arXiv:2301.03435v2 [cs.FL] 1 Feb 2024

非确定有限自动机代数

Roberto Gorrieri*

博洛尼亚大学信息学、科学与工程系，意大利博洛尼亚市 A. Zamboni 城墙路 7 号，邮编 41027

摘要

本文提出一种进程代数，其语义将一个项映射为一个非确定有限自动机（简称 NFA）。我们证明了一个可表示性定理：对于每个 NFA N，都存在一个进程代数项 p，使其语义所对应的 NFA 与 N 同构。此外，我们给出了语言等价的简洁公理化：两个 NFA N_1 和 N_2 识别相同语言，当且仅当相应的项 p_1和 p_2, 分别可以仅通过一组公理等同，这组公理包含 7 条公理和 3 条条件公理。

关键词：有限限自动机、语言等价、公理化 。

1. 引言

非确定有限自动机（简称非确定有限自动机，NFA）最初于 [25], 提出，是一种众所周知的顺序计算模型（例如，参见 [16] 中的入门教材），专门用于识别正则语言类，即能够用正则表达式 [17] 描述的语言。

Kleene 算法 [17] （例如，参见 [15, 16] 中更易读、更易理解的描述）可将给定的非确定有限自动机 N 转换为正则表达式 e_N ，该表达式描述的正是 N 所接受的同一正则语言。反过来，McNaughton 和 Yamada 算法 [23] 可将任意正则表达式 e 转换为与之等价的非确定有限自动机。因此，结合这两个结果，我们得到一个表示性定理（见图 1），指出正则表达式的克莱尼代数确实能够表示非确定有限自动机类（以语言等价为准）∼。事实上，

(i) 给定一个非确定有限自动机 N，我们通过 Kleene 算法构造一个与之等价的正则表达式 e_N：因此，所有非确定有限自动机都可以用正则表达式表示；并且

(ii) 对于每个正则表达式 e（因此也包括 e_N），我们通过 McNaughton 和 Yamada 算法构造一个与之等价的非确定有限自动机 N′(e)（因此也包括 N′(e_N)）；因此，只有非确定有限自动机才能用正则表达式表示；最后，

*通讯作者 电子邮件地址：roberto.gorrieri@unibo.it（Roberto Gorrieri）

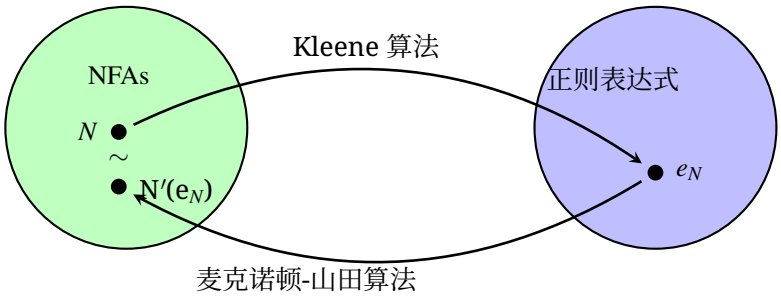

图 1：可表示性定理的图形描述（截至语言等价）

(iii) 非确定有限自动机 N 与 $N'(e_N)$ 语言等价，记作 $N \sim N'(e_N)$。

本文提出了一种称为 SFM1 的代数，它同样能够真正表示非确定有限自动机，但仅在同构意义下成立。更确切地说，SFM1 是有限状态 CCS 的一种方言 SFM 的小幅扩展 [20, 22, 11], , 见 [12, 14], ; 它引入了额外的常量 1，以区分终态和非终态，这一做法已在 BPA 及相关语言中采用（有关这一问题的详细研究，参见 [4] ）。除分别用于表示终态和非终态的两个常量 1 和 0 外，SFM1 还包含一个析取运算符（与正则表达式中的一样），记作 $+$ （类似于有限状态 CCS 的选择算子），以及$\alpha.$ 中每个 $\alpha \in A \cup \{\varepsilon\}$对应的前缀算子，其中 A 是有限字母表， ε 是表示空词的符号。前缀算子是正则表达式的连接算子 $\cdot$的一种弱化形式，因为它每次只能将一个符号连接到一项上，如 a.p。为了弥补这一较弱算子表达能力的不足，SFM1 用更强大的递归运算符取代了正则表达式的迭代算子 * （或 Kleene 星号）；该递归运算符通过进程常量实现（与 CCS[22, 11]中的做法相同），其用法与右线性文法[16]中非终结符的用法相同。例如，考虑递归常量 C，其定义为 $C \doteq a.C + \mathbf{1}$；那么，它的语义是一个只有一个状态的非确定有限自动机，该状态既是初始状态也是终态，并带有一个标记为 a 的自环；因此，C 接受语言 $\{a^n \mid n \geq 0\}$，可用正则表达式 a^*表示。

对于 SFM1，我们得到一个可表示性定理（见图 2），该定理指出 SFM1 确实表示了非确定有限自动机这一类，且在同构意义下 $\equiv$。事实上，

(i) 给定一个非确定有限自动机 N，我们通过定理 2 的证明中描述的算法，将其编译为 SFM1 项表示 p_N： 因此，所有非确定有限自动机都可以由 SFM1 表示；(ii) 对每个 SFM1 项 p（因此也包括 p_N），我们借助表2中描述的指称语义，将其关联到一个非确定有限自动机 $N'(p)$（因此也包括 $N'(p_N)$）：因此，只有非确定有限自动机才能由 SFM1 表示；最后，(iii) 非确定有限自动机 N 与 $N'(p_N)$ 同构，记作 $N \equiv N'(p_N)$。

这一定理更具体的可表示性优势在于，代数 SFM1 可作为研究所有可在

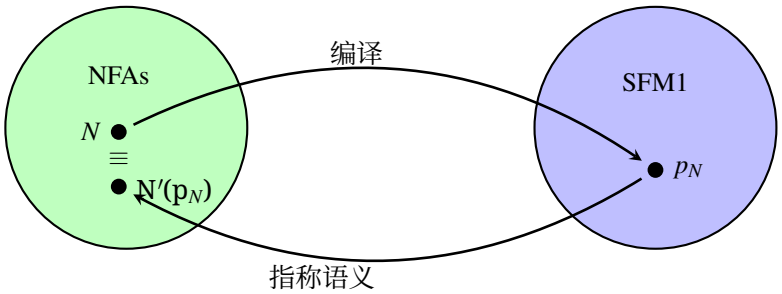

图 2：可表示性定理的图示描述（在同构意义下）

非确定有限自动机上定义的等价关系的基础，不仅包括语言等价 $\sim$（正则表达式也是如此），还包括更具体的等价关系，例如双模拟等价 [24, 22, 4, 11], ，或线性时/分支时谱 [10, 11]中的任何一种。

本文的主要贡献是证明：语言等价可以通过一种非常简洁的公理化在 SFM1 项上加以刻画，该公理化仅包含 7 条公理（析取有 4 条，前缀有 3 条）和 3 条条件公理（用于递归）。我们提出的公理与已知公理 [17, 27, 18,20, 21, 14] 非常相似。事实上，对于析取，它们就是常见的公理：选择算子构成一个幂等、交换的幺半群，且 0 为单位元。前缀的公理与连接的公理类似：0 是零元，前缀算子对选择项满足分配律，并且前缀 ε 可以被吸收。递归的公理也与针对 SFM [13, 14], 开发的公理类似，而后者又受到有限状态 CCS [21, 22] 的公理启发：展开公理（指出常量 C，若定义为 $\mathrm{C} \doteq \mathrm{p}\{\mathrm{C}/\mathrm{x}\}$，则可与其主体 $\mathrm{p}\{\mathrm{C}/\mathrm{x}\}$ 等同）；折叠公理（大致指出，若 $\mathrm{C} \doteq \mathrm{p}\{\mathrm{C}/\mathrm{x}\}$ 且 $\mathrm{q} = \mathrm{p}\{\mathrm{q}/\mathrm{x}\}$，则 $\mathrm{C} = \mathrm{q}$）；以及切除公理（指出，若 $\mathrm{C} \doteq (\varepsilon.\mathrm{x} + \mathrm{q})\{\mathrm{C}/\mathrm{x}\}$ 且 $\mathrm{D} \doteq \mathrm{q}\{\mathrm{D}/\mathrm{x}\}$，则 $\mathrm{C} = \mathrm{D}$）。

本文组织如下。第2节回顾有关非确定有限自动机的基本定义，包括语言等价 $\sim$、双模拟等价 $\simeq$ 和同构等价 $\equiv$。第3节介绍代数 SFM1（即其语法，以及以非确定有限自动机为基础的指称语义），并证明图2中概述的可表示性定理。第 4 节表明，语言等价 $\sim$ 是 SFM1 所有算子的同余，尤其是递归算子的同余。第5节研究 SFM1 项上语言等价的代数性质，这些性质有助于证明公理化的可靠性。本文特别运用不动点理论 [8, 28], 证明递归的折叠律；该定律仅当递归定义的常量 C 是观察守卫的，也就是说，不能执行标记为 ε的循环：$\mathrm{C} \overset{\varepsilon}{\not\Rightarrow} \mathrm{C}$ 时才成立。第6节描述如何在使用进程常量表示递归的代数中进行等式推导。第7节首先给出公理集并证明该公理化是可靠的。此外，我们还证明了公理化的完备性：首先针对观察守卫的 SFM1 项证明这一结果（先将观察守卫的项转化为不含 ε的范式，再仅用9条公理证明这些范式的完备性），随后又将完备性证明扩展到观察上无守卫的 SFM1 项，方法是证明，

借助额外的切除条件递归公理，每个观察上无守卫的项都可以等价地改写为一个观察守卫的项。第8节补充结论性意见，并对未来研究提出建议。

2. 非确定有限自动机

设 A 表示一个有限字母表，其元素记作 a、b……。设 A^* 表示 A 上所有词的集合（包括空词 ε），其元素记作 σ。设 α取遍 $A \cup \{\varepsilon\}$。设 $\mathscr{P}(A^*)$ 表示 A 上所有形式语言的集合，其元素记作 L，也可以带下标。

定义 1. 非确定有限自动机（简称 NFA）是一个元组 $N = (Q, A, T, F, q_0)$，其中

- Q 是一个有限状态集，其元素记作 q（也可以带下标）；
- A 是一个有限字母表；
- $T \subseteq Q \times (A \cup \{\varepsilon\}) \times Q$ 是转移的集合，遍历其中的 t（可以带索引）；
- $F \subseteq Q$ 是终态的集合；
- $q_0 \in Q$ 是初始状态。

给定一个转移 $t = (q\ \alpha, q')$，q 称为源，α 该转移的标签（也记作 l(t)），q′ 称为目标；通常表示为 $q \xrightarrow{\alpha} q'$。若 NFA $N = (Q, A, T, F, q_0)$ 满足以下条件，则称其为确定性的：

- $\forall t \in T\ l(t) \in A$（即不存在 ε无标签转移），并且
- $\forall q \in Q\ \forall a \in A$，恰好存在一个状态 $q' \in Q$，使得 $(q, a, q') \in T$，也就是说，T 可以等价地表示为一个类型为 $Q \times A \to Q$ 的函数。

确定性非确定有限自动机简称确定性有限自动机（DFA）。 □

定义 2。（可达关系与约简非确定有限自动机）给定 $N = (Q, A, T, F, q_0)$，可达关系 $\Rightarrow \subseteq Q \times A^* \times Q$ 是由以下公理和规则导出的最小关系：

$$\frac{}{q \overset{\varepsilon}{\Longrightarrow} q} \qquad \frac{q \xrightarrow{\alpha} q'}{q \overset{\alpha}{\Longrightarrow} q'} \qquad \frac{q_1 \overset{\sigma}{\Longrightarrow} q_2 \quad q_2 \xrightarrow{\alpha} q_3}{q_1 \overset{\sigma\alpha}{\Longrightarrow} q_3}$$

其中，当然我们假设 ε 是连接运算的单位元：$\sigma\varepsilon = \sigma = \varepsilon\sigma$。当存在一个词 σ使得 $q_1 \overset{\sigma}{\Longrightarrow} q_2$ 时，我们简单地写作 $q_1 \Rightarrow q_2$，表示从 q_1 可达 q_2。我们还可以如下定义 reach(q)：$\mathrm{reach}(q) = \{q' \mid q \Rightarrow q'\}$。若非确定有限自动机 $N = (Q, A, T, F, q_0)$ 满足 $\mathrm{reach}(q_0) = Q$，则称其为约简的。□

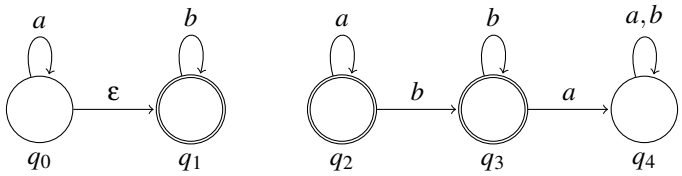

图 3：一个非确定有限自动机和一个确定有限自动机，它们都识别语言 a^*b^*

定义 3.（识别语言与等价）给定 $N = (Q, A, T, F, q_0)$，N 识别的语言为 $L[N] = \{\sigma \in A^* \mid \exists q \in F. q_0 \stackrel{\sigma}{\Longrightarrow} q\}$。状态 $q \in Q$ 识别的语言为 $L[N, q] = \{\sigma \in A^* \mid \exists q' \in F. q \stackrel{\sigma}{\Longrightarrow} q'\}$。若两个状态 q_1 和 q_2 等价，记作 $q_1 \sim q_2$，，当且仅当 $L[N, q_1] = L[N, q_2]$。若两个非确定有限自动机 $N_1 = (Q_1, A_1, T_1, F_1, q_{01})$ 和 $N_2 = (Q_2, A_2, T_2, F_2, q_{02})$ 识别相同的语言，则称它们等价，即 $L[N_1] = L[N_2]$。□

众所周知，非确定有限自动机所识别的语言类就是正则语言类（例如，参见 [16] 一本入门教材），也就是说，这些语言可以用正则表达式表示（最初由 Kleene 在 [17] 中提出；我们假定读者熟悉这一代数）。

例 1。图 3 展示了两个有限自动机：左边的是一个非确定有限自动机，其初始状态为 q_0，终态为 q_1,；右边的是一个确定有限自动机，其初始状态为 q_2，终态为 q_2 和 q_3。两者识别同一个正则语言 $\{a^n b^m \mid n, m \geq 0\}$，该语言可以用正则表达式 a^*b^*表示。事实上，$q_0 \sim q_2$，因为 $L[N, q_0] = L[N, q_2]$,，其中 N 是这两个自动机的并集（由于它们的状态集合互不相交，因此可以取并集）。□

可以在非确定有限自动机上定义更具体的等价关系，例如双模拟等价 [24, 22, 4, 11] 和同构等价。

定义 4。（互模拟）设 $N = (Q, A, T, F, q_0)$ 是一个非确定有限自动机。互模拟是一个关系 $R \subseteq Q \times Q$，满足：若 $(q_1, q_2) \in R$，则对所有 $\alpha \in A \cup \{\varepsilon\}$

- $\forall q_1'$ 使得 $q_1 \xrightarrow{\alpha} q_1'$，$\exists q_2'$ 使得 $q_2 \xrightarrow{\alpha} q_2'$，且 $(q_1', q_2') \in R$,
- $\forall q_2'$ 使得 $q_2 \xrightarrow{\alpha} q_2'$，$\exists q_1'$ 使得 $q_1 \xrightarrow{\alpha} q_1'$，且 $(q_1', q_2') \in R$，并且
- $q_1 \in F$ 当且仅当 $q_2 \in F$。

两个状态 q 和 q' 互模拟等价，记作 $q \simeq q'$，当且仅当存在一个互模拟 R，使得 $(q, q') \in R$。□

例 2. 给定一个非确定有限自动机 $N = (Q, A, T, F, q_0)$，很容易看出，如果 $q_1 \simeq q_2$，那么 $q_1 \sim q_2$。反向推论并不成立。例如，考虑图 3：显然，$q_0 \sim q_2$,，但 $q_0 \not\simeq q_2$。□

注 1. 有趣的是，如果 $N = (Q,A,T,F,q_0)$ 是一个确定有限自动机，那么语言等价与双模拟等价一致。事实上，很容易看出，对于确定有限自动机，关系 $R = \{(q_1,q_2) \mid q_1 \sim q_2\}$ 是一个互模拟。□

定义 5。（同构）如果存在一个双射 $f : Q_1 \to Q_2$，满足以下条件，则称两个非确定有限自动机 $N_1 = (Q_1,A_1,T_1,F_1,q_{01})$ 和 $N_2 = (Q_2,A_2,T_2,F_2,q_{02})$ 同构，记作 $N_1 \equiv N_2$, :

- 它是类型保持的：$q_1 \in F1$ 当且仅当 $f(q1) \in F2$;
- 它保持转移：$q \xrightarrow{\alpha}_1 q'$ 当且仅当 $f(q) \xrightarrow{\alpha}_2 f(q')$，对于所有 q、$q' \in Q1$ 以及所有$\alpha \in A_1 \cup A_2 \cup \{\varepsilon\}$；并且
- 它保持初始状态：$f(q01) = q02$。

□

3. SFM1：语法与语义

我们将要定义的进程代数 SFM1 是对有限状态 CCS 的一种方言 [22, 11], SFM 的小幅扩展。在 [12], 中，引入了额外的常量 1，以便区分终态和非终态; BPA 及相关语言中也采用了这一做法（有关该问题的深入研究，请参见 [4] ）。

3.1. 语法

令 $\mathscr{C}$ 为一个有限的常量集，与字母表 A 不相交，并用 C、D.....（也可以带下标）表示。有限集合 A 和 $\mathscr{C}$的大小并不重要：我们假定可以根据需要将它们选得足够大。SFM1 项由字母表符号和常量通过以下抽象语法生成:

$$\begin{array}{lcl} s & ::= & \mathbf{1} \mid \mathbf{0} \mid \alpha.p \mid s+s \qquad \textit{guarded processes} \\ p & ::= & s \mid C \qquad\qquad\qquad\qquad\quad \textit{processes} \end{array}$$

