2, w) \in [\![\beta]\!]$。

1. 对于（提交），假设 $\{u \cdot \tau_1 \cdot \tau' \mid \tau' \prec \tau_2\} \vDash A$。根据引理 8，得出 $\{v \cdot \tau_1 \cdot \tau' \mid \tau' \prec \tau_2\} \vDash A$，由此根据假设 $\{v \cdot \tau' \mid \tau' \preceq \tau_1\} \vDash A$ 可推出 $\{v \cdot \tau' \mid \tau' \prec \tau_1 \cdot \tau_2\} \vDash A$。于是，因为 $(v, \tau_1 \cdot \tau_2, w) \in [\![\alpha]\!] \triangleright [\![\beta]\!] \subseteq [\![\alpha;\ \beta]\!]$，可得 $v \cdot \tau_1 \cdot \tau_2 \vDash C$。最后，再次使用引理 8，得到 $u \cdot \tau_1 \cdot \tau_2 \vDash C$。2. 对于（后置条件），假设 $w \neq \bot$ 且 $\{u \cdot \tau_1 \cdot \tau' \mid \tau' \preceq \tau_2\} \vDash A$。根据引理 8，得出 $\{v \cdot \tau' \mid \tau' \preceq \tau_1 \cdot \tau_2\} \vDash A$。由于 $(v, \tau_1 \cdot \tau_2, w) \in [\![\alpha;\ \beta]\!]$，根据假设可得 $w \cdot \tau_1 \cdot \tau_2 \vDash \psi$。

反过来，设 $v \vDash [\alpha]_{\{A,C\}}[\beta]_{\{A,C\}}\psi$ and $(v, \tau, w) \in [\![\alpha;\ \beta]\!]$。若 $(v, \tau, w) \in [\![\alpha]\!]_\bot$，则根据假设，提交成立。由于 $w = \bot$，后置条件显然成立。否则，若 $(v, \tau, w) \in [\![\alpha]\!] \triangleright [\![\beta]\!]$，则存在满足 $\tau = \tau_1 \cdot \tau_2$ 的计算 $(v, \tau_1, u) \in [\![\alpha]\!]$ and $(u, \tau_2, w) \in [\![\beta]\!]$。现在，我们得出如下结论：

1. 对于提交，设 $\{v \cdot \tau' \mid \tau' \prec \tau\} \vDash A$。若 $\tau_2 = \epsilon$，则根据假设，提交成立，因为 $(v, \tau, \bot) \in [\![\alpha]\!]_\bot$。若 $\tau_2 \neq \epsilon$，则 $\{v \cdot \tau' \mid \tau' \preceq \tau_1\} \vDash A$。因此，根据后置条件，$u \cdot \tau_1 \vDash [\beta]_{\{A,C\}}\psi$。由引理 8，$\{u \cdot \tau' \mid \tau' \prec \tau_1 \cdot \tau_2\} \vDash A$，这意味着 $\{u \cdot \tau_1 \cdot \tau' \mid \tau' \prec \tau_2\} \vDash A$。根据 $u \cdot \tau_1 \vDash [\beta]_{\{A,C\}}\psi$ 和 $(u, \tau_2, w) \in [\![\beta]\!]$，我们得到 $u \cdot \tau_1 \cdot \tau_2 \vDash C$。再次使用引理 8，$v \cdot \tau_1 \cdot \tau_2 \vDash C$。

2. 对于后置条件，假设 $\{v \cdot \tau' \mid \tau' \preceq \tau\} \vDash A$ 和 $w \neq \bot$。那么 $u \cdot \tau_1 \vDash [\beta]_{\{A,C\}}\psi$ 如上所述。最后，$w \cdot \tau \vDash \psi$ 因为根据引理 8，$\{u \cdot \tau_1 \cdot \tau' \mid \tau' \preceq \tau_2\} \vDash A$。

$[\cup]_{AC}$：该公理可直接由选择的语义 $[\![\alpha \cup \beta]\!] = [\![\alpha]\!] \cup [\![\beta]\!]$ 得出。

$[*]_{\mathbf{AC}}$ 由于 $[\![\alpha^*]\!] = \bigcup_{n\in\mathbb{N}}[\![\alpha^n]\!]$，公式 $[\alpha^*]_{\{\mathsf{A},\mathsf{C}\}}\psi \leftrightarrow [\alpha^0]_{\{\mathsf{A},\mathsf{C}\}}\psi \wedge [\alpha;\ \alpha^*]_{\{\mathsf{A},\mathsf{C}\}}\psi$是有效的。公理 $[*]_{\mathbf{AC}}$ 可由公式根据公理 $[;\ ]_{\mathbf{AC}}$得出。

$\mathrm{I}_{\mathbf{AC}}$：令 $v \vDash [\alpha^*]_{\{\mathsf{A},\mathsf{C}\}}\psi$。那么 $v \vDash [\alpha^0]_{\{\mathsf{A},\mathsf{C}\}}\psi \wedge [\alpha;\ \alpha^*]_{\{\mathsf{A},\mathsf{C}\}}\psi$ 由公理 $[*]_{\mathbf{AC}}$ 和$[;\ ]_{\mathbf{AC}}$。由于 $[\![\alpha;\ \alpha^*]\!] = [\![\alpha^*;\ \alpha]\!]$ 由归纳法和引理 3，$v \vDash [\alpha^*]_{\{\mathsf{A},\mathsf{C}\}}[\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi$由公理 $[;\ ]_{\mathbf{AC}}$。最后，$v \vDash [\alpha^*]_{\{\mathsf{A},\mathsf{T}\}}(\psi \to [\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi)$ 由规则 $\mathrm{M}[\cdot]_{\mathbf{AC}}$。

