CLT 含递归算子的最大前同余性

邓鹏辉,张晋津
(南京航空航天大学 计算机科学与技术学院,江苏 南京 210016)

摘 要:进程之间的等价关系或精化关系的同余或前同余性(congruence 或 precongruence)是组合式推理和模块化设计验证的理论基础。针对面向 Web Service 的进程演算,Bernardi 和 Hennessy 提出了 Client-Must-Testing(CLT)语义及相关的测试前序⊑用于描述进程的精化关系,并对包含于 $\underset{\sim}{\subset}$ 的最大前同余关系 $\underset{\sim}{\subset}$ +进行了研究。递归算子是规范理论中重要而且是基础性的算子,Bernardi 和 Hennessy 对包含于 $\underset{\sim}{\subset}$ 的最大前同余关系的研究中未涉及递归算子,因此不能描述进程的无限行为。文中研究了 CLT 诱导出的精化关系在包含递归算子情形下的前同余性。在讨论了环境(context)、递归进程以及一步转换内在联系的基础上,给出包含于 $\underset{\sim}{\subset}$ 的最大前同余关系。

关键词:进程代数;must-testing 语义;精化关系;递归算子;最大前同余
中图分类号:TP301 **文献标识码**:A **文章编号**:1673-629X(2016)09-0143-06
doi:10.3969/j.issn.1673-629X.2016.09.032

Largest Precongurence with Recursive Operator in CLT

DENG Peng-hui,ZHANG Jin-jin
(School of Computer Science and Technology,Nanjing University of Aeronautics and Astronautics,
Nanjing 210016,China)

Abstract:Process algebra aims to provide algebraic theories for concurrent communication system,where the notions of behavioral equivalence and refinement play central roles. In particular,congruence or precongruence of behavioral relations provide theoretical foundation for compositional reasoning and modular designing and verifying. In order to capture the concurrent behavior of the server and the client, Bernardi and Hennessy present a Web Service-oriented semantic CLT (Client Must Testing). They studied the largest precongurence contained in the refinement relation $\underset{\sim}{\subset}$ induced by CLT without considering recursive. Recursive operator is important and fundamental in specification theory. Bernardi and Hennessy have studied the largest precongurence contained in $\underset{\sim}{\subset}$. However,infinite processes cannot be expressed in such framework due to lacking recursive operator. Based on the exploring relationship among contexts,recursive processes and one step transition,a characterization for the largest precongurence contained in $\underset{\sim}{\subset}$ in the presence of recursive operator is presented.

Key words:process algebra;must-testing semantic;refinement;recursive operator;largest precongurence

0 引 言

在进程代数理论中,Nicola 和 Hennessy 早期提出三种测试语义(may,must,may&must)用来描述精化关系,基于被测试进程与环境间的相互作用诱导出的计算路径序列,分析其行为[1-3]。近几年,Barbanera 等提出面向网络服务器的必须测试理论[4-7];Bernardi 和 Hennessy 提出了面向网络服务器的 Client Must Testing (CLT)语义用于描述精化关系[8]。它介绍了两种子行为关系:服务器(server)和客户(client),并描述了它们之间的相互作用,并且它们的语义定义一致,都可以看成是进程。

递归算子是规范理论中重要而且是基础性的算子,但文献[8]在处理同余性时对此未加考虑。文中基于 Hennessy 等提出的 CLT,研究环境、递归进程的展开与进程转换之间的内在联系,在此基础上考察 CLT 含递归算子的最大前同余关系。

1 预备知识

本节将给出文中使用的一些符号和基本概念,简单介绍 CLT 的语法及其结构化操作语义规则。

收稿日期:2015-12-08 **修回日期**:2016-04-05 **网络出版时间**:2016-08-23
基金项目:国家自然科学基金资助项目(11426136,60973045);江苏省高校自然科学基金(13KJB520012)
作者简介:邓鹏辉(1986-),男,硕士研究生,研究方向为进程代数、计算机科学中的逻辑学等;张晋津,讲师,博士,研究方向为形式化方式、计算机科学中的逻辑学等。

文中采用 Act 表示动作集,用符号 a、b、$\bar{a}$、$\bar{b}$ 等表示其元素,其中 a 和 $\bar{a}$ 是一对互补动作,约定 $\bar{\bar{a}} = a$。令 $\mathrm{Act}_{\surd} \triangleq \mathrm{Act} \cup \{\surd\}$,用符号 λ、μ 等表示其元素,其中$\surd$表示成功的动作。如果 A 是一集合,A^* 表示 A 中有限符号组成的文字集合,用符号 s、ε 等表示其元素,其中 ε 表示空文字。采用 Var 表示变元集合,用符号 X,Y 等表示其元素。采用 ω 表示自然数集合,用符号 m,n,k 等表示其元素。

定义 1[8]:CLT 的项由 BNF 范式定义如下:

$t ::= 0 \mid 1 \mid a.t \mid t + t \mid t \oplus t \mid X \mid \mathrm{rec}X.t$

其中,$X \in \mathrm{Var}$,$a \in \mathrm{Act}$。

为了书写方便,在不引起歧义的情况下,将 $a.t$ 记为 at。

各个算子简单介绍如下:0 表示“死”进程,不能执行任何动作;1 表示成功的记号,被处理成一个不执行任何动作的进程;$a.t$ 只能执行 a 动作,之后 t 才能执行;$t_1 + t_2$ 表示外部不确定选择,通过与外界环境的交互选择执行 t_1 或者 t_2,当执行 $t_1(t_2)$,$t_2(t_1)$ 被自动抛弃;$t_1 \oplus t_2$ 表示内部不确定选择,与 $t_1 + t_2$ 的不同之处在于由系统内部选择执行 t_1 或者 t_2,而与外界环境无关;$\mathrm{rec}X.t$ 表示递归项。