其中，特殊常量 1 和 0 分别表示终态和非终态， α.p 是一个进程，其中符号 $\alpha \in A \cup \{\varepsilon\}$ 作为前缀作用于剩余项 p（$\alpha.-$ 是一族前缀算子， α中每个元素各对应一个算子）； $s_1 + s_2$ 表示 s_1 与 s_2 的析取（$-+-$ 是选择算子）； C 是一个常量。常量 C 可以配有一个定义，但该定义必须是受守卫进程，即 $C \doteq s$。若谓词 $\downarrow$ 成立，则项 p 是终态项，其中 $p\downarrow$ 成立；谓词 $\downarrow$ 是由表 1 中列出的公理和规则生成的最小谓词。

我们用 Const(p) 表示 p 所使用的进程常量集合 $\delta(p,/0)$，其中辅助函数 δ 的定义如下；该函数还额外接受一个已知常量集合 I 作为参数:

$$\begin{array}{rcl} \delta(\mathbf{1},I) & = & \emptyset \qquad\qquad\qquad\quad \delta(\mathbf{0},I) = \emptyset \\ \delta(\alpha.p,I) & = & \delta(p,I) \qquad \delta(p_1+p_2,I) = \delta(p_1,I) \cup \delta(p_2,I) \\ \delta(C,I) & = & \begin{cases} \emptyset & C \in I, \\ \{C\} & C \notin I \wedge C \text{ undefined}, \\ \{C\} \cup \delta(p,I \cup \{C\}) & C \notin I \wedge C \doteq p. \end{cases} \end{array}$$

$\frac{}{\mathbf{1}\downarrow}$	$\frac{p_1\downarrow}{(\mathrm{p}_1+\mathrm{p}_2)\downarrow}$	$\frac{p_2\downarrow}{(\mathrm{p}_1+\mathrm{p}_2)\downarrow}$	$\frac{\mathrm{p}\downarrow \quad \mathrm{C}\doteq\mathrm{p}}{C\downarrow}$

表 1：终态：谓词 $\downarrow$

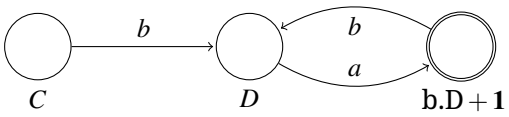

图4：例3中 $\mathrm{C}\doteq\mathrm{b.D}$ 的非确定有限自动机，其中 $\mathrm{D}\doteq\mathrm{a.(b.D}+\mathbf{1})$

若项 p 的 Const(p) 是有限集，且 Const(p) 中的每个常量都配有一个定义方程（属于类别 s），则称 p 为 SFM1 进程。SFM1 进程的集合记为 $\mathscr{P}_{SFM1}$，而其受守卫进程的集合（即属于语法类别 s 的进程）记为 $\mathscr{P}^{grd}{}_{SFM}1$。

3.2. 指称语义

现在我们给出一种构造与进程 p 相关联的非确定有限自动机 $[\![\mathrm{p}]\!]_\emptyset$ 的方法，其风格具有组合性和指称性。构造的细节概述于表2。编码以扫描 p 时已发现的常量集为参数；该集合初始为空，用于避免在递归常量上循环。定义由语法驱动，且所构造的非确定有限自动机的状态也是句法对象，即 SFM1 进程项。选择规则需要稍加注意：为了只纳入严格必要的状态和转移，只有当非确定有限自动机 $[\![\mathrm{p}_1]\!]_I$（或 $[\![\mathrm{p}_2]\!]_I$）中存在一条转移可达状态 p_1（或 p_2）时，非确定有限自动机 $[\![\mathrm{p}]\!]_\emptyset$（或 $_1$）中的初始状态 p_1（或 p_2）才应保留在 $\mathrm{p}_1+\mathrm{p}_2$ 的非确定有限自动机中；否则，新的非确定有限自动机中可以安全地移除 p_1（或 p_2）。常量规则也类似。在表2中，我们用 $\mathrm{T}(\mathrm{q})=\{\mathrm{t}\in\mathrm{T}\mid \exists\alpha\in\mathrm{A}\cup\{\varepsilon\},\exists\mathrm{q}'\in\mathrm{Q}.\mathrm{t}=(\mathrm{q}\ \alpha,\mathrm{q}')\}$ 表示 T 中以 q 为源状态的转移集合。

例3。考虑常量 $\mathrm{C}\doteq\mathrm{b.D}$，其中 $\mathrm{D}\doteq\mathrm{a.(b.D}+\mathbf{1})$。根据表2中的定义，$[\![\mathrm{D}]\!]_{\{C,D\}}=(\{\mathrm{D}\},/0,/0,/0,\mathrm{D})$。接着，通过前缀操作，$[\![\mathrm{b.D}]\!]_{\{C,D\}}=(\{\mathrm{b.D},\mathrm{D}\},\{\mathrm{b}\},\{(\mathrm{b.D},\mathrm{b},\mathrm{D})\},/0,\mathrm{b.D})$。现在，$[\![\mathbf{1}]\!]_{\{C,D\}}=(\{\mathbf{1}\},/0,/0,\{\mathbf{1}\},1)$。然后，通过求和 $[\![\mathrm{b.D}+\mathbf{1}]\!]_{\{C,D\}}=(\{\mathrm{b.D}+\mathbf{1},\mathrm{D}\},\{\mathrm{b}\},\{(\mathrm{b.D}+1,\mathrm{b},\mathrm{D})\},\{\mathrm{b.D}+\mathbf{1}\},\mathrm{b.D}+\mathbf{1})$。注意，状态 b.D 和 1 已被移除，因为在 $[\![\mathrm{b.D}]\!]_{\{C,D\}}$ 中没有转移可达 b.D，且在 $[\![\mathbf{1}]\!]_{\{C,D\}}$ 中没有转移可达 1。再次通过前缀操作，$[\![\mathrm{a.(b.D}+\mathbf{1})]\!]_{\{C,D\}}=(\{\mathrm{a.(b.D}+\mathbf{1}),\mathrm{b.D}+\mathbf{1},\mathrm{D}\},\{\mathrm{a},\mathrm{b}\},\{(\mathrm{a.(b.D}+\mathbf{1}),\mathrm{a},\mathrm{b.D}+\mathbf{1}),(\mathrm{b.D}+\mathbf{1},\mathrm{b},\mathrm{D})\},\{\mathrm{b.D}+\mathbf{1}\},\mathrm{a.(b.D}+\mathbf{1}))$。现在，常量规则保证 $[\![\mathrm{D}]\!]_{\{C\}}=(\{\mathrm{D},\mathrm{b.D}+\mathbf{1}\},\{\mathrm{a},\mathrm{b}\},\{(\mathrm{D},\mathrm{a},\mathrm{b.D}+\mathbf{1}),(\mathrm{b.D}+\mathbf{1},\mathrm{b},\mathrm{D})\},\{\mathrm{b.D}+\mathbf{1}\},\mathrm{D})$。注意，状态 $\mathrm{a.(b.D}+\mathbf{1})$ 已被移除，因为在 $[\![\mathrm{a.(b.D}+\mathbf{1})]\!]_{\{C,D\}}$ 中没有转移可达该状态。通过前缀操作，

$[\![\mathbf{1}]\!]_I$	=	$(\{\mathbf{1}\},\emptyset,\emptyset,\{\mathbf{1}\},\mathbf{1})$	
$[\![\mathbf{0}]\!]_I$	=	$(\{\mathbf{0}\},\emptyset,\emptyset,\emptyset,\mathbf{0})$	
$[\![\alpha.p]\!]_I$	=	$(Q,A,T,F,\alpha.p)$	given $[\![p]\!]_I=(Q',A',T',F',p)$ and where $Q=\{\alpha.p\}\cup Q'$ $F=F', T=\{(\alpha.p,\alpha,p)\}\cup T', A=\begin{cases}\{\alpha\}\cup A' & \text{if } \alpha\neq\varepsilon\\ A' & \text{o.w.}\end{cases}$
$[\![p_1+p_2]\!]_I$	=	(Q,A,T,F,p_1+p_2)	given $[\![p_i]\!]_I=(Q_i,A_i,T_i,F_i,p_i)$ for $i=1,2$, and where $Q=\{p_1+p_2\}\cup Q_1'\cup Q_2'$, with, for $i=1,2$, $Q_i'=\begin{cases}Q_i & \exists t\in T_i \text{ such that } t=(q,\alpha,p_i)\\ Q_i\setminus\{p_i\} & \text{o.w.}\end{cases}$ $A=A_1\cup A_2$, $T=T'\cup T_1'\cup T_2'$, with, for $i=1,2$, $T_i'=\begin{cases}T_i & \exists t\in T_i.t=(q,\alpha,p_i)\\ T_i\setminus T_i(p_i) & \text{o.w.}\end{cases}$ $T'=\{(p_1+p_2,\alpha,q)\mid (p_i,\alpha,q)\in T_i, i=1,2\}$ $F_i'=F_i\cap Q_i'$ for $i=1,2$, and $F=\begin{cases}F_1'\cup F_2'\cup\{p_1+p_2\} & \text{if } p_1\in F_1 \text{ or } p_2\in F_2\\ F_1'\cup F_2' & \text{o.w.}\end{cases}$
$[\![C]\!]_I$	=	$(\{C\},\emptyset,\emptyset,\emptyset,C)$	if $C\in I$
$[\![C]\!]_I$	=	(Q,A,T,F,C)	if $C\notin I$, given $C\doteq p$ and $[\![p]\!]_{I\cup\{C\}}=(Q',A',T',F',p)$ $A=A', Q=\{C\}\cup Q''$, where $Q''=\begin{cases}Q' & \exists t\in T' \text{ such that } t=(q,\alpha,p)\\ Q'\setminus\{p\} & \text{o.w.}\end{cases}$ $T=\{(C,\alpha,q)\mid (p,\alpha,q)\in T'\}\cup T''$ where $T''=\begin{cases}T' & \exists t\in T'.\ t=(q,\alpha,p)\\ T'\setminus T'(p) & \text{o.w.}\end{cases}$ $F''=F'\cap Q''$ and $F=\begin{cases}F''\cup\{C\} & \text{if } p\in F'\\ F'' & \text{o.w.}\end{cases}$

表2：指称语义

$[\![\text{b.D}]\!]_{\{C\}}=$({b.D, D, b.D +**1**}, {a, b}, {(b.D, b, D), (D, a, b.D +**1**), (b.D +**1**, b, D)},{b.D +**1**}, b.D)，最后，$[\![\text{C}]\!]_\emptyset=$({C, D, b.D +**1**}, {a, b}, {(C, b, D), (D, a, b.D +**1**), (b.D +**1**, b, D)},{b.D +**1**},C)。所得的非确定有限自动机如图 4 所示。□

定理 1. 对于每个 SFM1 进程 p，$[\![\text{p}]\!]_\emptyset$ 是一个约简非确定有限自动机。

证明。根据 $[\![\text{p}]\!]_I$ 的定义进行归纳法证明。于是，对于 I = /0，待证命题成立。

第一个基例针对 0，待证命题显然成立，因为对于任意 I $\subseteq\mathscr{C}$，$[\![\mathbf{0}]\!]_I=$({**0**}，/0，/0，/0，0) 显然是一个约简非确定有限自动机。对于 1，情况类似。第三个基例针对 C，其中 C $\in$ I，这对应于 C 未定义的情况。在这种情况下，对于任意 I $\subseteq\mathscr{C}$ 且 C $\in$ I，$[\![\text{C}]\!]_I=$({C}，/0，/0，/0，C) 是一个约简非确定有限自动机。

归纳情形如下。

前缀：根据归纳法，我们假设 $[\![p]\!]_I = (Q', A', T', F', p)$ 是一个约简非确定有限自动机。因此，$[\![\alpha.p]\!]_I = (Q' \cup \{\alpha.p\}, A, T' \cup \{(\alpha.p\ \alpha, p)\}, F', \alpha.p)$（其中，如果 $= A' \cup \{\alpha\}$ if$\alpha \neq \varepsilon$，则 $A = A'$；否则 $A = A'$）也是一个约简非确定有限自动机。

选择：根据归纳法，我们可以假设，对于 $i = 1、2$，$[\![p_i]\!]_I = (Q_i, A_i, T_i, F_i, p_i)$ 都是约化的非确定有限自动机。因此，$[\![p_1 + p_2]\!]_I = (Q, A, T, F, p_1 + p_2)$ 也是一个非确定有限自动机，因为根据表2中的定义，$|Q| \leq 1 + |Q_1| + |Q_2|$、$|A| \leq |A_1| + |$ 和 $|T| \leq |T'| + |T_1| + |T_2|$，其中 $|T'| \leq |T_1| + |T_2|$；而且按构造它也是约化的。

常量：在此情况下，我们假设 $C \doteq p$ 且 $C \notin I$。根据归纳法，我们可以假设 $[\![p]\!]_{I \cup \{C\}} = (Q', A', T', F', p)$ 是一个约化的非确定有限自动机。因此，$[\![C]\!]_I = (Q, A, T, F, C)$ 也是一个非确定有限自动机，因为根据表2中的定义，$|Q| \leq 1 + |Q'|$、$A = A'$ 和 $|T| \leq 2 \cdot |T'|$；而且按构造它也是约化的。□

定理 2.（可表示性）对于任意约简非确定有限自动机 N，都存在一个 SFM1 进程 p，使得 $[\![p]\!]_\emptyset$ 与 N 同构。

证明。设 $N = (Q, A, T, F, q_0)$ 是一个约简非确定有限自动机，其中 $Q = \{q_0, q1, ..., q_n\}$。对于 $i = 1, \ldots, n$，令 $T(q_i) = \{t \in T \mid \exists \alpha \in A \cup \{\varepsilon\}, \exists q_k \in Q.t = (q_i, \alpha, q_k)\}$ 表示 T 中以 q_i 为源状态的转移集合。我们为状态 q_i 定义与之对应的进程常量 C_i，其中 $i = 0, 1, ..., n$，定义如下：

- 如果 $q_i \notin F$ 且 $T(q_i) = /0$（即 q_i 是死锁），那么 $C_i \doteq \mathbf{0}$；
- 若 $q_i \in F$ 且 q_i 是一个死锁，则 $C_i \doteq \mathbf{1}$；
- 若 $qi \notin F$ 且 $T(qi) \neq /0$，则 $Ci \doteq \Sigma_{(q_i \alpha, q_k) \in T(q_i)} \alpha \cdot Ck$；
- 若 $qi \in F$ 且 $T(qi) \neq /0$，则 $Ci \doteq \Sigma_{(q_i \alpha, q_k) \in T(q_i)} \alpha \cdot Ck + \mathbf{1}$。

考虑 $[\![C_0]\!]_\emptyset$。不难看出，$\mathrm{reach}(C_0) = \{C_0, C1 ..., C_n\}$，因为 N 是约简的。因此，我们要寻找的双射是 $f : Q \to \{C_0, C1 ..., C_n\}$，定义为 $f(q_i) = C_i$。也很容易观察到，同构的三个条件均得到满足，即：

- $q \in F$ iff $f(q)\downarrow$, and
- $q \xrightarrow{\alpha}_1 q' \in N$ iff $f(q) \xrightarrow{\alpha}_2 f(q') \in [\![C_0]\!]_\emptyset$, and
- $C_0 = f(q_0)$.