反过来，令 $v \vDash [\alpha^0]_{\{\mathsf{A},\mathsf{C}\}}\psi \wedge [\alpha^*]_{\{\mathsf{A},\mathsf{T}\}}(\psi \to [\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi)$ 且 $(v,\tau,w) \in [\![\alpha^*]\!]$。由于 $(v,\tau,w) \in [\![\alpha^n]\!]$ 对某个 $n \in \mathbb{N}$ 成立，我们对 $n$ 进行归纳：1. $n = 0$，则 (commit) 由 $v \vDash [\alpha^0]_{\{\mathsf{A},\mathsf{C}\}}\psi$ 和公理 $\mathrm{W}[]_{\mathbf{AC}}$ 成立，因为$\tau = \epsilon$。对于 (post)，还需假设 $w \neq \bot$，并注意到 $v = w$，因为存在 $\alpha^0 \equiv ?\mathsf{T}$ 使得 $w \vDash \psi$。2. $n > 0$，则 $(v,\tau,w) \in [\![\alpha^n]\!] = [\![\alpha;\ \alpha^{n-1}]\!]$，根据引理 3，它等于$[\![\alpha^{n-1};\alpha]\!] = [\![\alpha^{n-1}]\!]_\bot \cup [\![\alpha^{n-1}]\!] \triangleright [\![\alpha]\!]$。在 $[\![\alpha^{n-1}]\!]_\bot \subseteq [\![\alpha^{n-1}]\!]$的情况下，(commit) 和 (post) 由归纳假设成立。否则，若 $(v,\tau,w) \in [\![\alpha^{n-1}]\!] \triangleright [\![\alpha]\!]$，则存在计算 $(v,\tau_1,u) \in [\![\alpha^{n-1}]\!]$ 和 $(u,\tau_2,w) \in [\![\alpha]\!]$，满足 $\tau = \tau_1 \cdot \tau_2$。(a) 若 $\tau_2 = \epsilon$，则 (commit) 由归纳假设成立，因为 $(v,\tau,\bot) \in [\![\alpha^{n-1}]\!]$。若 $\tau_2 \neq \epsilon$，假设 $\{v\cdot\tau' \mid \tau' \prec \tau\} \vDash \mathsf{A}$，这意味着 $\{v\cdot\tau' \mid \tau' \preceq \tau_1\} \vDash \mathsf{A}$。因此，根据假设有 $u \cdot \tau_1 \vDash \psi \to [\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi$。由于根据归纳假设和 (post) 有 $u \cdot \tau_1 \vDash \psi$，我们得到 $u \cdot \tau_1 \vDash [\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi$。根据引理 8 和假设$\{v\cdot\tau' \mid \tau' \prec \tau\} \vDash \mathsf{A}$，我们得到 $\{u\cdot\tau_1\cdot\tau' \mid \tau' \prec \tau_2\} \vDash \mathsf{A}$。因此，$u\cdot\tau_1\cdot\tau_2 \vDash \mathsf{C}$；根据引理 8，这意味着 $v\cdot\tau \vDash \mathsf{C}$。(b) 对于 (post)，令 $w \neq \bot$ 且 $\{v\cdot\tau' \mid \tau' \preceq \tau\} \vDash \mathsf{A}$。则 $\{v\cdot\tau' \mid \tau' \preceq \tau_1\} \vDash \mathsf{A}$ 且 $\{v\cdot\tau_1\cdot\tau' \mid \tau' \preceq \tau_2\} \vDash \mathsf{A}$。与 (commit) 的情况一样，我们得到$u\cdot\tau_1 \vDash [\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi$。现在，引理 8 表明存在 $\{u\cdot\tau_1\cdot\tau' \mid \tau' \preceq \tau_2\} \vDash \mathsf{A}$，使得 $w\cdot\tau \vDash \psi$。

$[\mathrm{k}\_]_{\mathbf{AC}}$：令 $v \vDash [\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi$ and $(v,\tau,w) \in [\![\alpha \parallel \beta]\!]$。则 $(v,\tau\downarrow\alpha,w_\alpha) \in [\![\alpha]\!]$ with$w = w_\alpha \oplus w_\beta$ for some $w_\beta \in \mathcal{S}_\bot$。对于（提交），假设 $\{v\cdot\tau' \mid \tau' \prec \tau\} \vDash \mathsf{A}$。若$\tau'_\alpha \prec \tau\downarrow\alpha$，则存在 $\tau' \prec \tau$，使得 $\tau'_\alpha = \tau'\downarrow\alpha$。因此，根据前缀闭合性（命题 2），$(v,\tau',\bot) \in [\![\alpha \parallel \beta]\!]$and $(v,\tau'_\alpha,\bot) \in [\![\alpha]\!]$。于是，由引理 9 可得 $\{v\cdot\tau' \mid \tau' \prec \tau\downarrow\alpha\} \vDash \mathsf{A}$，因为 $\beta$ 不会与 $[\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi$发生干扰。因此，根据 $v \vDash [\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi$，$v\cdot(\tau\downarrow\alpha) \vDash \mathsf{C}$。现在，我们再次利用引理 9 得到 $v\cdot\tau \vDash \mathsf{C}$。对于（后置条件），假设 $w \neq \bot$and $\{v\cdot\tau' \mid \tau' \preceq \tau\} \vDash \mathsf{A}$。根据第 2.2 节中 $\oplus$ 的定义，有 $w_\alpha \neq \bot$；并且如上所述，由引理 9 可得 $\{v\cdot\tau' \mid \tau' \preceq \tau\downarrow\alpha\} \vDash \mathsf{A}$。因此，根据 $v \vDash [\alpha]_{\{\mathsf{A},\mathsf{C}\}}\psi$，$w_\alpha\cdot(\tau\downarrow\alpha) \vDash \psi$。最后，由引理 9 可得 $w\cdot\tau \vDash \psi$。

$[]_{\top,\ \top}$：令 $v \vDash [\alpha]\psi$ 且 $(v,\tau,w) \in [\![\alpha]\!]$。那么 (提交) 显然成立。对于 (后置条件)，假设 $w \neq \bot$ 且 $\{v\cdot\tau' \mid \tau' \preceq \tau\} \vDash \mathsf{T}$。那么根据假设，$w\cdot\tau \vDash \psi$。反过来，令 $v \vDash [\alpha]_{\{\mathsf{T},\mathsf{T}\}}\psi$ 且 $(v,\tau,w) \in [\![\alpha]\!]$，其中 $w \neq \bot$。那么，由于 $\{v\cdot\tau' \mid \tau' \preceq \tau\} \vDash \mathsf{T}$ 显然成立，根据 (后置条件)，$w\cdot\tau \vDash \psi$ 成立。

$[]_{\mathbf{AC}}\wedge$：蕴含式 $[\alpha]_{\{\mathsf{A},\mathsf{C}_1\}}\psi_1 \wedge [\alpha]_{\{\mathsf{A},\mathsf{C}_2\}}\psi_2 \to [\alpha]_{\{\mathsf{A},\mathsf{C}_1\wedge\mathsf{C}_2\}}(\psi_1 \wedge \psi_2)$ 可由语义轻松证明。反向蕴含可由规则$\mathrm{M}[\cdot]_{\mathbf{AC}}$。

$[\mathrm{ch!}]_{\mathbf{AC}}$: 令 $v \vDash [\mathrm{ch}(h)!\theta]_{\{\mathsf{A},\mathsf{C}\}}\psi$。则 $v \vDash \mathsf{C}$ 由 $\mathrm{W}[]_{\mathbf{AC}}$ 得出。现在，假设 $v \vDash \mathsf{A}$，并令 $(v,\tau,w) \in [\![\mathrm{ch}(h)!\theta]\!]$ 满足 $w \neq \bot$。由于 $v \vDash \mathsf{A}$ 且 $|\tau| = 1$，我们有$\{v\cdot\tau' \mid \tau' \prec \tau\} \vDash \mathsf{A}$。因此，$v\cdot\tau \vDash \mathsf{C}$ 由（提交）得出，这意味着 $w\cdot\tau \vDash \mathsf{C}$ 由