下面给出变元 X 在项 t 中约束出现的递归定义:

(1)如果 X 在 $\tilde{t}$ 中约束出现,那么 X 在 $f(\tilde{t})$ 中约束出现,其中 f 为 CLT 中的非递归算子,$\tilde{t}$ 表示 t_1,t_2,…,t_n,n 与 f 算子的元数一致;

(2)如果 $X \equiv Y$,或者 X 在 t 中约束出现,那么 X 在 $\mathrm{rec}X.t$ 中约束出现。如果不是约束出现,则称它是自由出现。若 X 在 t 中自由出现,则称 X 是 t 的自由变元。

约定 1:与通常做法一样,文中假设对任意两个递归项 $\mathrm{rec}X.t_1$、$\mathrm{rec}Y.t_2$,有 $X \neq Y$ 并且对任何给定的进程 t 而言,任何变元不会在 t 中既有自由出现又有约束出现。显然,这两个约定均可通过对递归变元适当换名得以实现。

给定项 t,它的自由变元的集合(记为 $\mathrm{FV}(t)$)及子项的集合按通常方式定义,如果 $\mathrm{FV}(t) = \varnothing$,它就被称为进程,一般用符号 p、q 和 r 表示。$t_1 \equiv t_2$ 表示两个表达式 t_1 和 t_2 语法相同。

定义 2(环境):一个环境 $C_{\tilde{X}}$ 就是一个项,该项所含自由变元在 n -元组 $\tilde{X} = (X_1, X_2, \cdots, X_n)$ 中,元组中的变元互不相同且 $n \geqslant 0$。给定进程 n -元组 $\tilde{p} = (p_1, p_2, \cdots, p_n)$,将同时把 $C_{\tilde{X}}$ 中每个 X_i 替换为 p_i 而形成的项记为 $C_{\tilde{X}}\{p_1/X_1, p_2/X_2, \cdots, p_n/X_n\}$(简记为 $C_{\tilde{X}}\{\tilde{p}/\tilde{X}\}$)。

定义 3[2](扩展的标记转换系统):扩展的标记转换系统(Extended Labelled Transition System,ELTS)是一个 4 元组 $< P, \mathrm{Act}, \rightarrow, \ >$,转换关系 $\xrightarrow{a}$, 由图 1 中的结构化操作语义规则(Structural Operational Semantics,SOS)[8-9]按通常的方式决定,其中 P 为所有进程形成的集合,$a \in \mathrm{Act}$,$\alpha \in \mathrm{Act}_{\surd}$。

$$R_1 \ \frac{}{1 \xrightarrow{\surd} 0} \qquad R_2 \ \frac{}{a.p \xrightarrow{a} p}$$

$$R_{3-l} \ \frac{P \xrightarrow{\alpha} P'}{p + q \xrightarrow{\alpha} p'} \qquad R_{3-r} \ \frac{q \xrightarrow{\alpha} q'}{p + q \xrightarrow{\alpha} q'}$$

$$R_{4-l} \ \frac{P \mapsto P'}{p + q \mapsto p'} \qquad R_{4-r} \ \frac{q \mapsto q'}{p + q \mapsto q'}$$

$$R_{5-l} \ \frac{}{p \oplus q \mapsto p} \qquad R_{5-r} \ \frac{}{p \oplus q \mapsto q}$$

$$R_6 \quad \mathrm{rec}X.t \mapsto t[\mathrm{rec}X.t / X]$$

图 1 CLT 的结构化操作语义规则

$p \xrightarrow{a}$ 表示存在 q 使得 $p \xrightarrow{a} q$。$p \overset{a}{\Rightarrow} q$ 表示 $p(\ ) * \xrightarrow{a} (\ ) * q$,此处 $(\ ) *$ 是 的自反传递闭包。$p \overset{as}{\Rightarrow} q$ 表示 $p \overset{a}{\Rightarrow} \overset{s}{\Rightarrow} q$。$p \xrightarrow{a}\!\!\!\!\!\!/\ \ $ 表示对任意的 q,$p \xrightarrow{a} q$ 不成立。$p \overset{s}{\Rightarrow}_{\surd} q$ 表示存在转换序列 $p \overset{a_1}{\Rightarrow} p_1 \overset{a_2}{\Rightarrow} \cdots \overset{a_{n-1}}{\Rightarrow} p_{n-1} \overset{a_n}{\Rightarrow} q$,其中 $s = a_1 a_2 \cdots a_n$,并且这个转换序列中的任何状态 p' 都满足 $p' \xrightarrow{\surd}\!\!\!\!\!\!/\ \ $。类似地,针对关系 ,可以定义类似的记号,此外不再赘述。

如果存在无限序列 p p_1 p_2 …,则称 p 发散,记为 $p \Uparrow$;否则称 p 收敛,记为 $p \Downarrow$。

上述 SOS 规则直观、含义显然,需要指出的一点是,递归算子操作语义通常按如下方式定义:

$$R \ \frac{t[\mathrm{rec}X.t/X] \xrightarrow{\alpha} P}{\mathrm{rec}X.t \xrightarrow{\alpha} p}$$

例如,Milner 在 CCS 中采用上述方式定义递归。一般来讲,两者定义差别不大,文中选用的规则较常规定义方式仅多了一步内部转换。但是,关于 $\mathrm{rec}X.X$ 却截然不同,常规定义中,该进程表示“死”进程,既不能执行任何动作序列,也不能执行内动作。然而在文中,由 R_6 可知 $\mathrm{rec}X.X$ $\mathrm{rec}X.X$,所以该进程表示一个发散进程,记为 Θ。该进程在后续证明中将多次使用。

