数据传送进程的符号互模拟*

林惠民

(中国科学院软件研究所,北京 100080)

摘要 本文提出数据传送进程的符号迁移语义,引入符号互模拟的概念,证明了两个进程在传统意义下互模拟当且仅当它们符号互模拟.由于无穷域上的数据传送进程的传统迁移图是无穷的,而其中相当一部分的符号迁移图是有穷的,文章的结果为在有穷时间和空间内判定这类进程的互模拟关系开辟了可能性.

关键词 通讯进程,进程代数,互模拟.

CSP[1]和CCS[2]最初都是作为描述通讯进程的语言而提出的."通讯"指的是进程间可通过通道传送数据以实现协作.但是在随后的理论发展中,为了数学处理的方便,进程间的数据传送被简化为单纯的同步.从原先的数据传送语言(也称"完全语言")到单纯同步语言(也称"基本语言"或"纯语言")的过渡由一转换实现[2],其核心步骤是将输入前缀翻译成遍历数据域Val的选择算子:

$$\{\!|c?x.\,p|\!\}=\sum_{v\in Val}c?v.\{\!|P[v/x]|\!\}$$

当Val无穷时,$\sum_{v\in Val}$是无穷算子.

由于关于进程代数的大量理论结果均假定选择算子是有穷的,这些结果不适用于无穷域上的数据传送进程.由于同样的原因,现有的进程代数验证工具[3-6]也不能应用于数据传送进程.

如何避免上述转换,直接建立数据传送进程的语义理论,遂成为进程代数走向实际应用的关键环节,也是近年来该领域的一个研究热点.

本文提出对于数据传送进程的符号迁移语义,在此基础上引入符号互模拟的概念.这里"符号"一词意味着我们不将输入变量实例化,也不对数据和布尔表达式计值,而是把它们当作符号来处理.采用符号化方法在很多情形下可以避免传统迁移语义和互模拟概念涉及的无穷性.比如进程

$$P=c?x.\,if\ x\geqslant 0\ then\ \tau.d!x.P\ else\ \tau.d!-x.P$$

的传统迁移图是无穷的(图1左),而它的符号迁移图却是有穷的(图1中).若另有

---

* 本文1993-08-12收到,1993-12-18定稿

作者林惠民,1947年生,研究员,主要研究领域为分布式系统的代数理论与验证工具,程序模块理论,代数规范,时序逻辑.

本文通讯联系人:林惠民,北京 100080,中国科学院软件研究所

$$Q=c?x.\ \tau.d!|x|.Q$$

($|x|$表示 x 的绝对值),则以布尔表达式加标的关系族 $S=\{S^{true},S^{x\geqslant 0},S^{x<0}\}$,其中

$$S^{true}=\{(P,Q),(P_1,Q_1)\}$$

$$S^{x<0}=\{P_{21},Q_2\}$$

$$S^{x\geqslant 0}=\{(P_{22},Q_2)\}$$

就是 P 与 Q 之间的一个符号互模拟(略去恒等和对称的对偶).

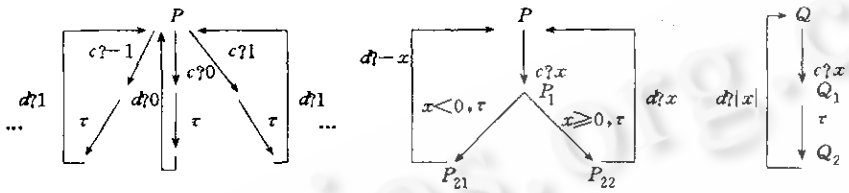

图1

我们的主要结果是:两个进程符号互模拟当且仅当它们在传统意义下互模拟.换句话说,判定进程间的互模拟可归结为判定符号互模拟.由于相当一部分数据传送进程具有有穷的符号迁移图,我们的结果为在有穷时间和空间内判定这类进程的互模拟关系提供了理论基础.

本文中所报告的工作是作者与英国 Sussex 大学 Hennessy 教授合作完成的.