引理 8。对于 A $\rightarrow\psi$，假设 $w\cdot\tau\vDash$A。则 $v\cdot\tau\vDash$A 由引理 8 得出，使得 $\{v\cdot\tau'\mid\tau'\preceq\tau\}\vDash$A。因此， $w\cdot\tau\vDash\psi$由（后置条件）得出。
反之，设 $v\vDash\Phi([\mathsf{ch}(h)!\theta]\Phi(\psi))$，其中 $\Phi(\phi)\equiv\mathsf{C}\wedge(\mathsf{A}\rightarrow\phi)$，且 $(v,\tau,w)\in[\![\mathsf{ch}(h)!\theta]\!]$。对于（提交），假设 $\{v\cdot\tau'\mid\tau'\prec\tau\}\vDash$A。若 $\tau=\epsilon$，则根据假设可得到$v\vDash\mathsf{C}$。若 $\tau\neq\epsilon$，则存在 $v\vDash\mathsf{A}$，使得 $v\vDash[\mathsf{ch}(h)!\theta]\Phi(\psi)$。不失一般性地， $w\neq\bot$，因为从任意 $v$出发，$\mathsf{ch}(h)!\theta$ 都有一个终止计算。因此，存在 $w\cdot\tau\vDash\Phi(\psi)$，使得 $w\cdot\tau\vDash\mathsf{C}$。根据引理 8，可得到 $v\cdot\tau\vDash\mathsf{C}$。对于（后置条件），假设 $w\neq\bot$且 $\{v\cdot\tau'\mid\tau'\preceq\tau\}\vDash$A。如上所述，存在 $w\cdot\tau\vDash\Phi(\psi)$，使得 $w\cdot\tau\vDash\mathsf{A}\rightarrow\psi$。由于根据假设有 $v\cdot\tau\vDash\mathsf{A}$，根据引理 8，这意味着 $w\cdot\tau\vDash\mathsf{A}$，因此可得到 $w\cdot\tau\vDash\psi$。

[ch!]: 设 $v\vDash\forall h_0\,(h_0=h\cdot\langle\mathsf{ch}\ \theta,\mu\rangle\rightarrow\psi(h_0))$ 且 $(v,\tau,w)\in[\![\mathsf{ch}(h)!\theta]\!]$ 满足 $w\neq\bot$。将 $\forall h_0$用 $\tau_0=[\![h\cdot\langle\mathsf{ch}\ \theta,\mu\rangle]\!]v$替换为 $u=v_{h_0}^{\tau_0}$后，我们有 $u\vDash h_0=h\cdot\langle\mathsf{ch}\ \theta,\mu\rangle$。因此， $u\vDash\psi(h_0)$。通过替换， $u_h^{[\![h_0]\!]u}\vDash\psi(h)$。由于 $h_0\notin FV(\theta)$，根据一致性（引理 6），我们有 $[\![h\cdot\langle\mathsf{ch}\ \theta,\mu\rangle]\!]u=[\![h\cdot\langle\mathsf{ch}\ \theta,\mu\rangle]\!]v$。此外， $[\![h_0]\!]u=[\![h\cdot\langle\mathsf{ch}\ \theta,\mu\rangle]\!]u$使得 $u_h^{[\![h\cdot\langle\mathsf{ch},\theta,\mu\rangle]\!]v}\vDash\psi(h)$，这根据一致性推出 $v_h^{[\![h\cdot\langle\mathsf{ch},\theta,\mu\rangle]\!]v}\vDash\psi(h)$，因为 $h_0\notin FV(\psi(h))$。现在，注意到 $\tau=\langle h,\mathsf{ch}\ [\![\theta]\!]v,v(\mu)\rangle$使得 $v\cdot\tau=v_h^{[\![h\cdot\langle\mathsf{ch},\theta,\mu\rangle]\!]v}$。最后， $w\cdot\tau\vDash\psi(h)$， 因为 $w=v$。
反过来，令 $v\vDash[\mathsf{ch}(h)!\theta]\psi(h)$。为证明量词，令 $\tau_0\in\mathcal{T}$并假设$v_{h_0}^{\tau_0}\vDash h_0=h\cdot\langle\mathsf{ch}\ \theta,\mu\rangle$。现在注意到 $\langle h\ [\![\theta]\!]v\ \mu\rangle=v\cdot\tau\vDash\psi\ h=v_h^{[\![h\cdot\langle\mathsf{ch},\theta,\mu\rangle]\!]v}\in[\![h\cdot,,)\in[\mathsf{ch}(h)!\theta]\!]$，其中 ,ch , ( ) 满足 ( )。由于 and $\langle\mathsf{ch}\ \theta,\mu\rangle]\!]v=[\![h_0]\!]v=\tau_0$，通过替换可得 $v_{h_0}^{\tau_0}\vDash\psi(h_0)$。

[ch?]$_{\mathsf{AC}}$: 首先，注意到 $[\![\mathsf{ch}(h)?x]\!]=[\![x:=*]\!]\triangleright[\![\mathsf{ch}(h)!x]\!]$。
现在，令 $v\vDash[\mathsf{ch}(h)?x]_{\{\mathsf{A},\mathsf{C}\}}\psi$，不失一般性地设 $(v,\epsilon,u)\in[\![x:=*]\!]$，其中 $u\neq\bot$。此外，令 $(u,\tau,w)\in[\![\mathsf{ch}(h)!x]\!]$。那么 $(v,\tau,w)\in[\![x:=*]\!]\triangleright[\![\mathsf{ch}(h)!x]\!]=[\![\mathsf{ch}(h)?x]\!]$。对于（提交），假设 $\{u\cdot\tau'\mid\tau'\prec\tau\}\vDash$A。由于 $[\mathsf{ch}(h)?x]_{\{\mathsf{A},\mathsf{C}\}}\psi$ 是良构的，我们有 $(FV(\mathsf{A})\cup FV(\mathsf{C}))\cap BV(\mathsf{ch}(h)?x)\subseteq V_{\mathcal{T}}$。由于 $x\in BV(\mathsf{ch}(h)?x)$ 且 $BV(x:=*)=\{x\}$，我们有 $v=u$ 关于 $FV(\mathsf{A})\cup FV(\mathsf{C})$。根据一致性（引理 6），可得 $\{v\cdot\tau'\mid\tau'\prec\tau\}\vDash$A，使得 $v\cdot\tau\vDash\mathsf{C}$ 由前提成立，这蕴含着 $u\cdot\tau\vDash\mathsf{C}$，再次根据一致性可得。对于（后置条件），假设$w\neq\bot$且 $\{u\cdot\tau'\mid\tau'\preceq\tau\}\vDash$A。那么如上所述， $\{v\cdot\tau'\mid\tau'\preceq\tau\}\vDash$A。根据前提， $w\cdot\tau\vDash\psi$。
反之，设 $v\vDash[x:=*][\mathsf{ch}(h)!x]_{\{\mathsf{A},\mathsf{C}\}}\psi$ 且 $(v,\tau,w)\in[\![\mathsf{ch}(h)?x]\!]$。则 $(v,\epsilon,u)\in[\![x:=*]\!]$ 以及 $(u,\tau,w)\in[\![\mathsf{ch}(h)!x]\!]$ 存在。根据前提，我们得到$u\vDash\phi$，其中 $\phi\equiv[\mathsf{ch}(h)!x]_{\{\mathsf{A},\mathsf{C}\}}\psi$。现在，我们必须证明 $v\vDash[\mathsf{ch}(h)?x]_{\{\mathsf{A},\mathsf{C}\}}\psi$。因此，假设 $\{v\cdot\tau'\mid\tau'\prec\tau\}\vDash\mathsf{A}$ 对于（提交）。如同反向情况， $\{u\cdot\tau'\mid\tau'\prec\tau\}\vDash\mathsf{A}$ 使得 $u\cdot\tau\vDash\mathsf{C}$ 根据 $u\vDash\phi$，这再次蕴含 $v\cdot\tau\vDash\mathsf{C}$。对于（后置条件），假设 $w\neq\bot$ 和 $\{v\cdot\tau'\mid\tau'\preceq\tau\}$。最后， $w\cdot\tau\vDash\psi$ 根据 $u\vDash\phi$。