由图 1 中 R_6 可知,由于递归算子的存在,进程的一步转换所到达的子进程结构可能比其自身结构更复杂,因此,结构归纳法一般不适用。所以,考虑根据证明树的深度进行归纳证明。

将形如 $p \xrightarrow{\alpha} q$ 或者 p q 的表达式称为文字,其中,p、q 是进程,$\alpha \in \mathrm{Act}\surd$,一般用 ϕ、φ、χ 等表示。由图 1 可知,CLT 的 SOS 规则最多只含有一个前提条件,因此给出其证明树的定义。

定义 4(证明树):一个文字 χ 的证明是一棵良基的(well-founded)向上分叉的树,树的每个节点都标记为文字,并且满足下面两个条件:

(1)根被标记为 χ;

(2)如果 ϕ、φ 分别是节点 p、q 的标记且 q 是 p 的子节点,则存在 SOS 规则的例化 R,使得 $R \equiv \frac{\varphi}{\phi}$。

为了描述进程的行为,测试语义引进了进程的复合结构 $p \parallel q$,其操作语义规则如图 2 所示[8]。

$$R_{7-l}\ \frac{p \mapsto p'}{p \parallel q \to p' \parallel q} \qquad R_{7-r}\ \frac{q \mapsto q'}{p \parallel q \to p \parallel q'}$$

$$R_8\ \frac{p \xrightarrow{a} p', q \xrightarrow{\bar{a}} q'}{p \parallel q \to p' \parallel q'}$$

图 2　复合结构操作语义规则

具有如下形式的转换序列称为 $p \parallel r$ 的一条计算路径。

$$p \parallel r = p_0 \parallel r_0 \to p_1 \parallel r_1 \to \cdots \to p_k \parallel r_k \to \cdots$$

如果它是无限的或者它的最终状态 $p_n \parallel r_n$ 满足 $p_n \parallel r_n \not\to$,则称它是极大的;如果存在 $0 \leqslant k < \omega$ 满足 $r_k \xrightarrow{\surd}$,则称它是成功的。

定义 5[8]:如果 $p \parallel r$ 的所有极大计算路径都是成功的,则称 p 必然满足 r,记为 p must r。

定义 6[8](有用进程):给定进程 r,如果存在进程 p 使得 p must r,则称 r 是有用进程。用 U_{clt} 表示所有有用进程形成的集合。

定义 7[8](测试前序):对任意的进程 p,如果存在 p must r_1 蕴含 p must r_2,则称 r_1 是 r_2 的精化,记为 $r_1 \underset{\sim}{\subset} r_2$。

如果 $r_1 \underset{\sim}{\subset} r_2$ 并且 $r_2 \underset{\sim}{\subset} r_1$,则称 r_1,r_2 精化相等,记为 $r_1 \simeq r_2$。

2　CLT 的最大前同余关系

在进程代数描述的并发系统中,进程之间的等价关系(或精化关系)的同余(congruence)(或前同余)性是组合推理的基础,同时也是模块化设计的必要条件。

定义 8(前同余性):对任意进程 r_1、r_2,环境 C_X 及进程之间的精化关系 $\underset{\sim}{\subset}$,如果 $r_1 \underset{\sim}{\subset} r_2$ 使得 $C_X\{p/X\} \underset{\sim}{\subset} C_X\{q/X\}$,则称 $\underset{\sim}{\subset}$ 具有前同余性。

但是,文中所研究的 CLT 的测试前序 $\underset{\sim}{\subset}$ 不具有前同余性,如下例所示:

给定进程 0、$b.0$,因为它们都不是有用进程,所有 $0 \underset{\sim}{\subset} b.0$。容易验证 $\bar{a}.1 + \bar{b}.1$ must $0 + a.1$ 并且 $\bar{a}.1 + \bar{b}.1$ must $b.0 + a.1$,因此 $0 + a.1 \underset{\sim}{\subset} b.0 + a.1$ 不成立。

从上例可以看出,$\underset{\sim}{\subset}$ 关于+算子不具有前同余性,而前同余性是进程代数中一个必备的性质。此时有两个选择:

(1)抛弃+算子;

(2)寻找一个包含于 $\underset{\sim}{\subset}$ 的最大的前同余关系。

Milner 在文献[10]中处理弱互模拟(weak-bisimulation)的等价关系 $\approx$ 时,遇到类似的问题,$\approx$ 关于+算子不具有同余性。Milner 给出了包含于 $\approx$ 的观测同余(observation-congurent)关系 $=$。

Hennessy 等在文献[8]中对最大前同余性进行了研究,但他们只考虑了有限的进程行为。为了刻画无限的进程行为,文中引入递归算子 rec$X.t$,将对包含递归算子的最大前同余关系进行研究。首先定义包含于 $\underset{\sim}{\subset}$ 二元关系集 $\underset{\sim}{\subset}^+$,接着研究环境、进程以及一步转换三者之间的关系,最后证明 $\underset{\sim}{\subset}^+$ 关系就是包含于 CLT 的最大前同余关系。

定义 9:$\underset{\sim}{\subset}^+$ 是一个满足如下两个条件的最大二元关系:

(1) $\underset{\sim}{\subset} \subseteq \underset{\sim}{\subset}$;

(2)对任意进程 r_1、r_2,若 $r_1 \underset{\sim}{\subset}^+ r_2$,则存在 $a \in \mathrm{Act}$ 使得 $r_1 + a.1 \underset{\sim}{\subset} r_2 + a.1$(其中 a 不在 r_1、r_2 中出现)。

$r_1 \simeq^+ r_2$ 与 $r_1 \simeq r_2$ 类似定义。

容易验证如果 $r_1 + a.1 \underset{\sim}{\subset} r_2 + a.1$,那么 $r_1 + b.1 \underset{\sim}{\subset} r_2 + b.1$(其中 a,b 不在 r_1,r_2 中出现)。所以将条件(2)中的存在改成任意是等价的定义。