1 数据传送 CCS 及互模拟

我们所考虑的进程语言由如下 BNF 语法给出:

$$t::=\mathbf{0}\mid a.t\mid b\rightarrow t\mid t+t\mid t|t\mid t\backslash c\mid P(\tilde{e})$$

$$a::=\tau\mid c?x\mid c!e$$

其中 $b\in BExp$ 是布尔表达式,$e\in DExp$ 是数据表达式;它们的具体语法形式不在这里规定,可以看作是我们进程语言的参数.本文中的例子均以整数为数据域.$c\in chan$ 是通道名.$\tilde{e}$ 表示表达式列.

这就是文献[2]中的"完全 CCS":$\mathbf{0}$ 是空进程,$\cdot$ 是动作前缀,$\rightarrow$ 是卫式命令[7];$+$ 是非确定选择,$|$ 是并行,$\backslash$ 是通道限制,P 是递归定义的进程名,τ 是表示内部通讯的不可见动作,$c?x$ 表示从通道 c 输入数据到 x,$c!e$ 表示向通道 c 输出 e.对应于每个进程名 P 有一声明

$$P(\tilde{x})\Leftarrow t\qquad fv(t)\subseteq\{\tilde{x}\}.$$

输入前缀 $c?x.t$ 引入受囿变量 x,其辖域是 t.我们用 $fv(t)$ 表示 t 中的自由变量集.称不含自由变量的项为闭项或进程,用 p,q 表示;可能含自由变量的项为开项,用 t,u 表示.项之间的语法恒等记作$\equiv$,$\alpha-$等价记作$\equiv_\alpha$.

我们假定可数无穷数据变量集 Var,其元素用 x,y,z 表示,数据值域 Val,其元素用 v 表示.映射 $\rho:Var\rightarrow Val$ 称为计值;$\rho\{v/x\}$ 表示除在 x 处取值为 v 外,其余都与 ρ 相同的计值.我们用 $t[e/y]$ 表示用 e 替换 t 中自由出现的 y 所得到的项(必要时将 t 中受囿变量换名以避免名字冲突).对任意数据表达式 e,假定 $\rho(e)\in Val$,即计值总是终止的;同样地对布尔表达式 b,$\rho(b)\in\{true,false\}$.我们用 $b=b'$ 表示对任意 ρ 只要 $\rho(b)=true$ 就有 $\rho(b')=true$;

$b=b'$ 表示 $b\models b'$ 并且 $b'\models b$. 设 $B=\{b_i\mid i\in I\}$，$\vee B$ 表示 $\bigvee_{i\in I} b_i$.

对于数据传送进程，可以定义两种不同的互模拟关系，分别称为早互模拟和迟互模拟[8]. 考虑进程

$$c?x.\ x\geqslant 0\rightarrow P+c?x.\ x<0\rightarrow P$$

和

$$c?x.\ P+c?x.\ 0$$

其中 P 是不同于 0 的进程. 如果我们认为进程所执行的输入动作均形如 $c?\ k$(k 为整数)，那么这两个进程互模拟等价，因为一进程的每个动作都能被另一进程所模拟. 但是如果我们考虑更为一般的输入动作 $c?$，那么这两个进程就不等价，因为第一个进程能做一 $c?$ 动作而变成 $\lambda x.\ x\geqslant 0\rightarrow P$，而第二个进程不能. 在前一观点下的互模拟称为早互模拟，后一观点下的互模拟称为迟互模拟. 限于篇幅本文中只讨论早互模拟. 对于迟互模拟可以建立平行的结果，这留给有兴趣的读者作为练习.

上述进程语言的早迁移语义[9]见表 1. 注意我们只给出闭项即进程的语义，从表中可以看出早迁移语义的动作有 τ，$c!v$ 和 $c?v$ 三种，其中 c 是通道名，v 是数据值.