M[·]$_{\mathsf{AC}}$: 设 $v\vDash[\alpha]_{\{\mathsf{A}_1,\mathsf{C}_1\}}\psi$ 且 $(v,\tau,w)\in[\![\alpha]\!]$。对于（提交），假设 $\{v\cdot\tau'\mid\tau'\prec\tau\}\vDash\mathsf{A}_2$。那么 $\{v\cdot\tau'\mid\tau'\prec\tau\}\vDash\mathsf{A}_1$,，根据假设可推出 $v\cdot\tau\vDash\mathsf{C}_1$。最后，根据前提 $\mathsf{C}_1\rightarrow\mathsf{C}_2$，有 $v\cdot\tau\vDash\mathsf{C}_2$。对于（后置条件），假设 $w\neq\bot$且 $\{v\cdot\tau'\mid\tau'\preceq\tau\}\vDash\mathsf{A}_2$。那么根据前提 $\mathsf{A}_2\rightarrow\mathsf{A}_1$，有 $\{v\cdot\tau'\mid\tau'\preceq\tau\}\vDash\mathsf{A}_1$。因此，根据假设有 $w\cdot\tau\vDash\psi_1$。最后，根据前提 $\psi_1\rightarrow\psi_2$，有 $w\cdot\tau\vDash\psi_2$。

$G_{AC}$：前提 $C \wedge \psi$ 有效。为证明 $[\alpha]_{\{A,C\}}\psi$有效，令 $v$ 为任意状态，并令 $(v,\tau,w) \in [\![\alpha]\!]$。条件（提交）成立，因为根据 $v \cdot \tau \vDash C$的有效性，有 C。对于（后置条件），假设 $w \neq \bot$。那么 $w \cdot \tau \vDash \psi$，因为 $\psi$ 有效。

$[\mu]$：设 $ode \equiv \{x' = \theta \,\&\, \chi\}$。现在，$(v,\tau,w) \in [\![\{\mu' = 1, ode\}]\!]$ 当且仅当存在一个解$\varphi$：$[0,s] \to \mathcal{S}$从 $v$到 $w$，使得 $\varphi(\zeta) \vDash \mu' = 1 \wedge \mu' = 1 \wedge x' = \theta$并且 $v = \varphi(\zeta)$ 在 $\{x,\mu\}^{\complement}$ 上，对于 $\zeta \in [0,s]$ 当且仅当，因为 $\mu' = 1 \wedge \mu' = 1 \leftrightarrow \mu' = 1$对所有$\varphi(\zeta)$，我们有 $(v,\tau,w) \in [\![ode]\!]$。因此，$v \vDash [\{\mu' = 1, ode\}]\psi$当且仅当 $v \vDash [ode]\psi$。□

推论 1. 图 5 中的公理和规则可进行句法推导。此外，我们还推导出以下规则 不变式$_{AC}$ 为准备规则 归纳$_{AC}$:

$$\text{inv}_{AC}\ \frac{\mathrm{I} \vdash [\alpha]_{\{A,C\}}\psi}{\mathrm{I} \vdash [\alpha^*]_{\{A,C\}}\psi}$$

证明（推论 1）。我们通过在本演算中推导来证明这些公理和规则。关于规则 CG，见图 16；关于规则 $[\![\ ]\!]_{AC}$R，见图 17；关于规则 $\text{inv}_{AC}$，见图 18；关于规则 $\text{ind}_{AC}$，见图 19；关于规则 $[!\theta]_{AC}$R，见图 20。□

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{\vdash h \cdot te = h \cdot te,\ \Phi(h)}\quad \dfrac{*}{\Phi(h) \vdash \Phi(h)}\ \text{Id}}{h \cdot te = h \cdot te \to \Phi(h) \vdash \Phi(h)}\ {\to}\text{L}}{\forall h_0(h_0 = h \cdot te \to \Phi(h_0)) \vdash \Phi(h)}\ \forall\text{L}}{[\text{通道}(h)!\theta]\Phi(h) \vdash \Phi(h)}\ [\text{ch!}]}{\Gamma, [\text{ch}(h)!\theta]\Phi(h) \vdash \Phi(h),\ \Delta}\ \text{WL, WR} \qquad \dfrac{\dfrac{\dfrac{\Gamma, h_0 = h \cdot te \vdash \Phi(h_0),\ \Delta}{\Gamma \vdash h_0 = h \cdot te \to \Phi(h_0),\ \Delta}\ {\to}\text{R}}{\Gamma \vdash \forall h_0\,(h_0 = h \cdot te \to \Phi(h_0)),\ \Delta}\ \forall\text{R}}{\Gamma \vdash [\text{通道}(h)!\theta]\Phi(h),\ \Delta}\ [\text{ch!}] \qquad \dfrac{}{\Gamma \vdash [\text{通信}(h)!\ \theta]\Phi(h)\ \Phi(h),\ \Delta}\ \text{WR}}{\Gamma \vdash \Phi(h),\ \Delta}\ \text{Cut}$$

图 16：规则 CG 的推导。在证明中，$te$缩写为 $\langle \text{ch}\ \theta,\ \mu\rangle$ 且 $\Phi(h)$ 缩写为 $[\alpha(h)]\psi$。

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdash \mathsf{K}}{\vdash \mathrm{Cl}_\forall \mathsf{K}}\ \forall\text{R}}{\Gamma \vdash \mathrm{Cl}_\forall \mathsf{K}, \Delta}\ \text{WL, WR} \qquad \dfrac{\dfrac{\dfrac{\Gamma \vdash [\alpha_j]_{\{A_j,C_j\}}\psi_j, \Delta \quad (\text{for } j = 1,2)}{\Gamma \vdash [\alpha_1 \parallel \alpha_2]_{\{A_j,C_j\}}\psi_j, \Delta \quad (\text{for } j = 1,2)}\ [\![\_]\!]_{AC}}{\Gamma \vdash [\alpha_1 \parallel \alpha_2]_{\{A_1 \wedge A_2, C_j\}}\psi_j, \Delta \quad (\text{for } j = 1,2)}\ \text{M}[\cdot]_{AC}}{\Gamma \vdash [\alpha_1 \parallel \alpha_2]_{\{A_1 \wedge A_2, C_1 \wedge C_2\}}(\psi_1 \wedge \psi_2), \Delta}\ [\,]_{AC}\wedge}{\Gamma \vdash \mathrm{Cl}_\forall \mathsf{K} \wedge [\alpha_1 \parallel \alpha_2]_{\{A_1 \wedge A_2, C_1 \wedge C_2\}}(\psi_1 \wedge \psi_2), \Delta}\ \wedge\text{R}}{\Gamma \vdash [\alpha_1 \parallel \alpha_2]_{\{A, C_1 \wedge C_2\}}(\psi_1 \wedge \psi_2), \Delta}\ [\,]_{\mathsf{K}}$$