下面证明 $\underset{\sim}{\subset}^+$ 是包含于 $\underset{\sim}{\subset}$ 的最大前同余关系。显然所有包含于 $\underset{\sim}{\subset}$ 的前同余关系都满足条件(2),所以只要证明 $\underset{\sim}{\subset}^+$ 具有前同余性(即,如果 $p \underset{\sim}{\subset}^+ q$,那么对任意环境 C_X 都有 $C_X\{p/X\} \underset{\sim}{\subset}^+ C_X\{q/X\}$)。为此,给出一些必要的引理。

引理 1(一步 $\xrightarrow{a}$ 转换):对任意的 $C_{\tilde{X}}$ 和 $\tilde{p}$,如果 $C_{\tilde{X}}\{\tilde{p}/\tilde{X}\} \xrightarrow{a} r$,则下面两个结论之一成立:

(1)存在 $C'_{\tilde{X}}$,使得 $r \equiv C'_{\tilde{X}}\{\tilde{p}/\tilde{X}\}$,并且对任意 $\tilde{q}$ 有 $C_{\tilde{X}}\{\tilde{q}/\tilde{X}\} \xrightarrow{a} C'_{\tilde{X}}\{\tilde{q}/\tilde{X}\}$。

(2)存在 p',$i \leqslant |\tilde{X}|$,$C'_{\tilde{X}}$,使 $r \equiv p'$,$p_i \xrightarrow{a} p'$,并且 $C_{\tilde{X}} \equiv X_i(+C'_{\tilde{X}})$(此处 $(+C'_{\tilde{X}})$ 表示可选项,即 $C_{\tilde{X}} \equiv X_i$ 或者 $C_{\tilde{X}} \equiv X_i + C'_{\tilde{X}}$,下文类似之处同理)。

证明:根据 $C_{\tilde{X}}$ 的形式分情形按 $C_{\tilde{X}}\{\tilde{p}/\tilde{X}\} \xrightarrow{a} r$ 的证明树的高度归纳易证。

引理 2(一步　转换):对任意的 $C_{\tilde{X}}$ 和 $\tilde{p}$,如果 $C_{\tilde{X}}\{\tilde{p}/\tilde{X}\}$　r,则下面两个结论之一成立:

(1)存在 $C'_{\tilde{X}}$,使得 $r \equiv C'_{\tilde{X}}\{\tilde{p}/\tilde{X}\}$,并且对任意 $\tilde{q}$ 有

$C_{\tilde{X}}\{\tilde{q}/\tilde{X}\}$ $C'_{\tilde{X}}\{\tilde{q}/\tilde{X}\}$。

(2)存在 p',$i \leqslant |\tilde{X}|$,$C'_{\tilde{X}}$,使得 $r \equiv p'$,p_i p',并且 $C_{\tilde{X}} \equiv X_i(+C'_{\tilde{X}})$。

证明:根据 $C_{\tilde{X}}$ 的形式分情形按 $C_{\tilde{X}}\{\tilde{p}/\tilde{X}\}$ r 的证明树的高度归纳易证。

引理 3:对任意的 $C_{\tilde{X}}$,$\tilde{p}$,$\tilde{q}$,如果 $\tilde{p} \subset \tilde{q}$,那么 $C_{\tilde{X}}\{\tilde{p}/\tilde{X}\} \xrightarrow{\surd}$ 蕴含 $C_{\tilde{X}}\{\tilde{q}/\tilde{X}\} \xrightarrow{\surd}$。

证明:根据 $C_{\tilde{X}}$ 的形式分情形按 $C_{\tilde{X}}\{\tilde{p}/\tilde{X}\} \xrightarrow{\surd}$ 的证明树的高度归纳易证。

引理 4:设式(1)为 $r \parallel C_{\tilde{X}}\{\tilde{q}/\tilde{X}\}$ 的一条极大计算路径。

$$r \parallel C_{\tilde{X}}\{\tilde{q}/\tilde{X}\}(\equiv r^0 \parallel q^0) \rightarrow r^1 \parallel q^1 \rightarrow r^2 \parallel q^2 \rightarrow \cdots \tag{1}$$

令

$\Omega_1 = \{k \mid$ 存在 $i \leqslant |\tilde{X}|$,$D'_{\tilde{X}}$,$D_{\tilde{X}}$,使得 $q_i \xrightarrow{a} q^k$,$q^{k-1} \equiv D_{\tilde{X}}\{\tilde{q}/\tilde{X}\}$,$D_{\tilde{X}} \equiv X_i(+D'_{\tilde{X}})\}$;

$\Omega_2 = \{k \mid$ 存在 $i \leqslant |\tilde{X}|$,$D'_{\tilde{X}}$,$D_{\tilde{X}}$,使得 q_i q^k,$q^{k-1} \equiv D_{\tilde{X}}\{\tilde{q}/\tilde{X}\}$,$D_{\tilde{X}} \equiv X_i(+D'_{\tilde{X}})\}$;

$\Omega = \Omega_1 \cup \Omega_2$。

则下面两个条件成立:

(1) $\Omega = \varnothing$,存在 $r \parallel C_{\tilde{X}}\{\tilde{p}/\tilde{X}\}$ 的一条与式(1)等长(式(1)无限时也无限)的计算路径。

$$r \parallel C_{\tilde{X}}\{\tilde{p}/\tilde{X}\}(\equiv r^0 \parallel p^0) \rightarrow r^1 \parallel p^1 \rightarrow r^2 \parallel p^2 \rightarrow \cdots \tag{2}$$