表 1　传统迁移语义(略去关于＋和∣的对称的规则)

$\tau.\ p\xrightarrow{\tau}_e p$	$c\in chan,\llbracket e\rrbracket=v$
$c?\ x.\ p\xrightarrow{c?v}_e p[v/x]$	$c\in chan,v\in Val$
$p\xrightarrow{a}_e p'\Rightarrow p+q\xrightarrow{a}_e p'$	
$p\xrightarrow{a}_e p'\Rightarrow p\mid q\xrightarrow{a}_e p'\mid q$	
$p\xrightarrow{c?v}_e p',q\xrightarrow{c!v}_e q'\Rightarrow p\mid q\xrightarrow{\tau}_e p'\mid q'$	
$p\xrightarrow{a}_e p'\Rightarrow p\backslash c\xrightarrow{a}_e p'\backslash c$	$a\neq c$
$p\xrightarrow{a}_e p'\Rightarrow b\rightarrow p\xrightarrow{a}_e p'$	$\llbracket b\rrbracket=true$
$t[\tilde{v}/\tilde{x}]\xrightarrow{a}_e p'\Rightarrow p(\tilde{v})\xrightarrow{a}_e p'$	$p(\tilde{x})\Leftarrow t$ 是声明

定义 1.1.（**强互模拟**）进程间的对称关系 R 称为是强互模拟，如果它满足：对任意 $(p,q)\in R$，只要 $p\xrightarrow{a}_e p'$，就有 $q\xrightarrow{a}_e q'$ 且 $(p',q')\in R$.

令 $\sim_e=\bigcup\{R\mid R$ 是强互模拟$\}$，即 $\sim_e$ 是最大的强互模拟关系.

预理 1.1. $\equiv_e$ 是强互模拟.

证明：对迁移 $p\xrightarrow{a}_e q$ 的推导长度施归纳可证，若 $p\equiv_e q$ 且 $p\xrightarrow{a}_e p'$，则存在 $q'\equiv_e p'$，$q\xrightarrow{a}_e q'$. □

按表 1 的迁移规则，当 Val 无穷时，输入进程 $c?\ x.\ t$ 有穷多个形为 $\xrightarrow{c?v}_e$ 的迁移. 因此在确定两个输入进程是否互模拟时，需要作无穷多次比较. 下面我们将引入另一种迁移语义和互模拟关系，以避免这种无穷性.

2　符号迁移语义

上节中我们看到传统语义产生无穷多迁移的原因在于输入变量被实例化为所有的数据

值. 在所谓符号迁移语义中，我们将不对输入变量实例化，从而也不对布尔及数据表达式计值. 这些表达式将“符号式”地保留在操作语义中.

表 2 列出了我们进程语言的符号迁移规则. 它们规定了开项之间的符号迁移关系 $\xrightarrow{b,\alpha}_E$，其中 b 是布尔表达式，$\alpha\in\{\tau,c!e,c?x\mid c\in chan,x\in Var,e\in DExp\}$ 是抽象动作. 我们时常将 $\xrightarrow{true,\alpha}_E$ 简写为 $\xrightarrow{\alpha}_E$. 直观地说，$\xrightarrow{b,\alpha}_E$ 表示“b 引发 α”，即 α 迁移当 b 为真时发生，否则不发生.

表 2　符号迁移语义(略去关于+和|的对称规则)

$a.t\xrightarrow{true,a}_E t$	$\alpha\in\{\tau,c!e,\mid c\in chan,e\in DExp\}$
$c?x.t\xrightarrow{true,c?y}_E t[y/x]$	$y\notin fv(c?x.t)$
$t\xrightarrow{b,\alpha}_E t'\Rightarrow t+u\xrightarrow{b,\alpha}_E t'$	
$t\xrightarrow{b,\alpha}_E t'\Rightarrow t\mid u\xrightarrow{b,\alpha}_E t'\mid u$	$bv(\alpha)\cap fv(u)=\varnothing$
$t\xrightarrow{b,c?x}_E t',u\xrightarrow{b',c!e}_E u'\Rightarrow t\mid u\xrightarrow{b\wedge b',\tau}_E t'[e/x]\mid u'$	
$t\xrightarrow{b,\alpha}_E t'\Rightarrow b'\to t\xrightarrow{b\wedge b',\alpha}_E t'$	
$t\xrightarrow{b,\alpha}_E t'\Rightarrow t\backslash c\xrightarrow{b,\alpha}_E t'\backslash c$	a 中不出现 c
$t[\tilde{e}/\tilde{x}]\xrightarrow{b,\alpha}_E t'\Rightarrow p(\tilde{e})\xrightarrow{b,\alpha}_E t'$	$p(\tilde{x})\Leftarrow t$ 是声明

预理 2.1. 若 $t\xrightarrow{b,c?x}_E t'$，则 $fv(b)\in fv(t),x\notin fv(t)$.