图 17：规则 $[\![\ ]\!]_{AC}$R 的推导。对于 $j = 1$、2，由 $\triangleleft$ 标记的开放前提 $A_1 \wedge A_2 \to A_j$显然成立。由于根据前提，$\alpha_{3-j}$ 不会干扰$[\alpha_j]_{\{A_j,C_j\}}\psi_j$，因此可以应用公理 $[\![\ ]\!]_{AC}$。

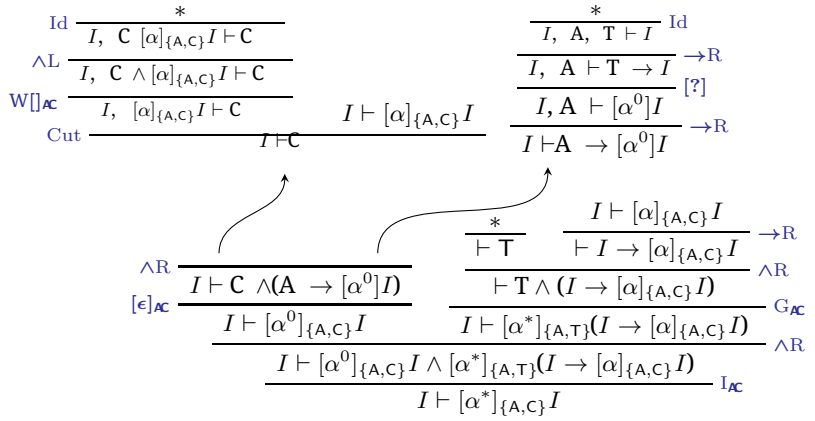

图 18：规则 $\text{inv}_{\text{AC}}$

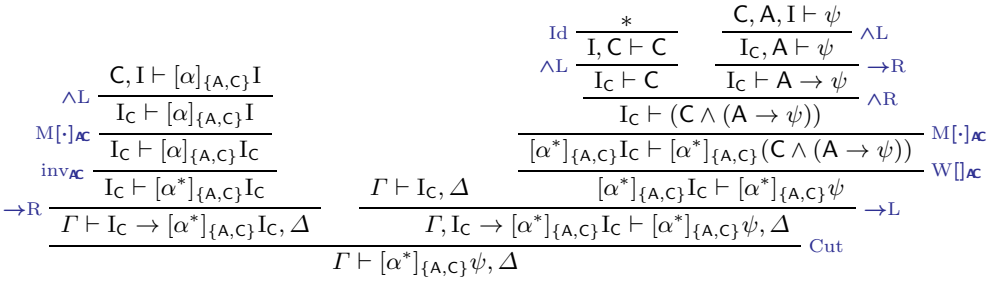

图 19：规则 $\text{ind}_{\text{AC}}$ 的推导。在证明中，我们默认多次应用弱化。公式 $\mathrm{I_C} \equiv \mathrm{I} \wedge \mathsf{C}$ 将不变式与承诺 C结合起来。此外，$\Psi$ 是 $\mathsf{C} \wedge (\mathsf{A} \to \psi)$ 的简写。

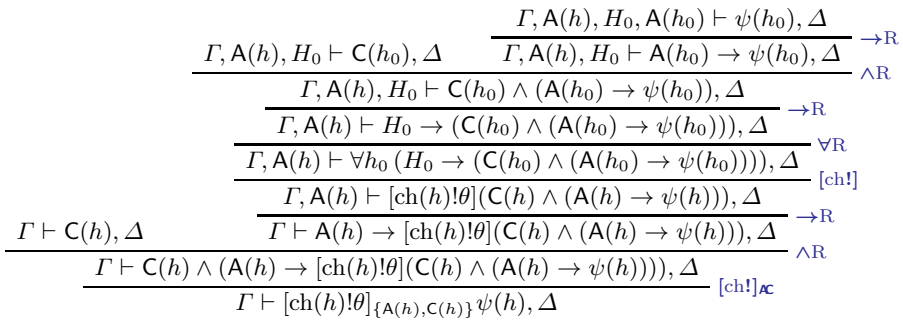

图 20：规则 $[!\theta]_{\text{AC}}\mathrm{R}$ 的推导。在证明中，$H_0$是 $h_0 = h \cdot \langle \mathrm{ch}\ \theta$ 的简写，$\mu\rangle$。

## D 示例的详细信息

我们继续第3节中示例的证明，并给出其余推导：

$$\dfrac{\dfrac{\dfrac{

$$\dfrac{\dfrac{*}{\mathsf{C},\ \mathsf{L}\ \chi_{vel}(v_0) \vdash 0 \le v_0 \le V}\ \triangleright\mathbb{N}}{\mathsf{C},\ \mathsf{L}\ \chi_{vel}(v_0) \vdash 0 \le \text{值}(h_{\text{vel}} \cdot \langle \text{out}\ v_0, \mu\rangle) \le V}\ \text{val}_{=}}{\mathsf{C}, \mathsf{L}\ \chi_{vel}(v_0)\ h_{\text{vel}} = h \cdot \langle \text{输出}\ v_0, \mu\rangle \vdash 0 \le \text{值}(h_0) \le V}\ =\text{R}$$

Id

图 23：继续图 21 中的证明

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\mathsf{C},\ \mathsf{L}\ \chi_{vel}(v_0) \vdash [\text{plant}_l(v_0)]\mathsf{L}(v_0, x_l, w, \mu, h)}\ \triangleright\text{Id}}{\mathsf{C},\ \mathsf{L}\ \chi_{vel}(v_0) \vdash \mathsf{C} \wedge [\text{plant}_l(v_0)]\mathsf{L}(v_0,\ x_l,\ w,\ \mu,\ h)}\ \wedge\text{R}}{\mathsf{C}, \mathsf{L}\ \chi_{vel}(v_0) \vdash \mathsf{T} \rightarrow \mathsf{C} \wedge [\text{plant}_l(v_0)]\mathsf{L}(v_0, x_l, w, \mu, h)}\ \rightarrow\text{R, WL}}{\mathsf{C},\ \mathsf{L}\ \chi_{vel}(v_0) \vdash [\text{跳过}](\mathsf{C} \wedge [\text{plant}_l(v_0)]\mathsf{L}(v_0,\ x_l,\ w,\ \mu,\ h))}\ [?]}{\mathsf{C},\ \mathsf{L}\ \chi_{vel}(v_0) \vdash \mathsf{C} \wedge [\text{跳过}](\mathsf{C} \wedge [\text{plant}_l(v_0)]\mathsf{L}(v_0, x_l, w, \mu, h))}\ \triangleright\text{Id}}{\mathsf{C},\ \mathsf{L}\ \chi_{vel}(v_0) \vdash [\text{跳过}]_{\{\mathsf{T},\mathsf{C}\}}[\text{plant}_l(v_0)]\mathsf{L}(v_0, x_l, w, \mu, h)}\ [\epsilon]_{\text{AC}}$$