因此，f 确实是一个 NFA 同构。□

推论 1. SFM1 在同构意义下表示约化的非确定有限自动机类。

证明。根据定理 1，SFM1 进程的语义是一个约简非确定有限自动机；因此，SFM1 进程只能表示约简非确定有限自动机。根据定理 2，每个约简非确定有限自动机都可以由某个合适的 SFM1 进程表示（同构意义下）；因此，所有约简非确定有限自动机都可以由 SFM1 进程表示。□

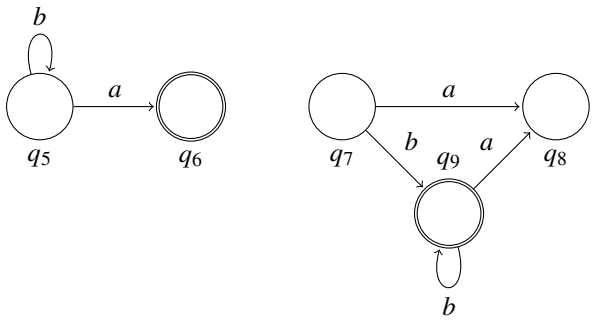

图5：例4的两个非确定有限自动机

例4。我们来考虑图 3 中的非确定有限自动机。根据定理 2 证明中的构造，SFM1 表示如下：

$$C_0 \doteq a.C_0 + \varepsilon.C_1$$
$$C_1 \doteq b.C_1 + \mathbf{1}$$

如果我们考虑图 3 中的确定有限自动机，其 SFM1表示如下：

$$C_2 \doteq a.C_2 + b.C_3 + \mathbf{1}$$
$$C_3 \doteq b.C_3 + a.C_4 + \mathbf{1}$$
$$C_4 \doteq a.C_4 + b.C_4$$

请注意，如果该非确定有限自动机未被约简，那么我们就无法找到表示它的 SFM1 进程。例如，如果我们对图 3 中初始状态为 q_0，的两个自动机取并集，那么 C_0 仅表示左侧的非确定有限自动机。

如果我们考虑图5中的第一个非确定有限自动机，就得到：

$$C_5 \doteq a.C_6 + b.C_5$$
$$C_6 \doteq \mathbf{1}$$

最后，如果我们考虑图5中的第二个非确定有限自动机，就得到：

$$C_7 \doteq a.C_8 + b.C_9$$
$$C_8 \doteq \mathbf{0}$$
$$C_9 \doteq a.C_8 + b.C_9 + \mathbf{1}$$

□

4. 同余

下文中，对于每个 SFM1 进程 p，其关联语言 L(p) 是按照表2中的指称语义计算出的约简非确定有限自动机 $[\![p]\!]_\emptyset$ 所识别的语言。

定义6. 若两个 SFM1 进程 p 和 q 满足 L(p) = L(q)，即它们识别相同的语言，则称它们语言等价，记作 $p \sim q$。□

命题1. 以下结论成立：

1) $L(0) = \emptyset$。

2) $L(1) = \{\varepsilon\}$。

3) 对每个 $p \in \mathscr{P}_{SFM1}$，对于所有 $a \in A$，都有 $L(a.p) = \{aw \mid w \in L(p)\}$。 4) 对每个 $p \in \mathscr{P}_{SFM1}$，都有 $L(\varepsilon.p) = \{\varepsilon w \mid w \in L(p)\} = L(p)$。
5) 对于每个 p、$q \in \mathscr{P}^{grd}{}_{SFM1}$，$L(p + q) = L(p) \cup L(q)$。

证明。由表2中的构造显然可得。 □

现在我们证明，语言等价是所有 SFM1 运算下的同余。

命题2。1）对于每个 p、$q \in \mathscr{P}_{SFM1}$，若 $p \sim q$，则对于所有 $\alpha \in A \cup \{\varepsilon\}$，有 $\alpha.p \sim \alpha.q$。
2）对于每个 p、$q \in \mathscr{P}^{grd}{}_{SFM1}$，若 $p \sim q$，则对于所有 $r \in \mathscr{P}^{grd}{}_{SFM1}$，有 $p + r \sim q + r$。

证明。根据假设，我们知道 $L(p) = L(q)$。于是，待证命题可由应用命题1轻易得出。

现在，对于情况1，$L(\alpha.p) = \{\alpha w \mid w \in L(p)\} = \{\alpha w \mid w \in L(q)\} = L(\alpha.q)$，因此 $\alpha.p \sim \alpha.q$。而对于情况2，$L(p + r) = L(p) \cup L(r) = L(q) \cup L(r) = L(q + r)$，因此 $p + r \sim q + r$。□

注意，对称的情形 $r + p \sim r + q$ 可由选择算子关于 $\sim$ 的交换性推出（见命题3）。

不过，还有一种构造尚未涉及：递归，它仅定义在受限项上。考虑对 SFM1 进行扩展，允许使用变量（例如 x、y……，它们属于句法范畴 p）来构造项：这样便定义了一个“开放”的 SFM1，其语法如下：

$$\begin{array}{lcl} s & ::= & \mathbf{1} \mid \mathbf{0} \mid a.p \mid s + s \\ p & ::= & s \mid C \mid x \end{array}$$

其中，x 的语义是非确定有限自动机 ({x}, /0, /0, /0, x)。

有时，我们使用记号 $p(x_1, \ldots, x_n)$，明确指出项 p 在变量元组 $(x_1, \ldots, x_n)$ 上是开放的。例如，$p_1(x) = a.(b.\mathbf{1} + c.x)$ 和 $p_2(x) = a.c.x + a.b$ 是开放守卫 SFM1 项。类似地，$C_1(x) \doteq a.x$ 明确表示常量 C_1 由一个在 x 上开放的项定义。

开放项 $p(x_1, \ldots, x_n)$ 可以通过如下替换来闭合（另请参见第6节，其中定义了替换应用，也包括进程常量的情况）：

$$p(x_1, \ldots, x_n)\{r_1/x_1, \ldots, r_n/x_n\}$$

其效果是：自由变量 x_i 的每次出现都会被封闭 SFM1 进程 r_i 替换，其中 $i = 1, \ldots, n$。举例来说，$p_1(x)\{d.\mathbf{0}/x\} = a.(b.\mathbf{1} + c.d.0)$，以及 $C_1(x)\{d.\mathbf{0}/x\}$，都是 $C_1 \doteq a.d.0$（也就是说，我们将定义 C_1 主体的开放项 a.x 封闭起来）。开放守卫项上的语言等价 $\sim$ 的一种自然推广如下：若对于所有由封闭 SFM1 项组成的元组 $(r_1, \ldots, r_n)$，都有 $p(x_1, \ldots, x_n) \sim q(x_1, \ldots, x_n)$，

$$p(x_1, \ldots, x_n)\{r_1/x_1, \ldots, r_n/x_n\} \sim q(x_1, \ldots, x_n)\{r_1/x_1, \ldots, r_n/x_n\}.$$

例如，很容易看出 $p_1(x) \sim p_2(x)$。事实上，对于所有 r，都有 $p_1(x)\{r/x\} = a.(b.\mathbf{1} + c.r) \sim a.c.r + a.b.\mathbf{1} = p_2(x)\{r/x\}$；这可以利用 $\sim$的代数性质（见下一节）和同余性质轻松证明。

为简化起见，我们现在将注意力限制在只使用一个未定义变量的开放守卫项上。我们可以借助递归定义的常量，递归地封闭开放项 p(x)。例如，$C \doteq p(x)\{C/x\}$。由此得到的进程常量 C 是一个封闭 SFM1 进程。所谓语言等价是递归的同余，意指如下：若 $p(x) \sim q(x)$，且 $C \doteq p(x)\{C/x\}$，并且 $D \doteq q(x)\{D/x\}$，则 $C \sim D$。下述定理陈述了这一事实。为简化起见，在下文中，只有当上下文不清楚时，才将关于变量 x 开放的项 p 标注为 p(x)，因为我们处理的是实际的项，而不是带标注的项。

注释 2. 在全文中，我们假定，只要常量 C 由 $C \doteq p\{C/x\}$ 定义，开放守卫项 p 就不含 C 的出现，即 $C \notin Const(p)$，因此 $p\{C/x\}$ 中所有 C 的实例都是由将 C 替换为 x 而产生的。此外，我们假定每个常量定义都使用不同的变量，例如 $D \doteq q\{D/y\}$。□

定理 3。设 p 和 q 是两个开放守卫 SFM1 项，且至多含有一个变量 x。令 $C \doteq p\{C/x\}$，$D \doteq q\{D/x\}$，并且 $p \sim q$。则 $C \sim D$。

证明。对于项 p，在 x 上开放后，我们定义以下语言：

- $L_p^{\downarrow} = \{\sigma \in A^* \mid \exists p' \in F.p \stackrel{\sigma}{\Longrightarrow} p'\}$ is the set of the words recognized by p;
- $L_p^x = \{\sigma \in A^* \mid p \stackrel{\sigma}{\Longrightarrow} x\}$ is the set of its maximal words reaching the variable x.

不难看出，对于 $C \doteq p\{C/x\}$，有 $L(C) = (L_p^x)^* \cdot L_p^{\downarrow}$，其中 $\cdot$ 是连接算子，* 是语言 [16] 上的 Kleene 星号算子。

不难看出，$p \sim q$ 当且仅当 $L_p^{\downarrow} = L_q^{\downarrow}$ 且 $L_p^x = L_q^x$，由此可立即得到待证命题 $C \sim D$。□

例 5。考虑 $p_1(x) = a.(b.\mathbf{1} + c.x)$ 和 $p_2(x) = a.c.x + a.b.1$。当然，它们语言等价，且确有 $L_{p_1}^{\downarrow} = \{ab\} = L_{p_2}^{\downarrow}$ 和 $L_{p_1}^x = \{ac\} = L_{p_2}^x$。若考虑 $C \doteq p_1\{C/x\}$ 和 $D \doteq p_2\{D/x\}$，则可得 $C \sim D$，因为二者都识别正则语言 $(ac)^*ab$。□

将其推广到由变量 $\{x1,\ldots, x_n\}$ 构成的集合上的开放项，是显而易见的。考虑一组形如以下形式的等价开放项对：

$$
\begin{aligned}
&p_1(x_1,\ldots,x_n) \sim q_1(x_1,\ldots,x_n)\\
&p_2(x_1,\ldots,x_n) \sim q_2(x_1,\ldots,x_n)\\
&\ldots\\
&p_n(x_1,\ldots,x_n) \sim q_n(x_1,\ldots,x_n)
\end{aligned}
$$

其中，对于 $i = 1,\ldots, n$，当且仅当 $L_{p_i}^{\downarrow} = L_{q_i}^{\downarrow}$ 且 $L^{x_j}{}_{p_i} = L^{x_j}{}_{q_i}$ 对于 $j = 1,\ldots, n$ 时，$p_i(x1,\ldots, x_n) \sim q_i(x1,\ldots, x_n)$。然后，我们可以递归地闭包这些项，如下所示：

$$C_1 \doteq p_1\{C_1/x_1,\ldots,C_n/x_n\} \qquad D_1 \doteq q_1\{D_1/x_1,\ldots,D_n/x_n\}$$
$$C_2 \doteq p_2\{C_1/x_1,\ldots,C_n/x_n\} \qquad D_2 \doteq q_2\{D_1/x_1,\ldots,D_n/x_n\}$$
$$\ldots$$
$$C_n \doteq p_n\{C_1/x_1,\ldots,C_n/x_n\} \qquad D_n \doteq q_n\{D_1/x_1,\ldots,D_n/x_n\}$$

那么，待证命题是：对于所有 $i = 1, 2, \ldots, n$，$C_i \sim D_i$。

最后，我们来谈谈第2节中定义的几种较为具体的等价关系。同构等价是最具体的一种，但它对于选择算子并不是同余。例如，$a.1$ 生成的非确定有限自动机与 $a.(\mathbf{1}+\mathbf{0})$ 生成的非确定有限自动机同构；然而，如果考虑上下文 $+a.1$，就会得到两个生成非确定有限自动机不同构的项：$a.\mathbf{1}+a.1$ 生成一个两状态非确定有限自动机，而 $a.(\mathbf{1}+\mathbf{0})+a.1$ 生成一个三状态非确定有限自动机。相反，可以通过标准证明技巧（例如，参见 [22, 11, 4, 28, 14]）证明，双模拟等价 $\simeq$（它严格细于语言等价 $\sim$）对于 SFM1 的所有算子都是同余。

5. 代数性质

现在我们列出语言等价的一些代数性质，并讨论它们是否也适用于双模拟等价或同构等价。

命题3。（选择算子定律）对于每个 $p,q \in \mathscr{P}^{grd}{}_{SFM}1$，以下结论成立：

$$\begin{array}{rcll} p+(q+r) & \sim & (p+q)+r & \text{(associativity)} \\ p+q & \sim & q+p & \text{(commutativity)} \\ p+\mathbf{0} & \sim & p & \text{(identity)} \\ p+p & \sim & p & \text{(idempotency)} \end{array}$$

证明。证明可直接由命题1(5)得出。例如，$p+q \sim q+p$ 成立，因为 $L(p+q) = L(p) \cup L(q) = L(q) \cup L(p) = L(q+p)$。□

选择算子定律对双模拟等价也成立 [22, 11, 4, 28], ，但对同构等价并不成立。例如，考虑 $p = a.A$，其中 $A \doteq a.(b.B + a.A)$，以及 $q = b.B$，其中 $B \doteq b.B + \mathbf{1}$；那么很容易看出，$p+q$ 对应的非确定有限自动机（四个状态）与 $q+p$ 对应的非确定有限自动机（三个状态）不同构。

命题 4。（前缀算子定律）对于每个 $p, q \in \mathscr{P}^{grd}{}_{SFM}1$、每个 $r \in \mathscr{P}_{SFM1}$、每个 $\alpha \in A \cup \{\varepsilon\}$，以下结论成立：

$$\begin{array}{rcll} \alpha.\mathbf{0} & \sim & \mathbf{0} & \text{(annihilation)} \\ \alpha.(p+q) & \sim & \alpha.p+\alpha.q & \text{(distributivity)} \\ \varepsilon.r & \sim & r & \text{(}\varepsilon\text{-absorption)} \end{array}$$

证明。该证明可由命题1直接得出。定律 $\alpha.\mathbf{0} \sim \mathbf{0}$ 成立，因为 L(α.**0** ={α | ∈ **0** }={α | ∈0}=0= **0** α. + ∼α. +) w w L( ) w w / / L( )。定律 (p q) p q 成 α. α. + ={α | ∈ + }={α | ∈ ∪ 立，因为 L((p q)) w w L(p q) w w L(p) L(q) } = {α | ∈ }∪{α | ∈ }= α. ∪ α. = α. +α. w w L(p) w w L(q) L(p) L(q) L(p q)。

定律 $\varepsilon.r \sim r$ 成立，因为 $L(\varepsilon.r) = \{\varepsilon w \mid w \in L(r)\} = \{w \mid w \in L(r)\} = L(r)$。□

很容易看出，前缀定律对于互模拟等价都不成立，因此对于同构等价也不成立。

现在我们聚焦于常量的性质。首先是展开律（它对双模拟等价也成立），然后是剔除律（可用于移除 ε 转移形成的循环），最后在下一小节讨论折叠律，其证明依赖一些辅助技术工具（完备格上的不动点定理，参见例如 [8, 28]）。

命题 5。（展开）对于每个 $\mathrm{p} \in \mathscr{P}^{grd}{}_{SFM}\mathbf{1}$ 和每个 $\mathrm{C} \in \mathscr{C}$，若 $\mathrm{C} \doteq \mathrm{p}$，则 $\mathrm{C} \sim \mathrm{p}$。

证明。由表2中的构造可知，结论显然成立。 □

展开律对双模拟等价也成立 [22, 11, 13], , 但对同构等价并不成立。例如，考虑 $\mathrm{C} \doteq \mathrm{a.a.C} + \mathbf{1}$：容易看出，C 的非确定有限自动机有两个状态，而 $\mathrm{a.a.C} + \mathbf{1}$ 的非确定有限自动机有三个状态。

注 3. 命题4中的 ε-吸收律最好拆分为两个独立的定律：

(i) $\varepsilon.p \sim p$ if $p \neq C$, and

(ii) $\varepsilon.C \sim p$ if $C \doteq p$,

其中第二个定律可由第一个定律和展开律推导得出。事实上，若 $\mathrm{C} \doteq \mathrm{p}$，则根据展开律有 $\mathrm{C} \sim \mathrm{p}$；接着，根据同余，有 $\varepsilon.\mathrm{C} \sim \varepsilon.\mathrm{p}$；再根据第一个定律，有 $\varepsilon.\mathrm{p} \sim \mathrm{p}$，因此根据传递性可得等式 $\varepsilon.\mathrm{C} \sim \mathrm{p}$。

与命题 4 中更一般的 ε-吸收律相比，第一个定律 (i) 的优点在于它保持守卫性；例如，若 $\mathrm{C} \doteq \varepsilon.\mathrm{D} + \mathbf{1}$ 且 $\mathrm{D} \doteq \mathrm{a}.\mathbf{1}$，则通过使用（展开律和）更一般的定律，我们可以推导出 $\mathrm{C} \sim \mathrm{D} + \mathbf{1}$，其中右侧不是守卫项；相反，通过使用（递归同余和）(i)，我们可以推导出 $\mathrm{C} \sim \mathrm{a}.\mathbf{1} + \mathbf{1}$，其中右侧是守卫项。□

命题 6。（切除）对于每个 $\mathrm{p} \in \mathscr{P}^{grd}{}_{SFM}\mathbf{1}$，以及每个 $\mathrm{C,D} \in \mathscr{C}$，如果 $\mathrm{C} \doteq (\varepsilon.\mathrm{x} + \mathrm{p})\{\mathrm{C}/\mathrm{x}\}$ 且 $\mathrm{D} \doteq \mathrm{p}\{\mathrm{D}/\mathrm{x}\}$，那么 $\mathrm{C} \sim \mathrm{D}$。

证明。显然，因为带有 ε 标签的自环转移不会促成任何词的生成。□

当然，剔除律不适用于双模拟等价，因此甚至也不适用于同构等价。

5.1. 折叠律

为了证明折叠律，我们首先注意到（$\mathscr{P}(\mathrm{A}^*) \subseteq$）是一个完备格，即具有如下性质：$\mathscr{P}(\mathrm{A}^*)$ 的所有子集（例如 $\{\mathrm{L}_i\}_{i\in I}$）都有上确界（即 $\bigcup_{i\in I}\mathrm{L}_i$）和下确界（即 $\bigcap_{i\in I}\mathrm{L}_i$），其最大元 $\top$ 是 A^*，最小元 $\bot$ 是 $/0$。

粗略地说，折叠律指出，若 $\mathrm{C} \doteq \mathrm{p}\{\mathrm{C}/\mathrm{x}\}$ 且 $\mathrm{q} \sim \mathrm{p}\{\mathrm{q}/\mathrm{x}\}$，则 $\mathrm{C} \sim \mathrm{q}$。当然，我们很容易发现，$\mathrm{L(C)} = \mathrm{L}_p^{\downarrow} \cup (\mathrm{L}_p^x \cdot \mathrm{L(C)})$，并且 $\mathrm{L(q)} = \mathrm{L}_p^{\downarrow} \cup (\mathrm{L}_p^x \cdot \mathrm{L(q)})$。因此，L(C) 和 L(q) 都是映射

		$a \in A$			
		og(p)	og(p) $C \doteq p\{C/x\}$	og(p) og(q)	
og(0)	og(1)	og(a.p)	og(ε.p)	og(C)	og(p + q)

表 3：观察守卫谓词

T (W) $= L_p^{\downarrow} \cup (L_p^x \cdot W)$ 的不动点。我们要证明，在一个温和的条件下，T 恰好有一个不动点，因此 L(C) = L(q)，从而 C $\sim$ q，正如所需。