证明：施归纳于迁移的推导长度. □

前面说过在 $c?x.t$ 中 x 是受囿变量. 下面的预理告诉我们，在 α－等价的意义下，符号输入动作中变量的具体取名是无关紧要的.

预理 2.2. 若 $t\xrightarrow{b,c?x}_E u,y\notin fv(t)$，则存在 $u'\equiv_\alpha u[y/x],t\xrightarrow{b,c?y}_E u'$.

证明：施归纳于迁移的推导长度. □

下面三个预理建立了符号迁移语义与上节中定义的传统迁移语义之间的联系.

预理 2.3. (1)若 $t\rho\xrightarrow{\tau}_e p$，则存在 b,t'，满足 $\rho\models b,p\equiv_\alpha t'\rho,t\xrightarrow{b,\tau}_E t'$.

(2)若 $t\xrightarrow{b,\tau}_E t',\rho\models b$，则存在 $p\equiv_\alpha t'\rho,t\rho\xrightarrow{\tau}_e p$.

预理 2.4. (1)若 $t\rho\xrightarrow{c!v}_e p$，则存在 b,e,t'，满足 $\rho\models b,\rho(e)=v,p\equiv_\alpha t'\rho,t\xrightarrow{b,c!e}_E t'$.

(2)若 $t\xrightarrow{b,c!e}_E t',\rho\models b$，则存在 $p\equiv_\alpha t'\rho,t\rho\xrightarrow{c!v}_e p$，其中 $v=\rho(e)$.

预理 2.5. (1)若 $t\rho\xrightarrow{c?v}_e p,x\notin fv(t)$，则存在 b,t'，满足 $\rho\models b,p\equiv_\alpha t'\rho\{v/x\},t\xrightarrow{b,c?x}_E t'$.

(2)若 $t\xrightarrow{b,c?x}_E t',\rho\models b$，则对任意 $v\in Val$，存在 $p\equiv_\alpha t'\rho\{v/x\},t\rho\xrightarrow{c?v}_e p$.

证明：为节省篇幅，这里只给出预理 2.5 的证明. 其余两个的证明均类似.

(1)施归纳于迁移 $t\rho\xrightarrow{c?v}_e p$ 的推导.

• $(c?y.u)\rho\xrightarrow{c?v}_e u\rho\{v/y\}$. 则 $c?y.u\xrightarrow{true,c?x}_E u[x/y]$，且 $u\rho\{v/y\}\equiv_\alpha u[x/y]\rho\{v/x\}$.

• $(u|u')\rho\xrightarrow{c?v}_e p|u'\rho$ 是由于 $u\rho\xrightarrow{c?v}_e p$. 由归纳假设,存在 b、t',$\rho\models b$,$p\equiv_a t'\rho\{v/x\}$,$u\xrightarrow{b,c?x}_E t'$. 于是 $u|u'\xrightarrow{b,c?x}_E t'|u'$,且 $p|u'\rho\equiv_a t'\rho\{v/x\}|u'\rho\equiv t'\rho\{v/x\}|u'\rho\{v/x\}\equiv(t'|u')\rho\{v/x\}$.

• $(b\to u)\rho\xrightarrow{c?v}_e p$ 是由于 $\rho\models b$ 且 $u\rho\xrightarrow{c?v}_e p$. 由归纳假设,存在 b',t',$\rho\models b'$,$p\equiv_a t'\rho\{v/x\}$,$u\xrightarrow{b',c?x}_E t'$. 于是 $b\to u\xrightarrow{b\wedge b',c?x}_E t'$.