$\wedge$R

图 24：延续图 21 中的证明

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{\mathsf{L}\ t \ge 0, w + t \le \epsilon \vdash w + t = \Delta(\mu + t, h_{\text{pos}}) \le \epsilon \wedge v_l \ge 0 \wedge x_l + t \cdot v_l \le x_l}\ \triangleright\mathbb{N}}{\mathsf{L}\ w = 0, t \ge 0, \mathcal{E} \vdash \mathsf{L}(v_l, x_l + t \cdot v_l, w + t, \mu + t, h \cdot \langle \text{位置}\ x_l, \mu\rangle)}\ \text{val}_{=}}{\mathsf{L}\ H_{\text{pos}}, w = 0, t \ge 0, \mathcal{E} \vdash \mathsf{L}(v_l, x_l + t \cdot v_l, w + t, \mu + t, h_{\text{pos}})}\ =\text{R}}{\mathsf{L}\ H_{\text{pos}}, w = 0, t \ge 0 \vdash \mathcal{E} \rightarrow \mathsf{L}(v_l, x_l + t \cdot v_l, w + t, \mu + t, h_{\text{pos}})}\ \rightarrow\text{R}}{\mathsf{L}\ H_{\text{pos}}, w = 0 \vdash \forall t{\ge}0\,(\mathcal{E} \rightarrow \mathsf{L}(v_l,\ x_l + t \cdot v_l,\ w + t,\ \mu + t,\ h_{\text{pos}}))}\ \forall\text{R}}{\mathsf{L}\ H_{\text{pos}}, w = 0, \vdash [\{\mu' {=} 1, w' {=} 1, x_l' {=} v_l\ \&\ w \le 0\}]\mathsf{L}(v_l, x_l, w, \mu, h_{\text{pos}})}\ [']}{\mathsf{L}\ H_{\text{pos}}, w = 0 \vdash [\text{plant}_l]\mathsf{L}(v_l, x_l, w, \mu, h_{\text{pos}})}\ [\mu]}{\mathsf{C}, \mathsf{L}\ H_{\text{pos}} \vdash [w := 0][\text{plant}_l]\mathsf{L}(v_l,\ x_l,\ w,\ \mu,\ h_{\text{pos}})}\ \triangleright\text{Id}}{\mathsf{C},\ \mathsf{L} \vdash [\text{pos}(h)!x_l]_{\{\mathsf{T},\mathsf{C}\}}[w := 0][\text{plant}_l]\mathsf{L}(v_l,\ x_l,\ w,\ \mu,\ h_{\text{pos}})}\ [:=], \text{WL}}{\mathsf{C},\ \mathsf{L} \vdash [\text{pos}(h)!x_l]_{\{\mathsf{T},\mathsf{C}\}}[w := 0]_{\{\mathsf{T},\mathsf{C}\}}[\text{plant}_l]\mathsf{L}(v_l,\ x_l,\ w,\ \mu,\ h_{\text{pos}})}\ [!\theta]_{\text{AC}}\text{R}}{\mathsf{C},\ \mathsf{L} \vdash [\text{updt}(h)]_{\{\mathsf{T},\mathsf{C}\}}[\text{plant}_l]\mathsf{L}(v_l,\ x_l,\ w,\ \mu,\ h_{\text{pos}})}\ [\epsilon]_{\text{AC}},\ \text{W}[]_{\text{AC}}\ [;\ ]_{\text{AC}}$$

$\mathbb{R}$

图 25：接续图 21 中的证明。我们将 $h_{\text{pos}} = h \cdot \langle \text{pos}\ x_l, \mu\rangle$˜ ˜简记为 $H_{\text{pos}}$。因此， $\mathcal{E}$是 $\forall 0 \le t \le t\, w + t \le \epsilon$的简写。

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{\mathsf{F}\ d \le \epsilon V, t \ge 0 \vdash \mathsf{F}(x_f + t \cdot v_f, \mu + t)}\ \triangleright}{\mathsf{F}、\ \mathsf{A}\ H_{\text{vel}}、\ \mathsf{A}(h_0)\ d \le \epsilon V、\ t \ge 0 \vdash \mathsf{F}(x_f + t \cdot v_f,\ \mu + t)}\ \text{WL}}{\mathsf{F},\ \mathsf{A}\ H_{\text{vel}},\ \mathsf{A}(h_0)\ d \le \epsilon V \vdash \forall t{\ge}0\,\mathsf{F}(x_f + t \cdot v_f,\ \mu + t)}\ \forall\text{R}}{\mathsf{F},\ \mathsf{A}\ H_{\text{vel}},\ \mathsf{A}(h_0)\ d \le \epsilon V \vdash [\{\mu' {=} 1, x_f' {=} v_f\}]\mathsf{F}(x_f,\ \mu)}\ [']}{\mathsf{F},\ \mathsf{A}\ H_{\text{vel}},\ \mathsf{A}(h_0)\ d \le \epsilon V \vdash [\{x_f' {=} v_f\}]\mathsf{F}(x_f,\ \mu)}\ [\mu]$$

$\mathbb{R}$

图 26：续接图 8 中的证明。公式 $H_{\text{vel}}$是 $h_0 = h_{\text{vel}}\ \langle$速度 $v_{tar}, \mu\rangle$的简写

$$
\dfrac{*}{\mathrm{F}\ d_0 = m - x_f, m - x_f \le \epsilon V, 0 \le v_0 < {}^{d_0}\!/_{\epsilon}, t \ge 0 \vdash 0 \le v_0 \le {}^{d_0}\!/_{\epsilon} \land v_0 \le V \land x_f + t \cdot v_0 + (\epsilon - (\mu + t - \mu)) {}^{d_0}\!/_{\epsilon} < m}\ \mathbb{R}
$$

$$
\dfrac{\mathrm{F}\ d_0 = m - x_f, m - x_f \le \epsilon V, 0 \le v_0 < {}^{d_0}\!/_{\epsilon}, t \ge 0 \vdash 0 \le v_0 \le {}^{d_0}\!/_{\epsilon} \land v_0 \le V \land x_f + t \cdot v_0 + (\epsilon - (\mu + t - \mu)) {}^{d_0}\!/_{\epsilon} < m}{\mathrm{F}\ d_0 = m - x_f, m - x_f \le \epsilon V, 0 \le v_0 < {}^{d_0}\!/_{\epsilon}, t \ge 0 \vdash 0 \le v_0 \le {}^{d_0}\!/_{\epsilon} \land v_0 \le V \land x_f + t \cdot v_0 + (\epsilon - \Delta(\mu + t, h \cdot \langle \text{位置}\ m, \mu \rangle)) {}^{d_0}\!/_{\epsilon} < m}\ \triangleright \mathbb{N}
$$

$$
\dfrac{\mathrm{F}\ d_0 = m - x_f, m - x_f \le \epsilon V, 0 \le v_0 < {}^{d_0}\!/_{\epsilon}, t \ge 0 \vdash 0 \le v_0 \le {}^{d_0}\!/_{\epsilon} \land v_0 \le V \land x_f + t \cdot v_0 + (\epsilon - (\mu + t - \mu)) {}^{d_0}\!/_{\epsilon} < m}{\mathrm{F}\ d_0 = m - x_f, m - x_f \le \epsilon V, 0 \le v_0 < {}^{d_0}\!/_{\epsilon}, t \ge 0 \vdash 0 \le v_0 \le {}^{d_0}\!/_{\epsilon} \land v_0 \le V \land x_f + t \cdot v_0 + (\epsilon - \Delta(\mu + t, h \cdot \langle \text{位置}\ m, \mu \rangle)) {}^{d_0}\!/_{\epsilon} < m}\ \triangleright \mathbb{N}
$$