如果映射 T 是连续的（即，对于所有递增序列 $L_0 \subseteq L_1 \subseteq L_2 \ldots$，我们都有 T ($\bigcup_i L_i$) = $\bigcup_i$ T (L_i)），那么最小不动点 lfp(T) = $\bigcup_{n \geq 0}$T n(/0)，其中 T ^{0}(L) = L，且 T n^{+1}(L) = T (T n(L))。事实上，T 是连续的，因为 T ($\bigcup_i L_i$) = $L_p^{\downarrow} \cup (L_p^x \cdot \bigcup_i L_i) = L_p^{\downarrow} \cup \bigcup_i (L_p^x \cdot L_i)$ = $\bigcup_i (L_p^{\downarrow} \cup (L_p^x \cdot L_i))$ = $\bigcup_i$ T (L_i)。最小不动点 lfp(T) = $\bigcup_{n \geq 0}$T n(/0) 可按如下方式计算：

$$
\begin{aligned}
T^0(\emptyset) &= \emptyset \\
T^1(\emptyset) &= L_p^{\downarrow} \\
T^2(\emptyset) &= L_p^{\downarrow} \cup (L_p^x \cdot L_p^{\downarrow}) \\
T^3(\emptyset) &= L_p^{\downarrow} \cup (L_p^x \cdot L_p^{\downarrow}) \cup (L_p^x \cdot (L_p^{\downarrow} \cup (L_p^x \cdot L_p^{\downarrow})) = L_p^{\downarrow} \cup (L_p^x \cdot L_p^{\downarrow}) \cup L_p^x \cdot (L_p^x \cdot L_p^{\downarrow}) \\
&\ldots
\end{aligned}
$$

其并集就是语言 lfp(T) = $(L_p^x)^* \cdot L_p^{\downarrow}$。

对偶地，若 T 是余连续的（也就是说，对于所有递减序列 $L_0 \supseteq L_1 \supseteq L_2 \ldots$，都有 T ($\bigcap_i L_i$) = $\bigcap_i$ T (L_i)），则最大不动点 gfp(T) = $\bigcap_{n \geq 0}$T n(A^*)。事实上，T 是余连续的，因为 T ($\bigcap_i L_i$) = $L_p^{\downarrow} \cup (L_p^x \cdot \bigcap_i L_i) = L_p^{\downarrow} \cup \bigcap_i (L_p^x \cdot L_i) = \bigcap_i (L_p^{\downarrow} \cup (L_p^x \cdot L_i))$ = $\bigcap_i$ T (L_i)。最大不动点 gfp(T) = $\bigcap_{n \geq 0}$T n(A^*) 可按如下方式计算：

$$
\begin{aligned}
T^0(A^*) &= A^* \\
T^1(A^*) &= L_p^{\downarrow} \cup (L_p^x \cdot A^*) \\
T^2(A^*) &= L_p^{\downarrow} \cup (L_p^x \cdot (L_p^{\downarrow} \cup (L_p^x \cdot A^*)) = L_p^{\downarrow} \cup (L_p^x \cdot L_p^{\downarrow}) \cup L_p^x \cdot (L_p^x \cdot A^*) \\
T^3(A^*) &= L_p^{\downarrow} \cup (L_p^x \cdot (L_p^{\downarrow} \cup (L_p^x \cdot L_p^{\downarrow}) \cup L_p^x \cdot (L_p^x \cdot A^*)) = \\
&\quad L_p^{\downarrow} \cup (L_p^x \cdot L_p^{\downarrow}) \cup L_p^x \cdot (L_p^x \cdot L_p^{\downarrow}) \cup L_p^x \cdot (L_p^x \cdot (L_p^x \cdot A^*)) \\
&\ldots
\end{aligned}
$$

它们的交集是语言 gfp(T) = $(L_p^x)^* \cdot L_p^{\downarrow}$，除非 L_p^x 包含空词 ε，因为在这种情况下，应用 T 不会限制新计算出的语言，因此对于所有 n ≥ 0，都有 $T^n(A^*) = A^*$，所以 T 的最大不动点就是完备格的最大元 A^*。我们可以用语法方式刻画这一条件如下。

定义 7.（观察守卫的）如果 og(p) 成立，则称（可能开放的）SFM1 进程 p 是观察守卫的；其中 og(–) 定义为由公理和表 3 中的规则生成的最小谓词。□

注意，C $\doteq$ p{C/x} 是观察守卫的，当且仅当 C $\stackrel{\varepsilon}{\not\Rightarrow}$C，或者等价地——

当且仅当 $p \overset{\varepsilon}{\nRightarrow} x$，也就是说，当且仅当 $\varepsilon \notin L_p^x$。

命题 7。（折叠）对于每个在 x 上开放的 $p \in \mathscr{P}^{grd}{}_{SFM}1$，以及每个 $C \in \mathscr{C}$，若 $C \doteq p\{C/x\}$，且 og(p)，并且 $q \sim p\{q/x\}$，则 $C \sim q$。

证明。若 p 是观察守卫的，则函数 $T(W) = L_p^{\downarrow} \cup (L_p^x \cdot W)$ 的最小不动点和最大不动点确实重合，因此不动点是唯一的。由于 L(C) 和 L(q) 都是 T 的不动点，因此 $L(C) = L(q)$。□

请注意，要求 p 是观察守卫的，这对折叠性质的正确性至关重要。例如，考虑 $p = \varepsilon.x + a.1$，它不是观察守卫的。那么，$C \doteq \varepsilon.C + a.1$ 定义了一个只能识别 a 的进程，因此它与 a.1 语言等价。然而，$q = a.1 + b.1$ 满足 $q \sim \varepsilon.q + a.1$，但 $C \not\sim q$。

注 4.（双模拟等价的折叠律）使用基于双模拟的标准证明技巧 [20, 13], ，可以证明，更具体的双模拟等价 $\simeq$ 满足更强的折叠律：对于每个 $p \in \mathscr{P}^{grd}{}_{SFM}1$（在 x 上开放），以及每个 $C \in \mathscr{C}$，若 $C \doteq p\{C/x\}$ 且 $q \simeq p\{q/x\}$，则 $C \simeq q$。□

6. 带进程常量的等式推导 nts

下文将说明，如何通过句法方式，即借助等式推导证明，证明两个 SFM1 进程识别相同的语言。首先，本节介绍如何在带进程常量的进程代数中实现等式推导；接着，下一节将为观测守卫的 SFM1 进程的语言等价给出一个可靠且完备的公理化，其中包含 7 条公理和 2 条条件公理；最后，我们将说明，借助一条额外的条件公理，每个观察非受保护进程都可以等式化为一个观测守卫的进程。因此，SFM1 上语言等价的有限公理化仅由 7 条公理和 3 条条件公理组成。现在先简要介绍等式推导。

给定一个（单排序）签名 Σ（即一个有限的常量集、一个有限的进程常量集，以及一个带有各自元数的有限函数符号集），我们可以定义由 Σ 和有限变量集 V 构成的项集（记作 $\mathscr{T}(\Sigma,V)$），它是满足以下条件的最小集合：

(i) V 中的每个变量 x 都是 $\mathscr{T}(\Sigma,V)$ 中的一个项；

(ii) Σ 中的每个常量 c 都是 $\mathscr{T}(\Sigma,V)$ 中的一个项；(iii) Σ 中的每个进程常量 C 都是 $\mathscr{T}(\Sigma,V)$ 中的一个项；此外，每个常量 C 都必须配有一个定义，例如 $C \doteq t$，其中 t 是 $\mathscr{T}(\Sigma,V)$ 中的一个项；(iv) 如果 f 是一个 n 元函数符号，且 $t1,\ldots,t_n$ 是 $\mathscr{T}(\Sigma,V)$ 中的项，那么 $f(t1,\ldots,t_n)$ 也是 $\mathscr{T}(\Sigma,V)$ 中的一个项。

此外，我们有 $\mathscr{T}(\Sigma)$ 表示闭项（或基项）的集合，其中当满足以下条件时，项 t 属于 $\in \mathscr{T}(\Sigma)$：

- t 中不存在变量出现
- $\forall C \in \mathrm{Const(t)}$，如果 $C \doteq p$，那么 $p \in \mathscr{T}(\Sigma)$。

这个定义显然是递归的，但这并不是问题，因为我们可以像在 SFM1 的指称语义中那样，通过跟踪已经遇到的进程常量来定义它。

替换 ρ 是从 V 到 $\mathscr{T}(\Sigma,V)$ 的映射。对于任意项 t，我们用 $t[\rho]$ 表示按如下方式得到的项：

(i) 对于 V 中的每个变量 x，$x[\rho] = \rho(x)$，

(ii) 对于 Σ 中的每个常量 c，$c[\rho] = c$，

(iii) 对于 Σ 中满足 $C \doteq t$ 的每个进程常量 C，$C[\rho] = C$，其中 $C \doteq t[\rho]$

(iv) 对于任意 n 元函数符号 f 和项 $t1,\ldots,t_n$，$f(t1,\ldots,t_n)[\rho]$ 是项 $f(t_1[\rho],\ldots,t_n[\rho])$。

若对于每个变量 $x \in V$，替换 ρ 都满足 $\rho(x) \in \mathscr{T}(\Sigma)$，则称其为闭替换。因此，将闭替换应用于开放项会得到闭项（或基项）。

备注 5。我们的开放 SFM1 语言的（一排序）签名 Σ 如下：

- 变量：$x \in$Var（其中 Var 是有限的）；
- 两个常量：1 和 0；
- 进程常量：$C \in \mathscr{C}$（其中 $\mathscr{C}$ 是有限的）；
- 算子：
  - $\alpha.\_$（一族有限的前缀算子，每个 $\alpha \in A \cup \{\varepsilon\}$ 对应一个），
  - $\_+\_$（一个二元选择组合算子）。

这意味着，在本节中，开放 SFM1 的句法定义仅通过以下一种句法范畴给出：

$$p ::= \mathbf{1} \mid \mathbf{0} \mid \alpha.p \mid p+p \mid C \mid x$$

从而可以写出诸如 $x+(y+z)$ 这样的项，而这些项无法用第 4 节开放 SFM1 的语法来描述。□

1.	自反性	$\dfrac{}{t = t}$	
2.	对称性	$\dfrac{t_1 = t_2}{t_2 = t_1}$	
3.	传递性	$\dfrac{t_1 = t_2 \; t_2 = t_3}{t_1 = t_3}$	
4.1	替换性	$\dfrac{t_i = t_i'}{f(t_1,\ldots t_i,\ldots t_k) = f(t_1,\ldots t_i',\ldots t_k)}$	对于任意 f 和 $1 \le i \le n$
4.2	递归	$\dfrac{t_1 = t_2 \wedge C \doteq t_1\{C/x\} \wedge D \doteq t_2\{D/x\}}{C = D}$	
5.	实例化	$\dfrac{t_1 = t_2}{t_1[\rho] = t_2[\rho]}$	对于任意替换 ρ
6.	公理	$\dfrac{}{t_1 = t_2}$	对所有公理 $t_1 = t_2$，均属于 E

表 4：等式推导规则

等式理论是一个元组 (Σ,E)，其中 Σ 是一个签名，E 是一组形式为 $t_1 = t_2$，的方程，其中 t_1 和 t_2 是 $\mathscr{T}(\Sigma,V)$ 中的项。E 中的方程通常称为公理，而等式理论 (Σ,E) 通常称为公理化。

对于任意等式理论 (Σ,E)，都有一组标准的证明规则，用于在 $\mathscr{T}(\Sigma,V)$ 上推导等式。这组证明规则构成等式演绎证明系统 D(E)，由表 4 中的规则组成。

证明是一个有限的等式序列 $t_1 = t_1', t_2 = t_2', \ldots t_k = t_k'$，其中每个 $t_i = t_i'$要么是公理（规则 1 或 6），要么可通过使用规则 $2-5$之一推导得出，其前提是前面某些等式 $t_1 = t_1', t_2 = t_2', \ldots t_{i-1} = t_{i-1}'$。这种证明的线性表示可以更方便地用树的形式表达（证明树）。

我们使用记号 $E \vdash t_1 = t_2$，表示存在一个证明，其最后一个等式为 $t_1 = t_2$，且只使用 E 中的公理（以及规则 1 中的公理）。这直接确定了项集上的一个同余：当且仅当 $E \vdash t_1 = t_2$ 时，$t_1 =_E t_2$。事实上，注意规则 $1-3$ 确保 D(E) 在 $\mathscr{T}(\Sigma,V)$ 上所诱导的关系 $=_E$ 是一个等价关系；类似地，规则 4.1 和 4.2 确保在任意上下文中都满足等量代换，即 D(E) 所诱导的关系 $=_E$ 是一个同余。

令 $S \subseteq \mathscr{T}(\Sigma)$ 为我们感兴趣的项集（我们可以认为 S 是 $\mathscr{P}_{SFM1}$SFM1 进程的集合，它包含于更大的所有闭项集合中，而后者属于

备注 5 中开放 SFM1 的语法）。

设 R $\subseteq$ S $\times$S 是定义在封闭（或基）项上的关系。对于等式理论 (Σ, E)，若等式演绎证明系统 D(E) 关于 R 是（基）可靠的，则

$$\forall (t_1, t_2) \in S \times S, \quad E \vdash t_1 = t_2 \ \text{ implies } \ (t_1, t_2) \in R.$$

若 D(E) 关于 R 是（基）完备的，则

$$(t_1, t_2) \in R \ \text{ implies } \ E \vdash t_1 = t_2.$$

换言之，若 (Σ,E) 是 S $\subseteq \mathscr{T}(\Sigma)$ 上同余关系 R 的可靠且完备的公理化，那么 D(E) 在 S 上诱导的同余 $t_1 =_E t_2$ 与 R 所定义的同余完全相同。

7. 公理化

本节将给出 SFM1 上语言等价的一个有限的可靠且完备的公理化。正如上一节所提示的（参见备注 5），为求简洁，开放 SFM1 的句法定义仅采用一个句法范畴，但公理的每个基实例化都必须遵循第 4 节给出的 SFM1 句法定义；这意味着我们可以写出公理 x + (y + z) =(x + y) + z，但不能将其实例化为 C + (a.**1** + b.1) =(C + a.1) + b.1，因为这些并非合法的 SFM1 进程（常量 C 不能用作加项）。

7.1. 公理

公理集合列于表 5 中。公理 A1-A4 是选择的通常公理 [17, 27, 18, 20]。公理模式 T1-T3 是前缀的公理模式，由于 A 是有限集，这些公理模式也是有限的。注意，T3 带有附加条件 x $\neq$C，这意味着只有在 x 未被实例化为进程常量时才能使用它：这是保持常量守卫性所必需的（见注释 3）。条件公理 R1-R3 与进程常量有关，并且类似于 [20, 21, 13, 14] 中的公理。注意，这些条件公理实际上是一个有限的公理集合，每个常量定义对应一个公理：由于进程常量的集合 $\mathscr{C}$ 是有限的，R1-R3 的实例也同样是有限的。

折叠公理 R2 与这个由 Arden [2] 和 Salomaa [27] 提出的“迭代”条件公理有一些相似之处：

$$x = (y \cdot x) + z \ \Rightarrow \ x = y^* z,$$

前提是 y 不具有空字性质（简称 ewp），即 ε $\notin$ L(y)。Kozen [18] 认为，这条条件公理不是代数性的，因为它在替换下不保持不变。R2 的附加条件 og(p)（等价于 $\varepsilon \notin \mathrm{L}_p^x$）实质上是否定 ewp 性质。不过，条件公理 R2 是代数性的，因为项 p 是一个具体项（而不是变量），其具体形式取决于常量 C 的定义。切除公理 R3 与 Salomaa 在 [27], 提出的一条定律有些相似，即 $(\mathrm{x} + \mathbf{1})^* = \mathrm{x}^*$。

除了折叠公理 R2，我们还考虑一种更强的变体，称为 R2′，其中省略了附加条件 og(p)：

A1	结合律	$x+(y+z)$	$=$	$(x+y)+z$	
A2	交换律	$x+y$	$=$	$y+x$	
A3	单位元	$x+\mathbf{0}$	$=$	x	
A4	幂等性	$x+x$	$=$	x	
T1	消去律	$\alpha.\mathbf{0}$	$=$	$\mathbf{0}$	
T2	分配律	$\alpha.(x+y)$	$=$	$\alpha.x+\alpha.y$	
T3	ε-吸收	$\varepsilon.x$	$=$	x	若 $x \neq C$
R1	展开	if $C \doteq p$		then	$C=p$
R2	折叠	if $C \doteq p\{C/x\} \wedge og(p) \wedge q = p\{q/x\}$		then	$C=q$
R3	切除	if $C \doteq (\varepsilon.x+p)\{C/x\} \wedge D \doteq p\{D/x\}$		then	$C=D$

表 5：语言等价的公理

R2′ (B-Folding) if $C \doteq p\{C/x\} \wedge q = p\{q/x\}$ then $C = q$

该变体对双模拟等价 [20, 13] 成立。

我们将 B 称为由公理 {A1、A2、A3、A4、R1、R2′} 组成的集合，这些公理对于双模拟等价是可靠且完备的；而将 W_g 称为由公理 {A1、A2、A3、A4、T1、T2、T3、R1、R2} 组成的集合。我们将证明，该集合构成了观测守卫的 SFM1 进程的语言等价的可靠且完备的公理化，而 $W = W_g \cup \{R3\}$ 则是整个 SFM1 上语言等价的完整公理化。记号 $W \vdash p = q$ 表示存在一个等式推导证明，使用 W 中的公理推导出等式 $p = q$。

定理 4。（可靠性）对于任意 $p、q \in \mathscr{P}_{SFM1}$，若 $W \vdash p = q$，则 $p \sim q$。

证明。证明采用对 $W \vdash p = q$ 的证明进行归纳。通过观察可得待证命题：W 中的所有公理都是可靠的（例如，T1-T3 由命题 4 得证），且 $\sim$ 是同余。□