对任意的 j($j \leqslant$ 式(1)路径的长度),存在 $D^j_{\tilde{X}}$,使得 $p^j \equiv D^j_{\tilde{X}}\{\tilde{p}/\tilde{X}\}$ 并且 $q^j \equiv D^j_{\tilde{X}}\{\tilde{q}/\tilde{X}\}$。

(2) $\Omega \neq \varnothing$,令 $K = \min\Omega$,存在 $r \parallel C_{\tilde{X}}\{\tilde{p}/\tilde{X}\}$ 的一条计算路径:

$$r \parallel C_{\tilde{X}}\{\tilde{p}/\tilde{X}\}(\equiv r^0 \parallel p^0) \rightarrow r^1 \parallel p^1 \rightarrow \cdots \rightarrow r^{K-1} \parallel p^{K-1}$$

对任意的 $j(j < K)$,存在 $D^j_{\tilde{X}}$,使得 $p^j \equiv D^j_{\tilde{X}}\{\tilde{p}/\tilde{X}\}$ 并且 $q^j \equiv D^j_{\tilde{X}}\{\tilde{q}/\tilde{X}\}$。

证明:两种情形类似,下面讨论 $\Omega \neq \varnothing$ 的情形,显然只需构造出所有的 p^n($n < K$)即可。

(1) $n = 0$,取 $p^0 \equiv C_{\tilde{X}}\{\tilde{p}/\tilde{X}\}$。

(2)构造 $p^{n+1}(n < K-1)$。

因为存在 $D^n_{\tilde{X}}$ 使得 $p^n \equiv D^n_{\tilde{X}}\{\tilde{p}/\tilde{X}\}$,$q^n \equiv D^n_{\tilde{X}}\{\tilde{q}/\tilde{X}\}$,并且以下三种情形之一成立:

a) $r^n \xrightarrow{a} r^{n+1}$ 并且 $q^n \xrightarrow{\bar{a}} q^{n+1}$。

b) r^n r^{n+1} 并且 $q^n \equiv q^{n+1}$。

c) $r^n \equiv r^{n+1}$ 并且 q^n q^{n+1}。

下面只讨论情形 a),其余两种情形或者比 a)简单或者相似。

称 $q^n \xrightarrow{\bar{a}} q^{n+1}$ 的一步 $\xrightarrow{a}$ 转换引理中的结论(1)成立,否则结论(2)成立。那么存在 $i \leqslant |\tilde{X}|$,$D'_{\tilde{X}}$,使得 $q_i \xrightarrow{\bar{a}} q^{n+1}$ 并且 $q^n \equiv q_i(+D'_{\tilde{X}}\{\tilde{q}/\tilde{X}\})$,从而 $n+1 \in \Omega$,也就是 $n+1 \geqslant K$,矛盾于 $n+1 < K$。

所以,存在 $D^{n+1}_{\tilde{X}}$,使得 $q^{n+1} \equiv D^{n+1}_{\tilde{X}}\{\tilde{q}/\tilde{X}\}$ 并且 $p^n \equiv D^n_{\tilde{X}}\{\tilde{p}/\tilde{X}\} \xrightarrow{\bar{a}} D^{n+1}_{\tilde{X}}\{\tilde{p}/\tilde{X}\}$(记为 p^{n+1}),从而 $r^n \parallel p^n \rightarrow r^{n+1} \parallel p^{n+1}$。

引理 5:如果 $p \not\xrightarrow{\surd}$,$r_2 \not\xrightarrow{\surd}$,$p$ must $r_1 + r_2$ 并且 $p \parallel r_1 \rightarrow$,那么 p must r_1。

证明:因为 $p \parallel r_1 \rightarrow$,$p \not\xrightarrow{\surd}$,所以 $p \parallel r_1$ 的所有极大计算路径都可以通过 $r_1 + r_2$ 替换 r_1,得到 $p \parallel r_1 + r_2$ 的极大计算路径。又因为 p must $r_1 + r_2$ 并且 $r_2 \not\xrightarrow{\surd}$,所以 p must r_1。

引理 6:如果 $p \subset^+ q$,$q \overset{a}{\Rightarrow} \surd$,那么 p $\surd$ 或者 $p \xrightarrow{a} \surd$。

证明:假设 $p \subset^+ q$,$q \overset{a}{\Rightarrow} \surd$,从而存在 $l \in \mathrm{Act}$(l 不在 p、q 中出现),使得 $p + l.1 \subset q + l.1$,并且 $\bar{a}.\Theta + \bar{l}.1$ must $q + \bar{l}.1$。因此 $\bar{a}.\Theta + \bar{l}.1$ must $p + \bar{l}.1$,从而 $\bar{a}.\Theta \parallel p \rightarrow$,所以 p $\surd$ 或者 $p \xrightarrow{a} \surd$。

定理 1:对任意进程 $\tilde{p}$、$\tilde{q}$,环境 $C_{\tilde{X}}$,如果 $\tilde{p} \subset^+ \tilde{q}$,那么 $C_{\tilde{X}}\{\tilde{p}/\tilde{X}\} \subset C_{\tilde{X}}\{\tilde{q}/\tilde{X}\}$。

证明:使用反正法。假设存在进程 r 使得 r must $C_{\tilde{X}}\{\tilde{p}/\tilde{X}\}$ 并且 r must $C_{\tilde{X}}\{\tilde{q}/\tilde{X}\}$。构造 $r \parallel C_{\tilde{X}}\{\tilde{p}/\tilde{X}\}$ 的一条极大不成功计算路径。