$$
\dfrac{\mathrm{F}\ d_0 = m - x_f, m - x_f \le \epsilon V, 0 \le v_0 < {}^{d_0}\!/_{\epsilon}, t \ge 0 \vdash \mathrm{F}(v_0, x_f + t \cdot v_f, d_0, \mu + t, h \cdot \langle \text{位置}\ m, \mu \rangle)}{\mathrm{F}\ d_0 = m - x_f, m - x_f \le \epsilon V, 0 \le v_0 < {}^{d_0}\!/_{\epsilon}, t \ge 0 \vdash \mathrm{F}(v_0, x_f + t \cdot v_f, d_0, \mu + t, h \cdot \langle \text{位置}\ m, \mu \rangle)}\ \downarrow\in,\ \text{值}=
$$

$$
\dfrac{\Gamma_{\text{mes}}, 0 \le v_0 < {}^{d_0}\!/_{\epsilon}, t \ge 0 \vdash \mathrm{F}(v_f, x_f + t \cdot v_f, d_0, \mu + t, h_{\text{pos}})}{\Gamma_{\text{mes}}, 0 \le v_0 < {}^{d_0}\!/_{\epsilon} \vdash \forall t \ge 0\, \mathrm{F}(v_f, x_f + t \cdot v_f, d_0, \mu + t, h_{\text{pos}})}\ =\mathrm{R}
$$

$$
\dfrac{\Gamma_{\text{mes}}, 0 \le v_0 < {}^{d_0}\!/_{\epsilon} \vdash \mathrm{F}(v_f, x_f + t \cdot v_f, d_0, \mu + t, h_{\text{pos}})}{\Gamma_{\text{mes}}, 0 \le v_0 < {}^{d_0}\!/_{\epsilon} \vdash \forall t \ge 0\, \mathrm{F}(v_f, x_f + t \cdot v_f, d_0, \mu + t, h_{\text{pos}})}\ \forall \mathrm{R}
$$

$$
\dfrac{\Gamma_{\text{mes}}, 0 \le v_0 < {}^{d_0}\!/_{\epsilon} \vdash [\{\mu' = 1, x_f' = v_0\}] \mathrm{F}(v_f, x_f, d_0, \mu, h_{\text{pos}})}{\Gamma_{\text{mes}}, 0 \le v_0 < {}^{d_0}\!/_{\epsilon} \vdash [\{x_f' = v_0\}] \mathrm{F}(v_f, x_f, d_0, \mu, h_{\text{pos}})}\ [\mu]
$$

$$
\dfrac{\Gamma_{\text{mes}} \vdash [?0 \le v_0 < {}^{d_0}\!/_{\epsilon}][\mathsf{plant}_f(v_0)] \mathrm{F}(v_f, x_f, d_0, \mu, h_{\text{pos}})}{\Gamma_{\text{mes}}, 0 \le v_0 < {}^{d_0}\!/_{\epsilon} \vdash [\{\mu' = 1, x_f' = v_0\}] \mathrm{F}(v_f, x_f, d_0, \mu, h_{\text{pos}})}\ [?],\ \to\mathrm{R}
$$

$$
\dfrac{\Gamma_{\text{mes}} \vdash [v_f := *][?0 \le v_f < {}^{d_0}\!/_{\epsilon}][\mathsf{plant}_f] \mathrm{F}(v_f, x_f, d_0, \mu, h_{\text{pos}})}{\Gamma_{\text{mes}} \vdash [?0 \le v_0 < {}^{d_0}\!/_{\epsilon}][\mathsf{plant}_f(v_0)] \mathrm{F}(v_f, x_f, d_0, \mu, h_{\text{pos}})}\ [:*],\ \forall \mathrm{R}
$$

$$
\dfrac{\Gamma_{\text{mes}} \vdash [v_f := *; ?0 \le v_f < {}^{d_0}\!/_{\epsilon}][\mathsf{plant}_f] \mathrm{F}(v_f, x_f, d_0, \mu, h_{\text{pos}}) \quad \triangleright \text{图28}}{\Gamma_{\text{mes}} \vdash [v_f := *][?0 \le v_f < {}^{d_0}\!/_{\epsilon}][\mathsf{plant}_f] \mathrm{F}(v_f, x_f, d_0, \mu, h_{\text{pos}})}\ [;]
$$

$$
\dfrac{\mathrm{F}\ H_{\text{pos}}, d_0 = m - x_f \vdash [\mathsf{cond}(d_0)][\mathsf{plant}_f] \mathrm{F}(v_f, x_f, d_0, \mu, h_{\text{pos}})}{\mathrm{F}\ H_{\text{pos}} \vdash [d := m - x_f][\mathsf{cond}(d)][\mathsf{plant}_f] \mathrm{F}(v_f, x_f, d, \mu, h_{\text{pos}})}\ [:=]
$$

$$
\dfrac{\mathrm{F}, \mathsf{A}(h)\ H_{\text{pos}} \vdash [d := m - x_f; \mathsf{cond}(d)][\mathsf{plant}_f] \mathrm{F}(v_f, x_f, d, \mu, h_{\text{pos}}) \quad \triangleright \top \mathrm{R}}{\mathrm{F}\ H_{\text{pos}} \vdash [d := m - x_f][\mathsf{cond}(d)][\mathsf{plant}_f] \mathrm{F}(v_f, x_f, d, \mu, h_{\text{pos}})}\ \mathrm{WL},\ [;]
$$

$$
\dfrac{\mathrm{F} \vdash [\mathsf{pos}(h)!m]_{\{\mathsf{A}(h), \mathsf{T}\}} [d := m - x_f; \mathsf{cond}(d)][\mathsf{plant}_f] \mathrm{F}(v_f, x_f, d, \mu, h)}{\mathrm{F}, \mathsf{A}(h)\ H_{\text{pos}} \vdash [d := m - x_f; \mathsf{cond}(d)][\mathsf{plant}_f] \mathrm{F}(v_f, x_f, d, \mu, h_{\text{pos}})}\ [!\theta]_{\mathsf{AC}}\mathrm{R}
$$

$$
\dfrac{\mathrm{F} \vdash [m := *][\text{位置}(h)!m]_{\{\mathsf{A}(h), \mathsf{T}\}} [d := m - x_f; \mathsf{cond}(d)][\mathsf{plant}_f] \mathrm{F}(v_f, x_f, d, \mu, h)}{\mathrm{F} \vdash [\mathsf{pos}(h)!m]_{\{\mathsf{A}(h), \mathsf{T}\}} [d := m - x_f; \mathsf{cond}(d)][\mathsf{plant}_f] \mathrm{F}(v_f, x_f, d, \mu, h)}\ [:*],\ \forall \mathrm{R}
$$

$$
\dfrac{\mathrm{F} \vdash [\mathsf{pos}(h)?m]_{\{\mathsf{A}(h), \mathsf{T}\}} [d := m - x_f; \mathsf{cond}(d)][\mathsf{plant}_f] \mathrm{F}(v_f, x_f, d, \mu, h)}{\mathrm{F} \vdash [m := *][\text{位置}(h)!m]_{\{\mathsf{A}(h), \mathsf{T}\}} [d := m - x_f; \mathsf{cond}(d)][\mathsf{plant}_f] \mathrm{F}(v_f, x_f, d, \mu, h)}\ [\mathrm{ch}?]_{\mathsf{AC}}
$$