7.2. 范式、唯一解与 ε-自由范式

若谓词 $n\,f\,(p)$ 成立，则 SFM1 进程 p 是范式。该谓词表示 $n\,f\,(p, /0)$，其归纳定义见表 6。不属于范式的项例如 $a.b.1$ 和 $C \doteq a.b.C + \mathbf{1}$。

注意，若 C 是范式，则其主体（忽略所有可能出现的加项 0 或重复加项 1，这些加项可通过公理 A3-A4 吸收）形式为 $\sum_{i=1}^{n} \alpha_i.C_i$ 或 $\sum_{i=1}^{n} \alpha_i.C_i + \mathbf{1}$（假设若 $n = 0$，则 $\sum_{i=1}^{n} \alpha_i.C_i$ 为 0）；其中，每个 C_i 又都是范式。事实上，根据定理 2 证明中的构造，表示约化的非确定有限自动机的进程都是范式。

现在我们证明，对于每个 SFM1 进程 p，都存在一个范式 q，使得 $B \vdash p = q$。由于双模拟等价细于语言等价，这保证了范式 q 与 p 语言等价。

$\frac{}{\mathrm{nf}(1,\mathrm{I})}$	$\frac{}{\mathrm{nf}(0,\mathrm{I})}$	$\frac{\text{非确定有限自动机的代数}\quad C \doteq p \quad \mathrm{C} \notin \mathrm{I}}{\mathrm{nf}(\mathrm{C},\mathrm{I})}$
$\frac{\mathrm{nf}(\mathrm{C},\mathrm{I})}{\mathrm{nf}(\alpha.\mathrm{C},\mathrm{I})}$	$\frac{\mathrm{nf}(\mathrm{p},\mathrm{I}) \quad \mathrm{nf}(\mathrm{q},\mathrm{I})}{\mathrm{nf}(\mathrm{p}+\mathrm{q},\mathrm{I})}$	$\frac{\mathrm{C} \in \mathrm{I}}{\mathrm{nf}(\mathrm{C},\mathrm{I})}$

表 6：范式谓词

命题8。（归约至范式）给定一个 SFM1 进程 p，存在一个范式 q，使得 $\mathrm{B} \vdash \mathrm{p} = \mathrm{q}$。

证明。我们对 p 的结构作归纳法，同时约定使用集合 I 来记录已经扫描过的常量，以避免递归定义的常量导致循环，其中 I 初始为空。我们证明，对于 (p, I)，存在一个项 q，使得 $\mathrm{nf}(\mathrm{q}, \mathrm{I})$ 成立，且 $(\mathrm{B}, \mathrm{I}) \vdash \mathrm{p} = \mathrm{q}$；这表示：当假设每个满足 $\mathrm{C} \in \mathrm{I}$ 的常量都只与自身相等时，可以由 B 中的公理推导出等式 $\mathrm{p} = \mathrm{q}$。考察 $(\mathrm{p}, /0)$ 即可得到待证命题。

第一个基例是 $(1, \mathrm{I})$；此时 $\mathrm{q} = \mathbf{1}$，因为 $\mathrm{nf}(1,\mathrm{I})$ 成立，而待证命题 $(\mathrm{B}, \mathrm{I}) \vdash \mathbf{1} = \mathbf{1}$ 可由自反性得出。第二个基例是 $(0,\mathrm{I})$，与前一个类似。

情形（$\alpha.\mathrm{p}, \mathrm{I}$）：根据归纳法，$(\mathrm{p}, \mathrm{I})$ 有一个与之对应的范式 $\mathrm{nf}(\mathrm{q}, \mathrm{I})$，使得 $(\mathrm{B}, \mathrm{I}) \vdash \mathrm{p} = \mathrm{q}$；因此，根据替换性，$(\mathrm{B}, \mathrm{I}) \vdash \alpha.\mathrm{p} = \alpha.\mathrm{q}$。若 q 是常量，则 $\alpha.\mathrm{q}$ 已经是一个范式。否则，取一个新的常量 $\mathrm{C} \doteq \mathrm{q}$，使得 $\mathrm{nf}(\mathrm{C}, \mathrm{I})$ 成立，因为 $\mathrm{nf}(\mathrm{q}, \mathrm{I} \cup \{\mathrm{C}\})$ 成立（注意，C 不出现在 q 中，因此这等同于 $\mathrm{nf}(\mathrm{q}, \mathrm{I})$，而后者根据归纳法成立）。所需的范式是 $\alpha.\mathrm{C}$。事实上，$\mathrm{nf}(\alpha.\mathrm{C}, \mathrm{I})$ 成立，因为 $\mathrm{nf}(\mathrm{C}, \mathrm{I})$ 成立；此外，由于根据归纳法有 $(\mathrm{B}, \mathrm{I}) \vdash \mathrm{p} = \mathrm{q}$，且根据公理 R1 有 $(\mathrm{B}, \mathrm{I}) \vdash \mathrm{C} = \mathrm{q}$，我们根据传递性可得 $(\mathrm{B}, \mathrm{I}) \vdash \mathrm{p} = \mathrm{C}$，因此根据替换性，$(\mathrm{B}, \mathrm{I}) \vdash \alpha.\mathrm{p} = \alpha.\mathrm{C}$。

情况 $(\mathrm{p}_1 + \mathrm{p}_2, \mathrm{I})$：根据归纳法，我们可以假设对于 $(\mathrm{p}_i, \mathrm{I})$，存在一个范式 $\mathrm{nf}(\mathrm{q}_i, \mathrm{I})$，使得 $(\mathrm{B}, \mathrm{I}) \vdash \mathrm{p}_i = \mathrm{q}_i \text{for i} = 1,2$。于是，$\mathrm{nf}(\mathrm{q}_1 + \mathrm{q}_2, \mathrm{I})$ 成立，并且根据替换性，$(\mathrm{B}, \mathrm{I}) \vdash \mathrm{p}_1 + \mathrm{p}_2 = \mathrm{q}_1 + \mathrm{q}_2$。

情况 (C, I)，其中 $\mathrm{C} \doteq \mathrm{r}\{\mathrm{C}/\mathrm{x}\}$。如果 $\mathrm{C} \in \mathrm{I}$，那么我们可以返回 C 本身来终止归纳：$\mathrm{nf}(\mathrm{C}, \mathrm{I})$ 成立，并且根据自反性，$(\mathrm{B}, \mathrm{I}) \vdash \mathrm{C} = \mathrm{C}$。否则（即，如果 $\mathrm{C} \notin \mathrm{I}$），根据 $(\mathrm{r}\{\mathrm{C}/\mathrm{x}\}, \mathrm{I} \cup \{\mathrm{C}\})$ 进行归纳，我们可以假设存在一个范式 $\mathrm{q}\{\mathrm{C}/\mathrm{x}\}$，使得 $\mathrm{nf}(\mathrm{q}\{\mathrm{C}/\mathrm{x}\}, \mathrm{I} \cup \{\mathrm{C}\})$ 成立，并且 $(\mathrm{B}, \mathrm{I} \cup \{\mathrm{C}\}) \vdash \mathrm{r}\{\mathrm{C}/\mathrm{x}\} = \mathrm{q}\{\mathrm{C}/\mathrm{x}\}$。注意，根据构造，如果 $(\mathrm{B}, \mathrm{I} \cup \{\mathrm{C}\}) \vdash \mathrm{r}\{\mathrm{C}/\mathrm{x}\} = \mathrm{q}\{\mathrm{C}/\mathrm{x}\}$，那么也有 $(\mathrm{B}, \mathrm{I}) \vdash \mathrm{r}\{\mathrm{C}/\mathrm{x}\} = \mathrm{q}\{\mathrm{C}/\mathrm{x}\}$。因此，由于根据公理 R1，$(\mathrm{B}, \mathrm{I}) \vdash \mathrm{C} = \mathrm{r}\{\mathrm{C}/\mathrm{x}\}$，可由传递性得出 $(\mathrm{B}, \mathrm{I}) \vdash \mathrm{C} = \mathrm{q}\{\mathrm{C}/\mathrm{x}\}$。然后，我们取一个新的常量 $\mathrm{D} \doteq \mathrm{q}\{\mathrm{D}/\mathrm{x}\}$，使得 $\mathrm{nf}(\mathrm{D}, \mathrm{I})$ 成立，因为 $\mathrm{nf}(\mathrm{q}\{\mathrm{D}/\mathrm{x}\}, \mathrm{I} \cup \{\mathrm{D}\})$ 成立。因此，根据公理 R2′，$(\mathrm{B}, \mathrm{I}) \vdash \mathrm{C} = \mathrm{D}$，其中 D 是一个范式。□

推论 2。（化为观察守卫范式）给定一个观察守卫的 SFM1 进程 p，存在一个观察守卫范式 q，使得 $\mathrm{W}_g \vdash \mathrm{p} = \mathrm{q}$。

证明。证明与前一个命题的证明非常相似。我们证明，对于满足 og(p) 的 (p, I)，存在一个项 q，使得 n f (q,I) 和 og(q) 成立，并且 $(W_{\mathcal{S}}, I) \vdash p = q$；这里的意思是，当假设每个常量 $C \in I$ 都等于其自身时，可以由 $W_{\mathcal{S}}$ 中的公理推导出等式 $p = q$。然后，考虑 (p, /0)，即可得到待证命题。

除递归的情形外，所有情形都只是对上述相应情形的简单改写。

情形 (C, I)，其中 $C \doteq r\{C/x\}$ 且 og(C) 成立。若 $C \in I$，则可停止归纳，直接返回 C：n f (C, I) 成立，并且根据自反性，$(W_{\mathcal{S}}, I) \vdash C = C$。否则（即若 $C \notin I$），根据 $(r\{C/x\}, I \cup \{C\})$ 且 og(r) 成立进行归纳，我们可以假设存在一个范式 $q\{C/x\}$，使得 n f $(q\{C/x\}, I \cup \{C\})$ 和 og(q) 成立；此外，$(W_{\mathcal{S}}, I \cup \{C\}) \vdash r\{C/x\} = q\{C/x\}$。注意，根据构造，若 $(W_{\mathcal{S}}, I \cup \{C\}) \vdash r\{C/x\} = q\{C/x\}$，则 $(W_{\mathcal{S}}, I) \vdash r\{C/x\} = q\{C/x\}$ 也成立。因此，由于根据公理 R1，$(W_{\mathcal{S}}, I) \vdash C = r\{C/x\}$，根据传递性可得 $(W_{\mathcal{S}}, I) \vdash C = q\{C/x\}$。接着，取一个新常量 $D \doteq q\{D/x\}$，使得 n f (D, I) 成立，因为 n f $(q\{D/x\}, I \cup \{D\})$ 成立；并且 og(D) 成立，因为 og(q) 成立。因此，根据公理 R2，$(W_{\mathcal{S}}, I) \vdash C = D$，其中 D 是观察守卫范式。□

注 6。（范式作为方程组）事实上，我们可以将注意力限制在仅由常量定义的范式上：如果 p 是一个范式且 p 不是常量，那么取一个新常量 $D \doteq p$。根据公理 R1，D 是一个范式，并且 $B \vdash D = p$。基于这一原因，下面我们将注意力限制在能够通过方程组定义的范式上：一组 $\tilde{C} = \{C_1, C2, \ldots, C_n\}$ 形式的范式中的定义常量，使得 $Const(C_l) = C$ 且 $\tilde{Const}(C_i) \subseteq C$，其中 $i = 1, \ldots, n$。该方程组 E(C) 中的方程具有以下形式（其中函数 f (i, j) 返回满足 $1 \leq k \leq n$ 的值）：

$$\begin{aligned} C_1 &\doteq \sum_{i=1}^{m(1)} \alpha_{1i}.C_{f(1,i)}\{+\mathbf{1}\} \\ C_2 &\doteq \sum_{i=1}^{m(2)} \alpha_{2i}.C_{f(2,i)}\{+\mathbf{1}\} \\ &\cdots \\ C_n &\doteq \sum_{i=1}^{m(n)} \alpha_{ni}.C_{f(n,i)}\{+\mathbf{1}\} \end{aligned}$$

其中，记号 $\{+\mathbf{1}\}$ 表示附加加项 1 是可选的，并且我们假设在 $m(i) = 0$的情况下 $C_i \doteq \mathbf{0}$。有时我们使用记号 $body(C_h)$ 来表示和式 $\sum^{m(h)}{}_{i=1}\ \alpha_{hi} \cdot C_{f(h,i)}\{+\mathbf{1}\}$。□

注 7.（观察守卫方程组）我们称一个方程组 E(C)（不一定像上面的方程组那样处于范式）是观察守卫的，如果对于每个 $C_i \in \tilde{C}$，都不存在静默循环 $C_i \stackrel{\varepsilon}{\Longrightarrow} C_i$。这个定义与定义 7 一致。例如，考虑下面的例子：

$$\begin{aligned} C_1 &\doteq a.C_2 + \varepsilon.a.C_1 \\ C_2 &\doteq b.C_2 + \varepsilon.C_1 \end{aligned}$$

当然，对于 $i = 1,2$，$C_i \stackrel{\varepsilon}{\nRightarrow} C_i$，因此该方程组是观察守卫的。事实上，我们可以证明 $og(C_1)$ 和 $og(C_2)$ 成立。□

下一个定理表明，每个观察守卫方程组（不一定处于范式）都有一个在可证明相等意义下的唯一解。

~定理 5。（W_g 的唯一解）设 $X = (x_1, x2, \ldots, x_n)$ 是一个变量元组，且 ~$p = (p_1, p2, \ldots, p_n)$ 是一个开放守卫的 SFM1 项元组，其中使用的变量~ ~属于 X。设 $C = (C_1, C2, \ldots, C_n)$ 是一个常量元组（其中的常量不出现在 ~p 中），使得方程组

$$
\begin{aligned}
C_1 &\doteq p_1\{\widetilde{C}/\widetilde{X}\}\\
C_2 &\doteq p_2\{\widetilde{C}/\widetilde{X}\}\\
&\ldots\\
C_n &\doteq p_n\{\widetilde{C}/\widetilde{X}\}
\end{aligned}
$$

~ ~是观察守卫的。因此，对于 $i = 1, \ldots, n$，$W_g \vdash C_i = p_i\{C/X\}$。

此外，如果 ~$q = (q_1, q2, \ldots, q_n)$ 也满足相同性质，即对于 $i = 1, \ldots, n$ ~$W_g \vdash q_i = p_i\{\tilde{}q/X\}$，那么 $W_g \vdash C_i = q_i$。

证明。对 n 使用归纳法。

当 $n = 1$ 时，我们有 $C_1 \doteq p_1\{C_1/x_1\}$，因此使用公理 R1 可立即得到结果 $W_g \vdash C_1 = p_1\{C_1/x_1\}$。此解是唯一的，因为 p_1 是观察守卫的（参见注 7）：如果 $W_g \vdash q_1 = p_1\{q_1/x_1\}$，根据公理 R2 可得 $W_g \vdash C_1 = q_1$。

现在假设有一个元组 ~$p = (p_1, p2, \ldots, p_n)$ 和项 p_{n+1}，使得它们在 $X = (x_1, x2, \ldots, x_n)$ 以及附加的 x_{n+1} 上全都 ~开放。假设不失一般性，x_{n+1} oc-~curs 出现在 p_{n+1} 中。首先，定义 $C_{n+1} \doteq p_{n+1}\{C_{n+1}/x_{n+1}\}$，使得 C_{n+1} 现在在 X 上开放。~因此，对于 $i = 1, \ldots, n$，每个 $p_i\{C_{n+1}/x_{n+1}\}$ 现在也都在 X 上开放。得到的观察守卫方程组如下：

$$
\begin{aligned}
C_1 &\doteq p_1\{C_{n+1}/x_{n+1}\}\{\widetilde{C}/\widetilde{X}\}\\
C_2 &\doteq p_2\{C_{n+1}/x_{n+1}\}\{\widetilde{C}/\widetilde{X}\}\\
&\ldots\\
C_n &\doteq p_n\{C_{n+1}/x_{n+1}\}\{\widetilde{C}/\widetilde{X}\}
\end{aligned}
$$

~这样，现在我们可以对 X 和 $(p_1\{C_{n+1}/x_{n+1}\}, \ldots, p_n\{C_{n+1}/x_{n+1}\})$ 使用归纳法，从而~得出，闭常量元组 $C = (C_1, C2, \ldots, C_n)$ 满足对于 $i = 1, \ldots n$：

$$W_g \vdash C_i = (p_i\{C_{n+1}/x_{n+1}\})\{\widetilde{C}/\widetilde{X}\} = p_i\{\widetilde{C}/\widetilde{X}, C_{n+1}\{\widetilde{C}/\widetilde{X}\}/x_{n+1}\}.$$

请注意，上文通过 $C_{n+1}\{\widetilde{C}/\widetilde{X}\}$，已隐式地将 C_{n+1} 的定义封闭为

$$C_{n+1} \doteq p_{n+1}\{C_{n+1}/x_{n+1}\}\{\widetilde{C}/\widetilde{X}\} = p_{n+1}\{\widetilde{C}/\widetilde{X}\}\{C_{n+1}/x_{n+1}\},$$

因此 $W_g \vdash C_{n+1} = p_{n+1}\{\widetilde{C}/\widetilde{X}\}\{C_{n+1}/x_{n+1}\}$。根据公理 R1，

元组 (C, C_{n+1}) 的唯一性可以通过公理 R2 证明。假设另有一个解元组（~q, q_{n+1}）。这意味着，对于 $i = 1, \ldots, n+1$，

$W_g \vdash q_i = p_i\{\tilde{}q/\widetilde{X}, q_{n+1}/x_{n+1}\}$。

根据归纳法，我们可以假设，对于 $i = 1, \ldots, n$，有 $W_g \vdash C_i = q_i$。

~ ~由于 $W_g \vdash C_{n+1} = p_{n+1}\{C/X\}\{C_{n+1}/x_{n+1}\}$ 根据公理 R1，由替换性可得~ $W_g \vdash C_{n+1} = p_{n+1}\{\tilde{}q/X\}\{C_{n+1}/x_{n+1}\}$。