• $P(\tilde{e})\rho\xrightarrow{c?v}_e p$ 是由于 $u[\tilde{e}\rho/\tilde{y}]\xrightarrow{c?v}_e p$,这里 $P(\tilde{y})\Leftarrow u$ 是递归定义,$fv(u)\subseteq\{\tilde{y}\}$. 故 $u[\tilde{e}\rho/\tilde{y}]=u[\tilde{e}/\tilde{y}]\rho$. 由归纳假设,存在 b,t',$\rho\models b$,$p\equiv_a t'\rho\{v/x\}$,且 $u[\tilde{e}/\tilde{y}]\rho\xrightarrow{b,c?x}_E t'$. 从而 $P(\tilde{e})\xrightarrow{b,c?x}_E t'$.

• 其余情形类似.

(2)施归纳于符号迁移 $t\xrightarrow{b,c?x}_E t'$ 的推导.

• $c?y.u\xrightarrow{true,c?x}_E u[x/y]$,$x\notin fv(c?y.u)$. 我们有 $(c?y.u)\rho\xrightarrow{c?v}_e u[v/y]\rho\equiv_a u[x/y]\rho\{v/x\}$.

• $u|u'\xrightarrow{b,c?x}_E t'|u'$ 是因为 $u\xrightarrow{b,c?x}_E t'$. 由归纳假设,$u\rho\xrightarrow{c?v}_e p\equiv_a t'\rho\{v/x\}$. 由预理 2.1,$x\notin fv(u|u')=fv(u,u')$. 我们有 $(u|u')\rho\xrightarrow{c?v}_e p|u'\rho\equiv_a t'\rho\{v/x\}|u'\rho\equiv(t'|u')\rho\{v/x\}$.

• $b\to u\xrightarrow{b\wedge b',c?x}_E t'$ 是因为 $u\xrightarrow{b',c?x}_E t'$. 从 $\rho\models b\wedge b'$ 知 $\rho\models b'$ 且 $\rho\models b$. 由归纳假设 $u\rho\xrightarrow{c?v}_e p\equiv_a t'\rho$. 于是 $(b\to u)\rho\xrightarrow{c?v}_e p$.

• $P(\tilde{e})\xrightarrow{b,c?x}_E t'$ 是因为 $u[\tilde{e}/\tilde{y}]\xrightarrow{b,c?x}_E t'$,这里 $P(\tilde{y})\Leftarrow u$,$fv(u)\subseteq\{\tilde{y}\}$ 是递归定义. 由归纳假设,$u[\tilde{e}/\tilde{y}]\rho\xrightarrow{c?v}_e p\equiv_a t'\rho\{v/x\}$,即 $u(\tilde{e}\rho/\tilde{y})\xrightarrow{c?v}_e p$,从而 $P(\tilde{e})\rho=P(\tilde{e}\rho)\xrightarrow{c?v}_e p$.

• 其余情形类似. □

3　符号互模拟

考虑下面两个进程

$$P=c?x(d!|x|.\mathbf{0}+d!-|x|.\mathbf{0})$$

$$Q=c?x(d!|x|.\mathbf{0}+d!-|x|.\mathbf{0}+d!x.\mathbf{0})$$

它们的符号迁移图见图 2. 按传统的迁移语义,对 P 的每个形为 $c?n$ 的动作 Q 都有相应的动作与之匹配,且它们在此动作后所达到的状态也具有同样的性质;反之亦然. 所以 $P\sim_e Q$. 按符号迁移语义,$Q\xrightarrow{c?x}_E Q_1$ 可由 $P\xrightarrow{c?x}P_1$ 匹配. 但是对 $Q_1\xrightarrow{d!x}_E Q_{23}$,$P_1$ 却缺乏相应的动作. 不过当 x 取定为任一整数值时,这个迁移都能被 P_1 的某个迁移所匹配. 具体地说,当 $x\geqslant 0$ 时,可用 $P_1\xrightarrow{d!|x|}_E P_{21}$ 与之匹配;当 $x<0$ 时,可用 $P_1\xrightarrow{d!-|x|}_E P_{22}$ 与之匹配.