$$
\dfrac{\mathrm{F} \vdash [\mathsf{pos}(h)?m]_{\{\mathsf{A}(h), \mathsf{T}\}} [d := m - x_f; \mathsf{cond}(d)]_{\{\mathsf{A}(h), \mathsf{T}\}} [\mathsf{plant}_f] \mathrm{F}(v_f, x_f, d, \mu, h)}{\mathrm{F} \vdash [\mathsf{pos}(h)?m]_{\{\mathsf{A}(h), \mathsf{T}\}} [d := m - x_f; \mathsf{cond}(d)][\mathsf{plant}_f] \mathrm{F}(v_f, x_f, d, \mu, h)}\ [\epsilon]_{\mathsf{AC}},\ \mathrm{W}[]_{\mathsf{AC}}
$$

$$
\dfrac{\mathrm{F} \vdash [\mathsf{dist}(h)]_{\{\mathsf{A}(h), \mathsf{T}\}} [\mathsf{plant}_f] \mathrm{F}}{\mathrm{F} \vdash [\mathsf{pos}(h)?m]_{\{\mathsf{A}(h), \mathsf{T}\}} [d := m - x_f; \mathsf{cond}(d)]_{\{\mathsf{A}(h), \mathsf{T}\}} [\mathsf{plant}_f] \mathrm{F}(v_f, x_f, d, \mu, h)}\ [;]_{\mathsf{AC}}
$$

图27：接续图 8 中的证明。程序 $\mathsf{cond}$ 是 $\mathsf{if}(d \le \epsilon V)\, \{v_f := *; ?0 \le v_f < {}^{d}\!/_{\epsilon}\}$ 的缩写。公式 $H_{\text{pos}}$ 是 $h_{\text{pos}} = h \cdot \langle \mathsf{pos}\ m, \mu \rangle$ 的简写。此外，$\Gamma_{\text{mes}}$ 表示公式列表 $\mathrm{F}\ H_{\text{pos}}, d_0 = m - x_f, d_0 \le \epsilon V$。

$$
\dfrac{*}{\mathrm{F}\ m - x_f > \epsilon V, t \ge 0 \vdash 0 \le v_f \le {}^{d_0}\!/_{\epsilon} \land v_f \le V \land x_f + t \cdot v_f + (\epsilon - (\mu + t - \mu)) {}^{d_0}\!/_{\epsilon} < m}\ \mathbb{R}
$$

$$
\dfrac{\mathrm{F}\ m - x_f > \epsilon V, t \ge 0 \vdash 0 \le v_f \le {}^{d_0}\!/_{\epsilon} \land v_f \le V \land x_f + t \cdot v_f + (\epsilon - (\mu + t - \mu)) {}^{d_0}\!/_{\epsilon} < m}{\mathrm{F}\ m - x_f > \epsilon V, t \ge 0 \vdash 0 \le v_f \le {}^{d_0}\!/_{\epsilon} \land v_f \le V \land x_f + t \cdot v_f + (\epsilon - \Delta(\mu + t, h \cdot \langle \text{位置}\ m, \mu \rangle)) {}^{d_0}\!/_{\epsilon} < m}\ \triangleright \mathbb{N}
$$

$$
\dfrac{\mathrm{F}\ m - x_f > \epsilon V, t \ge 0 \vdash 0 \le v_f \le {}^{d_0}\!/_{\epsilon} \land v_f \le V \land x_f + t \cdot v_f + (\epsilon - (\mu + t - \mu)) {}^{d_0}\!/_{\epsilon} < m}{\mathrm{F}\ m - x_f > \epsilon V, t \ge 0 \vdash 0 \le v_f \le {}^{d_0}\!/_{\epsilon} \land v_f \le V \land x_f + t \cdot v_f + (\epsilon - \Delta(\mu + t, h \cdot \langle \text{位置}\ m, \mu \rangle)) {}^{d_0}\!/_{\epsilon} < m}\ \triangleright \mathbb{N}
$$

$$
\dfrac{\mathrm{F}\ m - x_f > \epsilon V, t \ge 0 \vdash \mathrm{F}(v_f, x_f + t \cdot v_f, d_0, \mu + t, h \cdot \langle \text{位置}\ m, \mu \rangle)}{\mathrm{F}\ m - x_f > \epsilon V, t \ge 0 \vdash \mathrm{F}(v_f, x_f + t \cdot v_f, d_0, \mu + t, h \cdot \langle \text{位置}\ m, \mu \rangle)}\ \downarrow\in,\ \text{值}=
$$

$$
\dfrac{\mathrm{F}\ H_{\text{pos}}, m - x_f > \epsilon V, t \ge 0 \vdash \mathrm{F}(v_f, x_f + t \cdot v_f, d_0, \mu + t, h_{\text{pos}})}{\mathrm{F}\ H_{\text{pos}}, m - x_f > \epsilon V \vdash \forall t \ge 0\, \mathrm{F}(v_f, x_f + t \cdot v_f, m - x_f, \mu + t, h_{\text{pos}})}\ =\mathrm{R}
$$

$$
\dfrac{\mathrm{F}\ H_{\text{pos}}, m - x_f > \epsilon V \vdash \forall t \ge 0\, \mathrm{F}(v_f, x_f + t \cdot v_f, m - x_f, \mu + t, h_{\text{pos}})}{\mathrm{F}\ H_{\text{pos}}, m - x_f > \epsilon V \vdash [\mu' = 1, x_f' = v_f] \mathrm{F}(v_f, x_f, m - x_f, \mu, h_{\text{pos}})}\ \forall \mathrm{R}
$$

$$
\dfrac{\mathrm{F}\ H_{\text{pos}}, m - x_f > \epsilon V \vdash [\mathsf{plant}_f] \mathrm{F}(v_f, x_f, m - x_f, \mu, h_{\text{pos}})}{\mathrm{F}\ H_{\text{pos}}, m - x_f > \epsilon V \vdash [\mu' = 1, x_f' = v_f] \mathrm{F}(v_f, x_f, m - x_f, \mu, h_{\text{pos}})}\ [\mu]
$$

$$
\dfrac{\mathrm{F}\ H_{\text{pos}}, d_0 = m - x_f, d_0 > \epsilon V \vdash [\mathsf{plant}_f] \mathrm{F}(v_f, x_f, d_0, \mu, h_{\text{pos}})}{\mathrm{F}\ H_{\text{pos}}, m - x_f > \epsilon V \vdash [\mathsf{plant}_f] \mathrm{F}(v_f, x_f, m - x_f, \mu, h_{\text{pos}})}\ [']\ [:=]
$$

$$
\dfrac{*}{\mathrm{F}\ H_{\text{pos}}, d_0 = m - x_f, d_0 > \epsilon V \vdash [\mathsf{plant}_f] \mathrm{F}(v_f, x_f, d_0, \mu, h_{\text{pos}})}\ =\mathrm{L},\ =\mathrm{R}
$$

图28：接续图27中的证明