~注意，$p_{n+1}\{\tilde{}q/X\}$ 是一个关于 x_{n+1} 开放且观察守卫的项。令 ~F 为如下定义的常量：$F \doteq p_{n+1}\{\tilde{}q/X\}\{F/x_{n+1}\}$。那么，根据公理 R2，$C_{n+1} = F$。因此，由于

$$W_g \vdash q_{n+1} = p_{n+1}\{\widetilde{q}/\widetilde{X}\}\{q_{n+1}/x_{n+1}\}$$

由公理 R2，我们得到 $W_g \vdash F = q_{n+1}$；因此，根据传递性，待证命题 $W_g \vdash C_{n+1} = q_{n+1}$ 得证。□

如果方程组中不出现前缀 ε，则称其为 ε-自由的。形式上， ε-自由范式必须具有以下形式

$$\begin{aligned} C_1 &\doteq \textstyle\sum_{i=1}^{m(1)} a_{1i}.C_{f(1,i)}\{+\mathbf{1}\} \\ C_2 &\doteq \textstyle\sum_{i=1}^{m(2)} a_{2i}.C_{f(2,i)}\{+\mathbf{1}\} \\ &\cdots \\ C_n &\doteq \textstyle\sum_{i=1}^{m(n)} a_{ni}.C_{f(n,i)}\{+\mathbf{1}\} \end{aligned}$$

其中所有动作 $a_{ij} \in A$。

我们想要证明，利用 W_g 中的公理，特别是 T3，可以将观察守卫的范式化为无ε的范式。事实上，假设

$$C_h \doteq \textstyle\sum_{i=1}^{m(h)} a_{hi}.C_{f(h,i)} + \sum_{i=1}^{m'(h)} \varepsilon.C_{g(h,i)}\{+\mathbf{1}\}$$

and that $C_{g(h,i)} \doteq p_{g(h,i)}$. Then, by Rule 3 and 替换性, 我们有

$$W_g \vdash C_h = \textstyle\sum_{i=1}^{m(h)} a_{hi}.C_{f(h,i)} + \sum_{i=1}^{m'(h)} p_{g(h,i)}\{+\mathbf{1}\}.$$

Of 当然，n p $p_{g(h,i)}$ t erh 可能有 st 个id 的出现，但由于方程组是观察守卫的，我们可以像上面那样，从没有前缀 ε 的常量开始，然后反向推导，直到到达初始常量 C_1, ，如下面的例子所示。

例 6。考虑以下观察守卫的范式：

$$\begin{aligned} C_1 &\doteq a.C_1 + \varepsilon.C_2 + \mathbf{1} \\ C_2 &\doteq b.C_2 + \varepsilon.C_3 \\ C_3 &\doteq a.C_3 + \mathbf{1} \end{aligned}$$

显然，$W_g \vdash C_3 = a.C_3 + \mathbf{1}$、$W_g \vdash C_2 = b.C_2 + a.C_3 + \mathbf{1}$，因此同样有 $W_g \vdash C_1 = a.C_1 + b.C_2 + a.C_3 + \mathbf{1}$。因此，我们可以定义一个新的 ε-自由方程组：

$$\begin{aligned} D_1 &\doteq a.D_1 + b.D_2 + a.D_3 + \mathbf{1} \\ D_2 &\doteq b.D_2 + a.D_3 + \mathbf{1} \\ D_3 &\doteq a.D_3 + \mathbf{1} \end{aligned}$$

最后，根据定理 5，对于 i = 1、2、3，我们得到 $W_g \vdash C_i = D_i$。 □

~命题 9。（化为 ε-自由范式）设 X =(x_1,x2,... , x_n) 是一个变量元组。设 ~p =(p_1,p2,. .. , p_n) 是一个开放守卫的 SFM1 项元组，使用 ~X 中的变量，其形式为 $p_h = \sum^{m(h)}{}_{i=1}\ \alpha_{hi}{\cdot}x_{f(h,i)}\{+\mathbf{1}\}$，其中 h = 1、...、n，且 f~满足 1 ≤ f (h, i) ≤ n。设 C =(C_1,C2,... ,C_n) 是一个常量元组，使得范式下的方程组

$$\begin{aligned} C_1 &\doteq p_1\{\widetilde{C}/\widetilde{X}\} \\ C_2 &\doteq p_2\{\widetilde{C}/\widetilde{X}\} \\ &\cdots \\ C_n &\doteq p_n\{\widetilde{C}/\widetilde{X}\} \end{aligned}$$

是观察守卫的。那么，存在一个由开放守卫的 ~ ~SFM1 项组成的元组 ~q =(q_1,q2,... , q_n)，其中使用了 X 中的变量；还存在一个常量元组 D =(D_1, D2,... , D_n)，使得范式下的方程组

$$\begin{aligned} D_1 &\doteq q_1\{\widetilde{D}/\widetilde{X}\} \\ D_2 &\doteq q_2\{\widetilde{D}/\widetilde{X}\} \\ &\cdots \\ D_n &\doteq q_n\{\widetilde{C}/\widetilde{X}\} \end{aligned}$$

是 ε-自由的，并且对于 $i = 1,\dots, n$，$W_g \vdash C_i = D_i$。

证明。对 n 进行归纳。当 $n = 1$ 时，我们有 $C_1 \doteq p_1\{C_1/x_1\}$，其中 p_1 必定具有 $\sum_{i=1}^{m(1)} \alpha_{1i} \cdot x_1\{+\mathbf{1}\}$ 的形式。由于 p_1 是观察守卫的，所有 α_{1i} 都必须属于 A，因此 C_1 已经是 ε-自由的。

现在假设有一个元组 $\tilde{p} = (p_1, p2, \dots, p_n)$ 和项 p_{n+1}，使得它们都在 $X = (x_1, x2, \dots, x_n)$ 上 $\tilde{}$ 开放，并且还有额外的 x_{n+1}。不妨假设 x_{n+1} 出现于 p_{n+1} 中。首先，定义 $C_{n+1} \doteq p_{n+1}\{C_{n+1}/x_{n+1}\}$，使得 C_{n+1} 现在在 X 上开放。因此，对 $i = 1,\dots, n$，所有 $p_i\{C_{n+1}/x_{n+1}\}$ 现在也都在 X 上开放。所得的大小为 n 的范式中的观察守卫方程组为：

$$\begin{aligned} C_1 &\doteq p_1\{C_{n+1}/x_{n+1}\}\{\widetilde{C}/\widetilde{X}\} \\ C_2 &\doteq p_2\{C_{n+1}/x_{n+1}\}\{\widetilde{C}/\widetilde{X}\} \\ &\dots \\ C_n &\doteq p_n\{C_{n+1}/x_{n+1}\}\{\widetilde{C}/\widetilde{X}\} \end{aligned}$$

因此，根据归纳法，我们可以得出结论：存在一个由项组成的元组 $\tilde{q} = (q_1, q2, \dots, q_n)$，以及一个常量元组 $D = (D_1, D2, \dots, D_n)$，使得

$$\begin{aligned} D_1 &\doteq q_1\{C_{n+1}/x_{n+1}\}\{\widetilde{D}/\widetilde{X}\} \\ D_2 &\doteq q_2\{C_{n+1}/x_{n+1}\}\{\widetilde{D}/\widetilde{X}\} \\ &\dots \\ D_n &\doteq q_n\{C_{n+1}/x_{n+1}\}\{\widetilde{D}/\widetilde{X}\} \end{aligned}$$

是 ε-free 的，并且对于 $i = 1,\dots, n$，有 $W_g \vdash C_i = D_i$。注意

$$\tilde{}\,\tilde{}\quad\tilde{}\,\tilde{}\quad\tilde{}\,\tilde{q}_i\{C_{n+1}/x_{n+1}\}\{D/X\} = q_i\{D/X, C_{n+1}\{D/X\}/x_{n+1}\}$$

$\tilde{}\,\tilde{}$ 因此，通过 $C_{n+1}\{D/X\}$，我们隐式地将 C_{n+1} 的定义闭合为

$$C_{n+1} \doteq p_{n+1}\{C_{n+1}/x_{n+1}\}\{\widetilde{D}/\widetilde{X}\} = p_{n+1}\{\widetilde{D}/\widetilde{X}\}\{C_{n+1}/x_{n+1}\}.$$

注意，项 p_{n+1} D X 中不可能有形如 $\varepsilon \cdot x_{n+1}$ 的加项，因为该系统在观察意义下是受保护的。现在，我们展开项 $p_{n+1}\{D/X\}$ 中每个以 ε 为前缀的常量 $D_i\tilde{}\,\tilde{}$，将每个形如 $\tilde{}\,\tilde{}\varepsilon \cdot D_i$ 的加项替换为加项 body(D_i)，从而得到 ε-free 项 $q_{n+1}\{D/X\}$。注意，根据公理 T3，R1，我们有

$$W_g \vdash p_{n+1}\{\widetilde{D}/\widetilde{X}\} = q_{n+1}\{\widetilde{D}/\widetilde{X}\}.$$

$\tilde{}\,\tilde{}$ 现在定义一个新的常量 $D_{n+1} \doteq q_{n+1}\{D/X\}\{D_{n+1}/x_{n+1}\}$，使得 $W_g \vdash C_{n+1} = D_{n+1}$，这由递归同余得出。此外，根据公理 R1，我们有 $W_g \vdash D_{n+1} = \tilde{}\,\tilde{}\,\tilde{}\,\tilde{}\,q_{n+1}\{D_{n+1}/x_{n+1}\}\{D/X\}$。类似地，对于 $i = \tilde{}\,\tilde{}\,1, \dots, n$，也有 $W_g \vdash D_i = q_i\{C_{n+1}/x_{n+1}\}\{D/X\}$。根据替换性，我们还得到，对于 $i = 1,\dots, n$，$W_g \vdash D_i = q_i\{D_{n+1}/x_{n+1}\}\{D/X\}$。最后，我们定义一个新的 ε-free 范式方程组

$$\begin{aligned} E_1 &\doteq q_1\{E_{n+1}/x_{n+1}\}\{\widetilde{E}/\widetilde{X}\} \\ E_2 &\doteq q_2\{E_{n+1}/x_{n+1}\}\{\widetilde{E}/\widetilde{X}\} \\ &\dots \\ E_n &\doteq q_n\{E_{n+1}/x_{n+1}\}\{\widetilde{E}/\widetilde{X}\} \\ E_{n+1} &\doteq q_{n+1}\{E_{n+1}/x_{n+1}\}\{\widetilde{E}/\widetilde{X}\} \end{aligned}$$

根据定理 5，有 $W_g \vdash D_i = E_i$，其中 $i = 1,\dots, n+1$。待证命题 $W_g \vdash C_i = E_i$，其中 $i = 1, \dots, n+1$，由传递性得出。□

7.3. 确定性范式

给定一个字母表 A $=\{a1,\ldots,a_k\}$，我们称一个 ε-自由范式为确定性的，当且仅当它具有如下形式：

$$\begin{aligned} C_1 &\doteq \textstyle\sum_{i=1}^{k} a_i.C_{f(1,i)}\{+\mathbf{1}\} \\ C_2 &\doteq \textstyle\sum_{i=1}^{k} a_i.C_{f(2,i)}\{+\mathbf{1}\} \\ &\cdots \\ C_n &\doteq \textstyle\sum_{i=1}^{k} a_i.C_{f(n,i)}\{+\mathbf{1}\} \end{aligned}$$

也就是说，每个常量的主体对于每个动作 $a_i \in$A 恰好包含一个加项。当然，根据表2中的指称语义，与 C_1，关联的非确定有限自动机是确定性的，其字母表恰好为 A。

请注意，确定性的概念在很大程度上取决于所选的字母表。例如，根据表2中的指称语义，C $\doteq \mathbf{0}$ 对应的非确定有限自动机是确定性的，因为它的字母表为空。然而，如果考虑一个非空字母表，比如 A $=\{a\}$，它就不是确定性的，因为其中没有对应 a 的弧。在这种情况下，一个关于 A、与 C $\doteq \mathbf{0}$ 语言等价的确定有限自动机可以是与 E $\doteq$ a.E 关联的自动机。事实上，可以利用公理 T1、R1、R2 证明 $W_g \vdash$C $=$ E；具体来说，根据公理 T1，我们有 $W_g \vdash \mathbf{0} =$ a.0；接着，根据公理 R2，由 E $\doteq$ a.E 和 $W_g \vdash \mathbf{0} =$ a.0，可得 $W_g \vdash$E $= \mathbf{0}$；然后，根据公理 R1，我们有 $W_g \vdash$C $= \mathbf{0}$，因此由传递性可得 $W_g \vdash$C $=$ E。

类似地，C $\doteq \mathbf{1}$ 的非确定有限自动机是确定性的，因为它的字母表为空。然而，如果考虑非空字母表 A $=\{a\}$，它就不是确定性的。在这种情况下，与 C $\doteq \mathbf{1}$语言等价的、相对于 A 的确定有限自动机，可以是与 D $\doteq$ a.E $+\mathbf{1}$对应的自动机，其中 E $\doteq$ a.E 表示一个汇点，即错误状态。我们可以如下证明 $W_g \vdash$C $=$ D。首先，我们已经知道 $W_g \vdash$ E $= \mathbf{0}$；因此，根据替换性和 R1，有 $W_g \vdash$D $=$ a.$\mathbf{0}+\mathbf{1}$；然后根据 T1，有 $W_g \vdash$D $= \mathbf{0}+\mathbf{1}$；再根据公理 A2、A3，有 $W_g \vdash$D $= \mathbf{1}$，由此很容易得出 $W_g \vdash$C $=$ D。

现在我们证明，给定一个无 ε 的范式，可以构造一个可证明等价的确定性范式。以下证明的思路遵循经典的 Rabin-Scott 子集构造 [25], ，并通过下面的例子加以说明。

例 7。我们来考虑以下不含 ε 的范式

$$\begin{aligned} C_1 &\doteq a.C_1 + a.C_2 + a.C_1 \\ C_2 &\doteq a.C_2 + \mathbf{1} \end{aligned}$$

其字母表 A_C 为 $\{a\}$。我们取字母表 A $=\{a,b\}$，并希望相对于它定义一个等价的确定性范式。首先，我们定义一组以集合为索引的常量 B_I，其中 I $\subseteq \{1,2\}$，定义为 B $_I \doteq \sum_{i\in I}$ body(C_i)。更明确地说，

$$\begin{aligned} B_{\{1\}} &\doteq a.C_1 + a.C_2 + a.C_1 \\ B_{\{2\}} &\doteq a.C_2 + \mathbf{1} \\ B_{\{1,2\}} &\doteq a.C_1 + a.C_2 + a.C_1 + a.C_2 + \mathbf{1} \\ B_{\emptyset} &\doteq \mathbf{0} \end{aligned}$$

现在，对于其中每一个，我们证明它都可以等同于一个确定性定义。首先，根据公理 R1，我们可以证明，由于 $B_\emptyset = \mathbf{0}$，根据公理 T1、A3，也有 $W_g \vdash B_\emptyset =$ a.$B_\emptyset$ +b.$B_\emptyset$。

现在，根据公理 R1，我们知道 $W_g \vdash B^{\{1\}} = a.C_1 + a.C_2 + a.C_1,$，因此 $W_g \vdash C_1 = B^{\{1\}}$。然后，根据公理 A1-A4、T2、R1，我们可以推出 $W_g \vdash B^{\{1\}} = a.$（主体$(C_1)$+主体$(C_2)$）。此外，根据公理 R1、T1、A3，我们还可以推出 $W_g \vdash B^{\{1\}} = a.B^{\{1,2\}} + b.B_\emptyset$。

同样，我们可以证明 $W_g \vdash B^{\{2\}} = a.B^{\{2\}} + b.B_\emptyset + \mathbf{1}$，并且 $W_g \vdash B^{\{1,2\}} = a.B^{\{1,2\}} + b.B_\emptyset + \mathbf{1}$。

最后，我们定义一个新的确定性方程组

$$\begin{aligned} D_{\{1\}} &\doteq a.D_{\{1,2\}} + b.D_\emptyset \\ D_{\{2\}} &\doteq a.D_{\{2\}} + b.D_\emptyset + \mathbf{1} \\ D_{\{1,2\}} &\doteq a.D_{\{1,2\}} + b.D_\emptyset + \mathbf{1} \\ D_\emptyset &\doteq a.D_\emptyset + b.D_\emptyset \end{aligned}$$

其中 $D^{\{2\}}$ 是冗余的，因为 $D_{\{2\}} \notin$Const$(D^{\{1\}})$，因此根据定理 5，对于 $I = \{1\}, \{2\}, \{1,2\}, /0$，有 $W_g \vdash B_I = D_I$。所以，根据传递性，$W_g \vdash C_1 = D^{\{1\}}$。□

命题 10。（约化为确定性范式）给定 ε-自由范式

$$\begin{aligned} C_1 &\doteq \sum_{i=1}^{m(1)} a_{1i}.C_{f(1,i)}\{+\mathbf{1}\} \\ C_2 &\doteq \sum_{i=1}^{m(2)} a_{2i}.C_{f(2,i)}\{+\mathbf{1}\} \\ &\cdots \\ C_n &\doteq \sum_{i=1}^{m(n)} a_{ni}.C_{f(n,i)}\{+\mathbf{1}\} \end{aligned}$$

其字母表为 A_C，可以针对选定的 $A = \{a_1, a2, \ldots, a_k\}$（其中 $A_C \subseteq A$）构造一个确定性范式，其形式为

$$\begin{aligned} D_1 &\doteq \sum_{i=1}^{k} a_i.D_{g(1,i)}\{+\mathbf{1}\} \\ D_2 &\doteq \sum_{i=1}^{k} a_i.D_{g(2,i)}\{+\mathbf{1}\} \\ &\cdots \\ D_m &\doteq \sum_{i=1}^{k} a_i.D_{g(m,i)}\{+\mathbf{1}\} \end{aligned}$$