因为 r must $C_{\tilde{X}}\{\tilde{q}/\tilde{X}\}$,所以存在一条 $r \parallel C_{\tilde{X}}\{\tilde{q}/\tilde{X}\}$ 的极大不成功计算路径:

$$r \parallel C_{\tilde{X}}\{\tilde{q}/\tilde{X}\}(\equiv r^0 \parallel q^0) \rightarrow r^1 \parallel q^1 \rightarrow \cdots \tag{3}$$

令 $\Omega = \Omega_1 \cup \Omega_2$(与引理 4 中的定义一致)。按 Ω 是否为空分两种情形讨论。

情形 1:$\Omega = \varnothing$。

由引理 4 可知,存在 $r \parallel C_{\tilde{X}}\{\tilde{p}/\tilde{X}\}$ 的一条计算路径:

$r \parallel C_{\tilde{X}}\{\tilde{p}/\tilde{X}\}(\equiv r^0 \parallel p^0) \to r^1 \parallel p^1 \to r^2 \parallel p^2 \cdots$ (4)

并且对任意的 $j(j \leqslant$ 式(3)路径的长度),存在 $D^j_{\tilde{X}}$,使得 $p^j \equiv D^j_{\tilde{X}}\{\tilde{p}/\tilde{X}\}$ 并且 $q^j \equiv D^j_{\tilde{X}}\{\tilde{q}/\tilde{X}\}$。

情形 1.1:式(3)无限。

那么式(4)也是无限的。由引理 3 可知,对所有的 $j < \omega$ 有 $p^j \xrightarrow{\surd}$。所以式(4)是一条极大的不成功计算路径。

情形 1.2:式(3)有限。

那么存在 $k < \omega$,使得式(3)具有如下形式:

$r \parallel C_{\tilde{X}}\{\tilde{q}/\tilde{X}\}(\equiv r^0 \parallel q^0) \to r^1 \parallel q^1 \to \cdots \to r^k \parallel q^k \not\to$

由引理 4 可知,存在 $r \parallel C_{\tilde{X}}\{\tilde{p}/\tilde{X}\}$ 的一条计算路径:$r \parallel C_{\tilde{X}}\{\tilde{p}/\tilde{X}\}(\equiv r^0 \parallel p^0) \to r^1 \parallel p^1 \to \cdots \to r^k \parallel p^k$。下面用反证法证明 $r^k \parallel p^k \not\to$。假设存在 r^{k+1},p^{k+1},使得 $r^k \parallel p^k \to r^{k+1} \parallel p^{k+1}$。因为 $r^k \parallel q^k \not\to$,所以 $r^k \not/$。从而存在 $a \in \mathrm{Act}$ 使得 $r^k \xrightarrow{\bar{a}} r^{k+1}$ 并且 $p^k \xrightarrow{a} p^{k+1}$,或者 $r^k \equiv r^{k+1}$ 并且 p^k　p^{k+1}。下面分别讨论:

情形 1.2.1:$r^k \xrightarrow{\bar{a}} r^{k+1}$ 并且 $p^k \xrightarrow{a} p^{k+1}$。

因为 $p^k \equiv D^k_{\tilde{X}}\{\tilde{p}/\tilde{X}\}$,$q^k \equiv D^k_{\tilde{X}}\{\tilde{q}/\tilde{X}\}$,所以引理 1 的两个结论之一成立。

情形 1.2.1.1:结论(1)成立。

存在 $D'_{\tilde{X}}$,使得 $p^{k+1} \equiv D'_{\tilde{X}}\{\tilde{p}/\tilde{X}\}$ 并且 $D^k_{\tilde{X}}\{\tilde{q}/\tilde{X}\} \xrightarrow{a} D'_{\tilde{X}}\{\tilde{q}/\tilde{X}\}$,所以 $r^k \parallel q^k \to r^{k+1} \parallel D'_{\tilde{X}}\{\tilde{q}/\tilde{X}\}$,矛盾于 $r^k \parallel q^k \not\to$　。

情形 1.2.1.2:结论(2)成立。

存在进程 p',$i < |\tilde{X}|$,$D'_{\tilde{X}}$,使得 $p^{k+1} \equiv p'$,$p_i \xrightarrow{a} p'$ 并且 $D^k_{\tilde{X}} \equiv X_i(+D'_{\tilde{X}})$。

情形(a):$D^k_{\tilde{X}} \equiv X_i + D'_{\tilde{X}}$。

那么 $p^k \equiv p_i + D'_{\tilde{X}}\{\tilde{p}/\tilde{X}\}$,$q^k \equiv q_i + D'_{\tilde{X}}\{\tilde{q}/\tilde{X}\}$。因为 $p^k \xrightarrow{\surd}$,所以 $D'_{\tilde{X}}\{\tilde{p}/\tilde{X}\} \xrightarrow{\surd}$。由 r must $C_{\tilde{X}}\{\tilde{p}/\tilde{X}\}$,由文献[8]命题 3 可知 r^k must p^k。由引理 5 可知 r^k must p_i,从而 r^k must q_i。另一方面,因为 $r^k \parallel q^k(\equiv q_i + D'_{\tilde{X}}\{\tilde{q}/\tilde{X}\}) \not\to$,$q^k \xrightarrow{\surd}$,所以 r^k must q_i,互相矛盾。

情形(b):$D^k_{\tilde{X}} \equiv X_i$ 可以看成是情形(a)中 $D'_{\tilde{X}} \equiv 0$ 的一个特例。

情形 1.2.2:$r^k \equiv r^{k+1}$ 并且 p^k　p^{k+1}。

因为 $p^k \equiv D^k_{\tilde{X}}\{\tilde{p}/\tilde{X}\}$,$q^k \equiv D^k_{\tilde{X}}\{\tilde{q}/\tilde{X}\}$,所以引理 2 的两个结论之一成立。证明与情形 1.2.1 类似。

情形 2:$I \neq \varnothing$。

令 $K \in \min\Omega$,由引理 4 可知存在 $r \parallel C_{\tilde{X}}\{\tilde{p}/\tilde{X}\}$ 的一条计算路径:$r \parallel C_{\tilde{X}}\{\tilde{p}/\tilde{X}\}(\equiv r^0 \parallel p^0) \to r^1 \parallel p^1 \to \cdots \to r^{K-1} \parallel p^{K-1}$,并且对任意的 $j(j \leqslant K)$,存在 $D^j_{\tilde{X}}$,使得 $p^j \equiv D^j_{\tilde{X}}\{\tilde{p}/\tilde{X}\}$、$q^j \equiv D^j_{\tilde{X}}\{\tilde{q}/\tilde{X}\}$。将式(1)中的 q^{K-1} 替换为 q_i 后得到 $r^{K-1} \parallel q_i$ 的一条极大不成功计算路径:$r^{K-1} \parallel q_i \to r^K \parallel q^K \to \cdots$。所以得出 $q_i \xrightarrow{a} q^K$ 且 $r^{K-1} \xrightarrow{\bar{a}} r^K$,或者 q_i　q^K 且 $r^{K-1} \equiv r^K$。

情形 2.1:$q_i \xrightarrow{a} q^K$,$r^{K-1} \xrightarrow{\bar{a}} r^K$。

关于 p_i 是否属于 U_{clt} 分情形讨论。

情形 2.1.1:$p_i \notin U_{\mathrm{clt}}$。

因为 $q_i \xrightarrow{a} \surd q^K$,$p \subset^+ q$,由引理 6 可知 p_i　或者 $p_i \xrightarrow{a} \surd$。

情形 2.1.1.1:p_i　。

情形(a):$r^{K-1} \Uparrow$　。

那么存在无限序列 r^{K-1}　r^1_1　r^2_1　…,所以 $r \parallel C_{\tilde{X}}\{\tilde{p}/\tilde{X}\} \to \cdots \to r^{K-1} \parallel p^{K-1} \to r^1_1 \parallel p^{K-1} \to \cdots$ 是一条极大的不成功计算路径。

情形(b):$r^{K-1} \Downarrow$　。

那么存在 r',使得 $r^{K-1} \overset{\varepsilon}{\Rightarrow} r' \not/$。因为 $p_i \notin U_{\mathrm{clt}}$,所以 r' must p_i,从而存在 $r' \parallel p_i$ 的一条极大不成功计算路径:$r' \parallel p_i(\equiv r^0_2 \parallel p^0_2) \to r^1_2 \parallel p^1_2 \to \cdots$。因为 p_i　,$p^{K-1} \equiv p_i(+D'_{\tilde{X}}\{\tilde{p}/\tilde{X}\})$,从而 $r' \parallel p^{K-1} \to r^1_2 \parallel p^1_2$。所以,$r \parallel C_{\tilde{X}}\{\tilde{p}/\tilde{X}\} \to \cdots \to r^{K-1} \parallel p^{K-1} \to \cdots \to r^1_2 \parallel p^1_2 \to \cdots$ 是 $r \parallel C_{\tilde{X}}\{\tilde{p}/\tilde{X}\}$ 的一条极大不成功计算路径。

情形 2.1.1.2:$p_i \xrightarrow{a} \surd$ 并且 $p_i \not/$。

那么 $\bar{a}.r^K \parallel p_i \to$。因为 $p_i \notin U_{\mathrm{clt}}$,所以 $\bar{a}.r^K$ must p_i,从而存在 $\bar{a}.r^K \parallel p_i$ 的一条极大不成功计算路径:$\bar{a}.r^K \parallel p_i(\equiv r^0_3 \parallel p^0_3) \to r^1_3 \parallel p^1_3 \to \cdots$,并且 $r^1_3 \equiv r^K$。进而 $r^{K-1} \parallel p^{k-1} \to r^1_3 \parallel p^1_3$,因此 $r \parallel C_{\tilde{X}}\{\tilde{p}/\tilde{X}\} \to r^1 \parallel p^1 \to \cdots \to r^{K-1} \parallel p^{K-1} \to r^1_3 \parallel p^1_3 \to \cdots$ 是极大的不成功计算路径。

情形 2.1.2:$p_i \in U_{\mathrm{clt}}$。

因为 $q_i \xrightarrow{a} \surd q^K$,$\tilde{p} \subset \tilde{q}$,所以由文献[8]命题 4.8 可知 $p_i \overset{a}{\Rightarrow} \surd$。令 $I = \{p \mid p_i \overset{a}{\Rightarrow} \surd p\}$,所以 $I \neq \varnothing$。下面利用反正法证明存在 $p' \in I$ 使得 r^K must p'。

假设对所有的 $p_i \overset{a}{\Rightarrow} \surd p'$ 都有 r^K must p',那么 $\bar{a}.r^K$ must p_i,从而 $\bar{a}.r^K$ must q_i,所以 r^K must q^K,与式(3)是

一条极大不成功计算路径矛盾。

因为 $p^{k-1}\overset{a}{\Rightarrow}\surd p'$，$r^{K-1}\xrightarrow{\bar{a}}r^K$，从而 $r^{K-1}\parallel p^{k-1}\Rightarrow\surd r^K\parallel p'$，所以存在 $r\parallel C_{\tilde{X}}\{\tilde{p}/\tilde{X}\}$ 的极大不成功计算路径：

$r\parallel C_{\tilde{X}}\{\tilde{p}/\tilde{X}\}\rightarrow\cdots r^{K-1}\parallel p^{K-1}\Rightarrow\surd r^K\parallel p'\rightarrow r_4^1\parallel p_4^1\cdots$