其中 $m \geq n$，使得 $W_g \vdash C_1 = D_1$。

证明。我们定义一组集合索引常量 $B_I \doteq \sum_{i\in I}$body(C_i)，每个 $I \subseteq \{1, \ldots, n\}$ 对应一个。注意，根据公理 R1，$W_g \vdash C_1 = B^{\{1\}}$。现在，对于这些常量中的每一个 B_I，我们要证明它可以等同于一个确定性定义，即对于 A 中的每个符号，恰好有一个加项的定义。首先，令 In(B_I) 表示 B_I 的初始符号集合，即 $\cup_{i\in I}\{a_{i1}, \ldots, a_{im(i)}\}$。然后，利用公理 A1- A4,R1,T2 和替换性，我们可以证明

$$W_g \vdash B_I = \sum_{a_h \in In(B_I)} a_h.(\sum_{i\in I_h} body(C_i)),$$

其中 $I_h = \{f(i,j) \mid a_{i,j} = a_h, a_{i,j} \in$ In$(B_I)\}$。下一步要注意到，$\sum_{i\in I}$body(C_i) 根据公理 R1 可以替换为 B_{I_h}，因此

$$W_g \vdash B_I = \sum_{a_h \in In(B_I)} a_h.B_{I_h}.$$

下一步是构造与 A 中不属于 In(B_I) 的那些符号相关的加项。首先注意，借助公理 R1、T1、A3，可以将 $B_\emptyset \doteq \mathbf{0}$ 等同于

$$W_g \vdash B_\emptyset = \sum_{a_i \in A} a_i.B_\emptyset,$$

这是错误状态 $B_\emptyset$ 的确定性定义。因此，根据公理 T1、A3，我们有

$$W_g \vdash B_I = \sum_{a_h \in In(B_I)} a_h.B_{I_h} + \sum_{a_h \notin In(B_I)} a_h.B_\emptyset$$

这是常量B_I的确定性定义。最后，我们可以定义如下形式的确定性方程组

$$D_I \doteq \sum_{a_h \in \mathrm{In}(B_I)} a_h.D_{I_h} + \sum_{a_h \notin \mathrm{In}(B_I)} a_h.D_{\emptyset}$$

对于每个$I \subseteq \{1,\ldots,n\}$，根据定理 5，我们有$W_g \vdash B_I = D_I$。因此，根据传递性，$W_g \vdash C_1 = D^{\{1\}}$。□

7.4. 观察守卫进程的完备性

命题 10 是下述引理的基础，而该引理又是下文所述观察守卫进程完备性证明的关键。下述引理的证明技巧受到定理 5.10 证明的启发，而该证明又受到 [20], 中定理 2 证明的启发。 [27]

引理 1。（ε-自由范式的完备性）对于每个$p,p' \in \mathscr{P}_{SFM1}$ ε-自由范式，若$p \sim p'$，则$W_g \vdash p = p'$。

证明。设A_p为 p 的字母表，$A_{p'}$为 p′的字母表。取$A = A_p \cup A_{p'}$。根据命题 10，存在p_1和p'_1，它们是关于 A 的确定性范式，使得$W_g \vdash p = p_1$且$W_g \vdash p' = p'_1$。根据定理 4，我们有$p \sim p_1$且$p' \sim p'_1$，因此根据传递性，也有$p_1 \sim p'_1$。

设$A = \{a1, \ldots, a_k\}$。我们可以假设p_1是如下确定性方程组：

$$\begin{aligned} C_1 &\doteq \sum_{i=1}^{k} a_i.C_{f(1,i)}\{+\mathbf{1}\} \\ C_2 &\doteq \sum_{i=1}^{k} a_i.C_{f(2,i)}\{+\mathbf{1}\} \\ &\cdots \\ C_n &\doteq \sum_{i=1}^{k} a_i.C_{f(n,i)}\{+\mathbf{1}\} \end{aligned}$$

因此$p_1 = C_1$。对于每个$h = 1,\ldots, n$，根据公理 R1，我们得到$W_g \vdash C_h =$主体(C_h)；其中，$\mathrm{body}(C_h)$表示$\sum_{i=1}^{k} a_i.C_{f(h,i)}\{+\mathbf{1}\}$。

同样，我们可以假设p'_1是如下确定性方程组：

$$\begin{aligned} C'_1 &\doteq \sum_{i=1}^{k} a_i.C'_{f'(1,i)}\{+\mathbf{1}\} \\ C'_2 &\doteq \sum_{i=1}^{k} a_i.C'_{f'(2,i)}\{+\mathbf{1}\} \\ &\cdots \\ C'_{n'} &\doteq \sum_{i=1}^{k} a_i.C'_{f'(n',i)}\{+\mathbf{1}\} \end{aligned}$$

因此$p'_1 = C'_1$。对于每个$h' = 1$、...、n'，根据公理 R1，我们得到$W_g \vdash C'_{h'} = \mathrm{body}(C'_{h'})$，其中$\mathrm{body}(C'_{h'})$表示$\sum_{i=1}^{k} a_i.C'^{\{+\mathbf{1}\}}_{f'(h',i)}$。此外，由于$p_1 \sim p'_1$，我们有$C_1 \sim C'_1$。

现在，令$H = \{(h, h') \mid C_h \sim C'_{h'}\}$。当然，请注意，$(1,1) \in H$。此外，对于$(h, h') \in H$，由于$C_h$和$C'_{h'}$语言等价且具有确定性（因此是互模拟等价的，参见注 1），以下结论成立：

- for each $i = 1,\ldots,k$, we have $(f(h,i), f'(h',i)) \in H$, and
- 可选加项 1 属于$\mathrm{body}(C_h)$，当且仅当它属于$\mathrm{body}(C'_{h'})$。

现在，对于每个$(h, h') \in H$，我们来考虑开放项

$$t_{hh'} = \sum_{i=1}^{k} a_i.x_{f(h,i),f'(h',i)}\{+\mathbf{1}\}$$

根据定理 5，对于每个 (h, h′) ∈ H，都存在一个常量 $D_{hh'}$，使得 $W_g \vdash D_{hh'} = \tilde{t}_{hh'}\{D/X\}$，其中 D 表示对于每个 (h, h′) ∈ H 所对应的常量 $D_{hh'}$ 组成的元组，而 X 表示对于每个 (h, h′) ∈ H 所对应的变量 $x_{hh'}$ 组成的元组。更明确地说，$W_g \vdash D_{hh'} = \sum_{i=1}^{k} a_i.D\ f(h,i), f'(h',i)\{+\mathbf{1}\}$。如果我们通过将 x f(h,i), f′(h′,i) 替换为 $C_{f(h,i)}$，来闭合每个 $t_{hh'}$，就得到

$$\tilde{\sum}_{i=1}^{k} a_i.C_{f(h,i)}\{+\mathbf{1}\}$$

它等于 body(C_h)。因此，我们注意到 C_h 满足 $W_g \vdash C_h = t_{hh'}\{C/X\}$，所以根据定理 5，我们有 $W_g \vdash D_{hh'} = C_h$。由于 (1, 1) ∈ H，因此 $W_g \vdash D_{11} = C_1$。类似地，如果我们通过将 $x_{f(h,i),f'(h',i)}$ 替换为 $C'_{f'(h',i)}$来闭合每个 $t_{hh'}$，就得到

$$\sum_{i=1}^{k} a_i.C'_{f'(h',i)}\{+\mathbf{1}\}$$

它等于 body $C_{h'}$)。因此，(我们注意到 $C'_{h'}$ 满足 $W_g \vdash C'_{h'} = \tilde{t}_{hh'}\{C'/X\}$，所以根据定理 5，我们有 $W_g \vdash D_{hh'} = C'_{h'}$。由于 (1, 1) ∈ H，因此 $W_g \vdash D_{11} = C'_1$；根据传递性可得 $W_g \vdash C_1 = C'_1$，进而有 $W_g \vdash p_1 = p'_1$。最后，待证命题 $W_g \vdash p = p'$ 由传递性得证。□

定理 6。（观察守卫进程的完备性）
对于任意受守卫的 p、q，若 $p \sim q$，则 $W_g \vdash p = q$。

证明。根据推论 2，存在观察守卫范式 p_1 和 q_1，使得 $W_g \vdash p = p_1$ 且 $W_g \vdash q = q_1$。根据定理 4，我们有 $p \sim p_1$ 且 $q \sim q_1$，，因此根据传递性，也有 $p_1 \sim q_1$。根据命题 9，存在不含 p_2 和 q_2 ε的范式，使得 $W_g \vdash p_1 = p_2$ 且 $W_g \vdash q_1 = q_2$。根据定理 4，我们有 $p_1 \sim p_2$ 且 $q_1 \sim q_2$，，因此根据传递性，也有 $p_2 \sim q_2$。根据引理 1，由 $p_2 \sim q_2$可推出 $W_g \vdash p_2 = q_2$，，因此根据传递性，也有 $W_g \vdash p = q$。□

7.5. 无守卫进程的完备性

下面我们将注意力限定在方程组上，这些方程组不一定是范式。事实上，若 p 是一个进程且 p 不是常量，那么我们可以取一个新的常量 D ≐ p（使得 W ⊢ D = p 由公理 R1 成立），从而 p 可以等价地表示为定义在常量集 Const(D) 上的方程组。

现在我们证明，在 W_g 中加入公理 R3，足以使任意 SFM1 进程 p 等价于一个观察守卫的 SFM1 进程 q。为了证明这一结果，我们需要一些辅助记号。

首先，我们用 $n_x(p)$ 表示 p 中 x 的无守卫出现次数（包括 p 中出现的常量的定义体）。例如，若 C ≐ p{C/x} 且 $p = \varepsilon.x + a.x + \varepsilon.D$，其中 $D \doteq \varepsilon.D + \varepsilon.x$，那么 $n_x(p) = 2$；此外，我们规定 $n_x(C) = n_x(p)$。

接下来，我们需要引入一个度量，用来衡量所有通向未守卫变量 x 的出现位置的、以 ε 为标签的计算的长度。SFM1 项 p 的这个值 len(p)（它可以是关于 x 的开放项，但该定义也适用于闭项）由表 7 中定义的长度函数计算。注意，如果字母表中的一个符号（例如 a）作为前缀作用于一个进程，那么返回值为 0；而变量 x 的返回值为 1。此外，对于选择算子组合 $p + p'$，我们取 len(p) 与 len(p′) 之和。关键规则针对常量：如果 C ≐ p{C/x}，那么即使 C 是闭的，其长度也根据开放项 p 计算。可以很容易地证明

$\mathrm{len}(1)$	$=$	0	$\mathrm{len}(0)$	$=$	0	
$\mathrm{len}(p+p')$	$=$	$\mathrm{len}(p)+\mathrm{len}(p')$	$\mathrm{len}(C)$	$=$	$\mathrm{len}(p)$	if $C \doteq p\{C/x\}$
$\mathrm{len}(x)$	$=$	1	$\mathrm{len}(\varepsilon.p)$	$=$	$\begin{cases} 1+\mathrm{len}(p) & \text{若 } \mathrm{len}(p)\neq 0 \\ 0 & \text{否则} \end{cases}$	
$\mathrm{len}(a.p)$	$=$	0				

表 7：长度函数

开放项 p 是观察守卫的（参见定义 7），当且仅当 $\mathrm{len}(p) = n_x(p) = 0$。此外，如果 p 是闭的（实际上是一个封闭方程组），那么 p 是观察守卫的（参见注 7），当且仅当 $\mathrm{len}(p) = n_x(p) = 0$。

~命题 11。（将 W 归约为观察守卫的进程）设 $X = (x_1, x2, \ldots, x_n)$ 是一个变量元组，且 $\tilde{p} = (p_1, p2, \ldots, p_n)$ 是一个由变量 X 中变量构成的开放受守卫 SFM1 项元组。设 $C = (C_1, C2, \ldots, C_n)$ 是一个常量元组（其中的常量不出现在 $\tilde{p}$ 中），使得方程组

$$\begin{aligned} C_1 &\doteq p_1\{\widetilde{C}/\widetilde{X}\} \\ C_2 &\doteq p_2\{\widetilde{C}/\widetilde{X}\} \\ &\cdots \\ C_n &\doteq p_n\{\widetilde{C}/\widetilde{X}\} \end{aligned}$$

是观察上无守卫的。那么，存在一个元组 $\tilde{q} = (q_1, q2, \ldots, q_n)$，其元素是由变量 X 中变量构成的开放受守卫 SFM1 项；还存在一个元组 $D = (D_1, D2, \ldots, D_n)$（其中的常量不出现在 $\tilde{q}$ 中），使得方程组

$$\begin{aligned} D_1 &\doteq q_1\{\widetilde{D}/\widetilde{X}\} \\ D_2 &\doteq q_2\{\widetilde{D}/\widetilde{X}\} \\ &\cdots \\ D_n &\doteq q_n\{\widetilde{C}/\widetilde{X}\} \end{aligned}$$

是观察守卫的，并且对于 $i = 1, \ldots, n$，$W \vdash C_i = D_i$。

证明。该证明采用双重归纳法：首先对 n 进行归纳，然后对二元组 $(n_x(p), \mathrm{len}(p))$（对于所考虑的开放观察守卫项 p）进行归纳；其中我们假设，如果 $n_1, k_2 < (n_2, k_2)$，则 $n_1 < n_2$，或 $n_1 = n_2$ 且 $k_1 < k_2$。

对于 $n = 1$，如果 $(n_{x1}(p_1), \mathrm{len}(p_1)) = (0, 0)$，那么证明即告完成，因为 $C_1 \doteq p_1\{C_1/x_1\}$ 实际上是观察守卫的。相反，如果 p_1 在观察上无守卫，则它必定具有 $\varepsilon.r + q$ 的形式，其中 r 在观察上无守卫。现在我们进行分类讨论：

- $r = x1$：在这种情况下，根据公理 R1（也可能还包括 A1-A4），$W\ B \vdash C_1 = (\varepsilon.x_1 + q)\{C_1/x_1\}$。现在定义 $C_2 \doteq (\varepsilon.x_1 + q)\{C_2/x_1\}$，使得根据递归同余，$W \vdash C_1 = C2$。定义 $C_3 \doteq q\{C_3/x_1\}$：根据公理 R3，我们有 $W \vdash C_2 = C3$。注意，$n_{x1}(q) = n_{x1}(\varepsilon.x_1 + q) - 1$，因此可以运用归纳法，得出存在一个观测守卫进程 q1 和一个常量 D1，使得 $D_1 \doteq q_1\{D_1/x_1\}$，且 $W \vdash C_3 = D1$；由传递性可得 $W \vdash C_1 = D1$。

• r $= \varepsilon.p_1 + p2$，其中 p1 在观察上无守卫。因此，根据公理 R1（也可能还包括 A1-A4），$W \vdash C_1 = (\varepsilon.(\varepsilon.p_1 + p2) + q)\{C_1/x_1\}$。由于根据公理 T3，我们有 $W \vdash \varepsilon.(\varepsilon.p_1 + p2) = \varepsilon.p_1 + p2$，根据替换性，我们也有 $W \vdash C_1 = ((\varepsilon.p_1 + p2) + q)\{C_1/x_1\}$。现在定义 $C_2 \doteq ((\varepsilon.p_1 + p2) + q)\{C_2/x_1\}$，使得根据递归同余，$W \vdash C_1 = C2$。注意，$len((\varepsilon.p_1 + p2) + q) < len(\varepsilon.(\varepsilon.p_1 + p2) + q)$，因此可以运用归纳法，得出存在一个观测守卫进程 q1 和一个常量 D1，使得 $D_1 \doteq q_1\{D_1/x\}$，且 $W \vdash C_2 = D1$；由传递性可得 $W \vdash C_1 = D1$。

由于不可能有其他情况，$n = 1$ 的基例证明完成。

现在假设有一个元组 $\tilde{p} = (p_1, p2, \ldots, p_n)$ 和项 p_{n+1}，使得它们都在 $X = (x_1, x2, \ldots, x_n)$ 上开放，并且还有额外的 x_{n+1}。不失一般性地，假设 x_{n+1} 出现在 p_{n+1} 中。首先，定义

$$C_{n+1} \doteq p_{n+1}\{C_{n+1}/x_{n+1}\},$$

从而 C_{n+1} 现在在 X 上开放。然后，我们定义 $p_i\{C_{n+1}/x_{n+1}\}$；对于 $i = 1, \ldots, n$，它是项 p_i，其中变量 x_{n+1} 的每次出现都被 C_{n+1} 替换；注意 $\tilde{}$，每个项 $p_i\{C_{n+1}/x_{n+1}\}$ 都在 X 上开放。因此

$$\begin{aligned} C_1 &\doteq p_1\{C_{n+1}/x_{n+1}\}\{\widetilde{C}/\widetilde{X}\} \\ C_2 &\doteq p_2\{C_{n+1}/x_{n+1}\}\{\widetilde{C}/\widetilde{X}\} \\ &\cdots \\ C_n &\doteq p_n\{C_{n+1}/x_{n+1}\}\{\widetilde{C}/\widetilde{X}\} \end{aligned}$$

这是一个大小为 n 的方程组，因此根据归纳法，我们可以得出结论：存在 $\tilde{}$ 一个项的元组 $\tilde{q} = (q_1, q2, \ldots, q_n)$ 以及一个常量元组 $D = (D_1, D2, \ldots, D_n)$，使得

$$\begin{aligned} D_1 &\doteq q_1\{C_{n+1}/x_{n+1}\}\{\widetilde{D}/\widetilde{X}\} \\ D_2 &\doteq q_2\{C_{n+1}/x_{n+1}\}\{\widetilde{D}/\widetilde{X}\} \\ &\cdots \\ D_n &\doteq q_n\{C_{n+1}/x_{n+1}\}\{\widetilde{D}/\widetilde{X}\} \end{aligned}$$

是观察守卫的，并且对 $i = 1, \ldots, n$，有 $W \vdash C_i = D_i$。注意，$\tilde{q}_i\{C_{n+1}/x_{n+1}\}\{D/X\} = q_i\{D/X, C_{n+1}\{D/X\}/x_{n+1}\}$

因此，由 $C_{n+1}\{\widetilde{D}/\widetilde{X}\}$ 我们已隐式地将 C_{n+1} 的定义封闭为

$$C_{n+1} \doteq p_{n+1}\{C_{n+1}/x_{n+1}\}\{\widetilde{D}/\widetilde{X}\} = p_{n+1}\{\widetilde{D}/\widetilde{X}\}\{C_{n+1}/x_{n+1}\}.$$

现在，我们将每个常量 D_i 从项 $p_{n+1}\{\widetilde{D}/\widetilde{X}\}\{C_{n+1}/x_{n+1}\}$ 中展开，使 C_{n+1} 可能出现的后续位置都显露出来。注意，根据公理 R1，

$$WB \vdash p_{n+1}\{\widetilde{D}/\widetilde{X}\} = p_{n+1}\{\widetilde{body(D)}/\widetilde{X}\}.$$

更简洁地说，我们可以写成

$$p_{n+1}\{\widetilde{body(D)}/\widetilde{X}\} = r_{n+1}\{\widetilde{D}/\widetilde{X}\}.$$

引入一个新常量 $C'_{n+1} = r_{n+1}\{D/X\}\{C'_{n+1}/x_{n+1}\}$，使得 $W \vdash C_{n+1} = C'_{n+1}$ 根据递归同余成立。注意，我们现在处于类似于 $n = 1$ 的基例的情形：

• 若 $(n_{x_{n+1}}(r_{n+1}\{\widetilde{D/X}\}), len(r_{n+1}\{\widetilde{D/X}\})) = (0,0)$，那么我们（几乎）就完成了，因为 $\tilde{}\ \tilde{}C'_{n+1} \doteq r_{n+1}\{D/X\}\{C'_{n+1}/x_{n+1}\}$ 实际上是观察守卫的。根据公理 $\tilde{}\ \tilde{}$R1，我们有 $W \vdash C'_{n+1} = r_{n+1}\{C'_{n+1}/x_{n+1}\}\{D/X\}$。

~ ~类似地，对于 i = 1, . . . , n，也有 W ⊢ $D_i = q_i\{C_{n+1}/x_{n+1}\}\{D/X\}$。根据替换性，对于 i = 1, . . . , n，我们也得到 W ⊢ $D_i = q_i\{C'_{n+1}/x_{n+1}\}\{D/X\}$。最后，我们定义一个新的观察守卫方程组

$$\begin{aligned} E_1 &\doteq q_1\{E_{n+1}/x_{n+1}\}\{\widetilde{E}/\widetilde{X}\} \\ E_2 &\doteq q_2\{E_{n+1}/x_{n+1}\}\{\widetilde{E}/\widetilde{X}\} \\ &\cdots \\ E_n &\doteq q_n\{E_{n+1}/x_{n+1}\}\{\widetilde{E}/\widetilde{X}\} \\ E_{n+1} &\doteq r_{n+1}\{E_{n+1}/x_{n+1}\}\{\widetilde{E}/\widetilde{X}\} \end{aligned}$$

使得 W ⊢ $D_i = E_i$ 对于 i = 1,..., n 成立，并由定理 5 得到 W ⊢ $C'_{n+1} = E_{n+1}$。待证命题 W ⊢ $C_i = E_i$ 对于 i = 1,... , n + 1 成立，由传递性可得。

• 相反，如果 $r n_{+1}\{\widetilde{D}/\widetilde{X}\}$ 在观察上无守卫，那么它必定具有ε.r + q 的形式，其中 r 在观察上无守卫。现在我们可以像处理基例时那样进行分类讨论；由于情况确实非常相似，我们省略这部分证明。于是，最后我们得到一个新的观测有守卫项 qn_{+1} 和一个~ ~新的常量 Dn_{+1}，使得 $Dn_{+1} \doteq qn_{+1}\{Dn_{+1}/xn_{+1}\}\{D/X\}$，且 W ⊢$C'n_{+1}$ =Dn_{+1}。由传递性可得 W ⊢$Cn_{+1} = Dn_{+1}$。此外，根据公理 R1，我们有~ ~ W ⊢$Dn_{+1} = qn_{+1}\{Dn_{+1}/xn_{+1}\}\{D/X\}$。

~ ~类似地，还可得 W ⊢ $D_i = q_i\{C_{n+1}/x_{n+1}\}\{D/X\}$对 i = 1, . . . , n。由替换性，我们还可得 W ⊢ $D_i = q_i\{D_{n+1}/x_{n+1}\}\{D/X\}$对 i = 1, . . . , n。最后，我们定义一个新的观察守卫方程组

$$\begin{aligned} E_1 &\doteq q_1\{E_{n+1}/x_{n+1}\}\{\widetilde{E}/\widetilde{X}\} \\ E_2 &\doteq q_2\{E_{n+1}/x_{n+1}\}\{\widetilde{E}/\widetilde{X}\} \\ &\cdots \\ E_n &\doteq q_n\{E_{n+1}/x_{n+1}\}\{\widetilde{E}/\widetilde{X}\} \\ E_{n+1} &\doteq q_{n+1}\{E_{n+1}/x_{n+1}\}\{\widetilde{E}/\widetilde{X}\} \end{aligned}$$

使得 W ⊢ $D_i = E_i$对 i = 1, . . . , n + 1，由定理 5 得出。待证命题 W ⊢ $C_i = E_i$对 i = 1, . . . , n + 1，由传递性得出。□

定理 7。（W 在整个 SFM1 上的完备性）对于每个 p,q ∈ $\mathscr{P}_{SFM1}$，如果 p ∼ q，则 W ⊢ p = q。

证明。由命题 11，存在 p′ 和 q′，它们是观察守卫的，使得 W ⊢ p = p′ 且 W ⊢ q = q′。由定理 4，我们有 p ∼ p′ 以及 q ∼ q′，因此，由传递性还可得 p′ ∼ q′。由定理 6，我们有 W ⊢ p′ = q′，因此待证命题 W B ⊢ p = q 由传递性得出。□

8. 结论与未来研究

本文展示了如何使用进程代数 SFM1（它在同构意义下真正表示非确定有限自动机），以找到语言等价的可靠且完备的公理化，从而也为正则语言提供一种可靠、完备且有限的公理化；这种公理化不同于基于正则表达式的克莱尼代数的公理化

。 [27, 7, 18]事实上，我们的公理化由 7 条公理和 3 条条件公理组成，似乎比这些公理化更简洁。一方面，Kozen [18] 提出的经典公理化包含 11 条用于析取和连接的公理，以及 4 条用于迭代的公理（其中两条是条件公理）。然而，这并非目前关于克莱尼代数中语言等价的最优公理化；事实上，[19] 证明，可以通过增加几条等式公理来移除 Kozen 的一条条件公理，随后 [9] 进一步改进了这一结果，证明语言等价可以由一个（左手）克莱尼代数公理化，该代数由 13 条公理定义，其中只有一条是条件公理。另一方面，值得注意的是，我们的公理化使用了公理模式（尤其是递归方面），而[18, 9] 则没有。

Alexandra Silva 在她的博士论文 [29], 中运用余代数技术 [26]研究了不含 ε 标签转移的非确定有限自动机。在第 5 章中，她基于与 Bonsangue 和 Rutten 的合作成果 [30], ，提出了一种用于描述此类非确定有限自动机的（余）代数。与 SFM1 类似，它包含一个动作前缀算子（但不考虑前缀 ε），并以递归（通过 [20] 的标准不动点算子实现）代替 Kleene 星号，而非使用连接；不过，这种代数还包含一些额外的算子。对于这种（余）代数，她证明了一个语言等价意义下的可表示性定理。此外，她还为语言等价定义了一套公理化方案。由于其（余）代数在语法上的特殊性，这套方案相当冗长，共包含 18 条公理（而我们的 SFM1 公理化方案在不含前缀 ε 时仅包含 8 条公理，因为无需 T3 和 R3，而且 R2 还可以替换为更简单的 R2′）。

不含 ε 标记转移的非确定有限自动机也是另一种进程代数的模型，该代数在 [4] 中称为 $\mathrm{BSP}_{gf\,递归}(\mathrm{A})$（参见推论 5.8.3），它与 SFM1 相当相似（但不含前缀 ε）。然而，其中提出的公理理论仅针对双模拟等价；它没有使用公理 R2，而是采用了一些递归原理，尤其是 RSP（递归规范原理，它确保每个递归规范至多有一个解）。ACP/BPA 学界广泛推崇这一原理。

本文的另一个目标是展示可表示性定理（如定理 2）在同构意义下对语义模型（如非确定有限自动机）代数研究的作用。事实上，SFM1 使我们得以研究非确定有限自动机上的双模拟等价，并提出了一个由 4 条公理和 2 条条件公理组成的、针对该等价的可靠且完备的公理化体系（集合 B）。未来的研究可以将 SFM1 的公理理论扩展到线性时间/分支时间谱系 [10, 11] 中的其他行为等价。例如，我们认为，弱模拟等价 [24, 1]可以通过将集合 W 中的公理 T2 替换为以下公理来实现公理化

$$\mathbf{T2'}\quad a.(x+y) = a.(x+y) + a.y.$$

有趣的是，我们提出了关于各种类别 Petri网的类似可表示性定理 [12], ：针对每一类，提供一种特定的进程代数，使其能够在同构意义下真正表示该类的模型。在 [13, 14] 这些结果中，有一项已被用于对一小类有限Petri网上基于互模拟的行为等价关系进行公理化。

文献中还有其他描述正则行为的进程代数，其中最著名的是 BPA^*（例如参见 [5, 3, 11]），它在语法上对应于

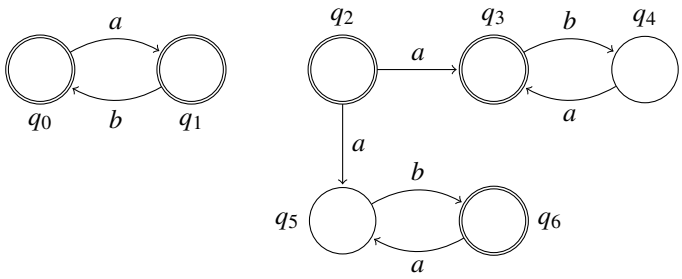

图6：(a) 中的非确定有限自动机在双模拟等价意义下无法用 BPA* 表示；(b) 中的非确定有限自动机可用 BPA* 表示，且与 (a) 中的非确定有限自动机语言等价

正则表达式的定义。BPA* 的抽象语法为

$$p ::= \mathbf{0} \mid \mathbf{1} \mid \alpha \mid p + p \mid p \cdot p \mid p^*$$

其中 $p_1 \cdot p_2$ 是顺序组合算子，p^* 是迭代算子。用于为该进程代数赋予语义的语义模型是非确定有限自动机。例如，$(a \cdot b)^* + a \cdot (b \cdot a)^*$ 的语义与图6(b)中所示的非确定有限自动机同构。注意，与 BPA* 进程 $(a \cdot b)^* + a \cdot (b \cdot a)^*$ 相关联的非确定有限自动机所识别的语言，恰好就是与正则表达式 $(a \cdot b)^* + a \cdot (b \cdot a)^*$ 相关联的语言。

有趣的是，这种进程代数的表达能力严格弱于 SFM1。事实上，Milner 早在 [20] 中就已指出，存在一些非确定有限自动机，它们与任何 BPA* 进程都不双模拟等价：例如图6(a)中的非确定有限自动机，它可以在同构意义上（因而也在双模拟等价意义上）用 SFM1 表示，具体可通过以下方程组表示

$$C_0 \doteq a.C_1 + \mathbf{1}$$
$$C_1 \doteq b.C_0 + \mathbf{1}$$

然而，BPA* 可以表示所有正则语言：给定一个正则语言 L，存在一个 BPA* 进程 p，使其关联的非确定有限自动机能够识别 L。例如，与图6(a)中的进程语言等价的 BPA* 进程实际上是 $(a \cdot b)^* + a \cdot (b \cdot a)^*$，其关联语义与图6(b)中的非确定有限自动机同构。这并不十分令人意外，因为我们已在引言中指出（参见图1），正则表达式是一种能够表示所有非确定有限自动机的形式体系，但仅限于语言等价意义下。文献 [3] 介绍了一项有趣的研究，探讨了哪些非确定有限自动机子类能够用 BPA* 表示（以互模拟等价为准）。

我们的公理化以进程代数领域中针对基于双模拟的等价关系所发展的结果和技术为基础，并将其应用于语言等价并加以改造；语言等价是一种通常未在进程代数上下文中得到深入研究的等价关系。

参考文献

参考文献

[1] L. Aceto, D. de Frutos Escrig, C. Gregorio-Rodriguez, A. Ing´olfsd´ottir，针对 BCCSP 上的弱模拟语义进行公理化，《理论计算机科学》537:42-71，2014。[2] D.N. Arden，《延迟逻辑与有限状态机》，载于《计算机设计理论》，第 1-35 页。密歇根大学出版社，1960。[3] J.C.M. Baeten, F. Corradini, C.A. Grabmayer，《双模拟下正则表达式的刻画》，《ACM期刊》54(2:6),1-28，2007。[4] J.C.M. Baeten, T. Basten, M.A. Reniers，《进程代数：通信进程的等式理论》，《剑桥理论计算机科学论丛》50，剑桥大学出版社，2010。[5] J.A. Bergstra, W.J. Fokkink, A. Ponse，《带递归操作的进程代数》，[6], 333-389 的第 5 章，2001。[6] J.A. Bergstra, A. Ponse, S.A. Smolka（编），《进程代数手册》，爱思唯尔，2001。[7] J.H. Conway，《正则代数与有限机》，Chapman and Hall，伦敦，1971。ISBN 0-412-10620-5。[8] B.A. Davey, H.A. Priestley，《格与序导论》（第二版），剑桥大学出版社，2002。[9] A. Das, A. Doumane, D. Pous，《通过循环证明实现克莱尼代数的左手完备性》，载于：Gilles Barthe, Geoff Sutcliffe, Margus Veanes（编），LPAR-22，第 22 届国际逻辑编程、人工智能与推理会议，《EPiC计算系列》第 57 卷，第 271-289 页，2018。[10] R.J. van Glabbeek，《线性时间—分支时间谱 I》，[6],3-99 的第 1 章，2001。[11] R. Gorrieri, C. Versari，《并发理论导论：迁移系统与CCS》，《EATCS理论计算机科学丛书》，施普林格出版社，2015。[12] R. Gorrieri，《Petri网进程代数：分布式系统的字母化》，《EATCS理论计算机科学专著》，施普林格出版社，2017。[13] R. Gorrieri，《有限状态机团队等价的公理化》，《计算系统建模艺术》（Catuscia Palamidessi 纪念文集），LNCS 11760，14-32，施普林格，2019。[14] R. Gorrieri，《具有静默迁移的有限状态机的团队等价》，《信息与计算》第 275 卷，2020，DOI:10.1016/j.ic.2020.104603

[15] Gross J.L., Yellen J.（编），《图论手册》。离散数学及其应用。CRC出版社，2004。[16] J.E. Hopcroft、R. Motwani、J.D. Ullman，《自动机理论、语言与计算导论》，第2版，Addison-Wesley出版社，2001。[17] S.C. Kleene，神经网络和有限自动机中的事件表示，收录于《自动机研究》，《数学研究年刊》，普林斯顿大学出版社，第34卷（第7.2节，第26–27页），1956。[18]D. Kozen，克莱尼代数与正则事件代数的完备性定理，《信息与计算》110(2):366–390，1994。doi:10.1006/inco.1994.1037[19] D. Kozen、A. Silva，左手完备性，《理论计算机科学》807:220–233，2020。doi:10.1016/j.tcs.2019.10.040 先前的会议版本发表于：Wolfram Kahl、Timothy G. Griffin（编），《计算机科学中的关系与代数方法》（RAMiCS 2012），《计算机科学讲义》第7560卷，第162–178页，施普林格，2012。[20] R. Milner，一类正则行为的完备推理系统，《计算机与系统科学杂志》28:439–466，1984。[21] R. Milner，有限状态行为观察同余的完备公理化，《信息与计算》81:227–247，1989。[22] R. Milner。《通信与并发》，普伦蒂斯·霍尔，1989。[23] R. McNaughton、H. Yamada，自动机的正则表达式与状态图，《IEEE电子计算机汇刊》9(1):39–47，1960。[24] D.M.R. Park，无限序列上的并发与自动机，载于第5届GI理论计算机科学会议论文集，LNCS 104，第167–183页，施普林格出版社，1981。[25] M.O. Rabin、D. Scott，有限自动机及其判定问题，《IBM研究与开发杂志》3(2):114–125，1959。[26] J.J.M.M. Rutten，泛余代数：一种系统理论，《理论计算机科学》249(1):3–80，2000。[27] A. Salomaa，正则事件代数的两个完备公理系统，ACM期刊13(1):58–169，1966。doi:10.1145/321312.321326[28] D. Sangiorgi，《互模拟与余归纳导论》，剑桥大学出版社，2012。[29] A. Silva，《Kleene余代数》，博士论文，奈梅亨拉德堡德大学，2010。ISBN: 978-90-6464-433-7[30] A. Silva、M.M. Bonsangue 和 J.J.M.M. Rutten，非确定性 Kleene 余代数，《计算机科学中的逻辑方法》6(3)，2010。