情形 2.2：$q_i\quad q^K, r^{K-1}\equiv r^K$

如果能证明 $p_i\quad\surd$ 或者 $p_i\xrightarrow{a}\surd$ 且 $r^{K-1}\overset{\bar{a}}{\Rightarrow}$，则同情形 2.1 相似，可证。

按式(5)是否有限分情形讨论。

$$r^{K-1}\parallel q_i(\equiv r_5^0\parallel q_5^0)\rightarrow r^K\parallel q^K(\equiv r_5^1\parallel q_5^1)\rightarrow\cdots \tag{5}$$

情形 2.2.1：式(5)有限。

那么存在 $s\in \mathrm{Act}^*, n<\omega$，使得 $r^{K-1}\overset{s}{\Rightarrow}r_5^n, q_i\overset{s}{\Rightarrow}q_5^n$ 并且 $r_5^n\parallel q_5^n\not\rightarrow$。

情形(a)：$s\equiv\varepsilon$。

那么 $\bar{l}.\Theta$ must $q_i+l.1$，从而 $\bar{l}.\Theta$ must $p_i+l.1$，所以 $p_i\quad\surd$。

情形(b)：$s\equiv a.s'$。

那么存在 q'，使得 $q_i\overset{a}{\Rightarrow}\surd q'$。由引理 5 可知 p_i $\surd$ 或者 $p_i\xrightarrow{a}\surd$。

情形 2.2.2：式(5)无限。

情形(a)：$r^{K-1}\Uparrow$（同情形 2.1.1.1(a)）。

情形(b)：$q_i\Uparrow$。

那么 $\bar{l}.\Theta$ must $q_i+l.1$，从而 $\bar{l}.\Theta$ must $p_i+l.1$，所以 $p_i\quad\surd$。

情形(c)：存在 r', q'，使得 $r^{K-1}\overset{\bar{a}}{\Rightarrow}r', q_i\overset{a}{\Rightarrow}\surd q'$。

所以，由引理 6 可知，$p_i\quad\surd$ 或者 $p_i\xrightarrow{a}\surd$。

所以，$p_i\quad\surd$ 或者 $p_i\xrightarrow{a}\surd$ 且 $r^{K-1}\overset{\bar{a}}{\Rightarrow}$。

定理 2：对任意进程 $\tilde{p}$、$\tilde{q}$，环境 $C_{\tilde{X}}$，如果 $\tilde{p}\subset^+\tilde{q}$，那么 $C_{\tilde{X}}\{\tilde{p}/\tilde{X}\}\subset^+ C_{\tilde{X}}\{\tilde{q}/\tilde{X}\}$。

证明：根据定理 1 易证。

上述结论说明，给出的关系 $\subset^+$ 具有前同余性，并且是最大的包含于 $\subset$ 的关系，所以 $\subset^+$ 是包含于 $\subset$ 的最大前同余关系。

3 结束语

在进程代数理论发展中，提出了许多刻画进程语义的概念[11-17]。为了刻画无限的进程行为，文中基于 CLT 语义，研究环境、递归进程的展开与进程转换之间的内在联系，给出了一步转换背后的模式以及含递归算子的进程间的关系集 $\subset^+$，并证明 $\subset^+$ 就是包含于 $\subset$ 的最大前同余关系。

文中的研究只是相关领域的一部分，针对不同问题还有许多值得研究的方向，如：mutually must-testing semantic（P2P）的含递归算子的最大前同余性，CLT、P2P 方程唯一解和最大解等等。

参考文献：

[1] DeNicola R, Hennessy M. Testing equivalences for processes [J]. ELSEVIER, 1983, 34(1-2): 83-133.

[2] Hennessy M. Algebraic theory of processes[M]. [s. l.]: MIT Press, 1988.

[3] DeNicola R, Hennessy M. Ccs without tau's[M]//LNCS. Berlin: Springer, 1987: 138-152.

[4] Castagna G, Gesbert N, Padovani L. A theory of contracts for web services[J]. ACM SIGPLAN Notices, 2008, 31(5): 261-272.

[5] Barbanera F, De'Liguoro U. Two notions of sub-behaviour for session-based client/server systems[C]//Proc of PPDP. New York: ACM, 2010: 155-164.

[6] Laneve C, Padovani L. The must preorder revisited[M]// CONCUR 2007 - concurrency theory. Berlin: Springer, 2007: 212-225.

[7] Padovani L. Contract-based discovery of web services modulo simple orchestrators[J]. Theoretical Computer Science, 2010, 411(37): 3328-3347.

[8] Bernardi G, Hennessy M. Mutually testing processes[J]. Logical Methods in Computer Science, 2015, 11(2): 61-75.

[9] Plotkin G. A structural approach to operational semantics[R]. Aarhus: Aarhus University, 1981.

[10] Milner R. Communication and concurrency[M]. [s. l.]: Prentice Hall, 1989.

[11] Keller R M. Formal verification of parallel programs[J]. Communications of ACM, 1976, 19(7): 371-384.

[12] van Glabbeek R J. The linear time-branching time[M]. Berlin: Springer, 1990: 278-297.

[13] Hoare C A R. Communicating sequential process[J]. Communications of the ACM, 1978, 21(8): 666-677.

[14] Milner R. An algebraic definition of simulation between programs[C]//Proc of the 2nd international joint conference on artificial intelligence. San Francisco: Morgan Kaufmann Publisher, 1971: 481-489.

[15] Park D. Concurrency and automata on infinite sequences[M]. Berlin: Springer, 1981: 167-183.

[16] Bloom B, Istrail S, Meyer A R. Bisimulation can't be traced [J]. Journal of ACM, 1995, 42(1): 232-268.

[17] Lrsen K G, Skou A. Bisimulation through probabilistic testing [J]. Information and Computation, 1991, 94(1): 84-94.