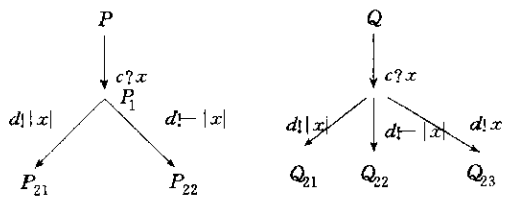

图2

一般地，符号互模拟将以布尔表达式为参数. 对上面这个例子，我们有 $P_{11}\sim_E^{x\geqslant 0}Q_{13}$，$P_{12}\sim_E^{x<0}Q_{13}$. 而对于 P_1 和 Q_1，我们可断言 $P_1\sim_E^{true}Q_1$，因为 *true* 所代表的值空间可以被分割为 $x\geqslant 0$ 与 $x<0$ 两个子空间，在每个子空间上 P_1 都与 Q_1 等价.

在给出符号互模拟的定义之前，我们还需要两个技术性的概念.

设 b 是布尔表达式，B 是布尔表达式的有穷集. 如果 $\vee B=b$，就说 B 是个 b—分割.

设 α,α' 是两个符号动作，b 是布尔表达式. α 与 α' 在 b 上相等，记作 $\alpha=^b\alpha'$，表示(1)如果 α 形如 $c!e$ 则 α' 形如 $c!e'$ 且 $b\models e=e'$，(2)否则 $\alpha\equiv\alpha'$.

定义 3.1. 设 $S=\{S^b\mid b\in BExp\}$ 是由布尔表达式加标的项上对称关系族. 称 S 是一符号互模拟，如果下面条件成立：对 $(t,u)\in S^b$，都有 $fv(b)\subseteq fv(t,u)$，并且只要 $t\xrightarrow{b_1,\alpha}_E t'$，其中 $bv(\alpha)\cap fv(t,u)=\varnothing$，就存在 $b\wedge b_1$—分割 B，满足 $fv(B)\subseteq bv(\alpha)\cup fv(t,u)$，对任一 $b'\in B$，存在 $u\xrightarrow{b_2,\alpha'}_E u'$，$b'\models b_2$，$\alpha=^{b'}\alpha'$，且 $(t',u')\in S^{b'}$.

记 $\sim_E=\{\sim_E^b\}$ 为最大的符号互模拟.

现在我们来考察符号互模拟与传统互模拟之间的关系.

命题 3.1. 设 $S=\{S^b\}$ 是符号互模拟. 令

$$R_S=\{(t\rho,u\rho)\mid\exists\ b,\rho\models b\text{ 且 }(t,u)\in S^b\}$$

则 R_S 是传统互模拟.

证明：设 $(t\rho,u\rho)\in R_S$，即存在 $b,\rho\models b$ 且 $(t,u)\in S^b$.

考虑三种情形：

· $t\rho\xrightarrow{\tau}_c p$. 由预理 2.3(1)，存在 b_1 与 t'，满足 $\rho\models b_1$，$p\equiv_a t'\rho$，$t\xrightarrow{b_1,\tau}_E t'$. 于是有 $b\wedge b_1$—分割 B，对任一 $b'\in B$，都存在 $u\xrightarrow{b_2,\tau}_E u'$，$b'\models b_2$ 且 $(t',u')\in S^{b'}$. 由于 $\rho\models b\wedge b_1$，$b\wedge b_1=\vee B$，存在 $b'\in B$，$\rho\models b'$. 设 $u\xrightarrow{b_2,\tau}_E u'$ 是与该 b' 相联系的符号迁移，则 $\rho\models b_2$. 由预理 2.3(2)，有 $u\rho\xrightarrow{\tau}_c q\equiv_a u'\rho$. 由于 $\rho\models b'$，$(t',u')\in S^{b'}$，于是 $(t'\rho,u'\rho)\in R_S$. 再由预理 1.1，$(p,q)\in R_S$.

· $t\rho\xrightarrow{c?v}_c p$. 由预理 2.5(1)，存在 b_1,x 与 t'，$x\notin fv(t)$，满足 $\rho\models b_1$，$p\equiv_a t'\rho\{v/x\}$，且 $t\xrightarrow{b_1,c?v}_E t'$. 由预理 2.2 可假定 $x\notin fv(u)$. 于是存在 $b\wedge b_1$—分割 B，具有符号互模拟定义中所述的性质. 由于 $\rho\models b\wedge b_1$，$x\notin fv(b_1,b)$，$\rho\{v/x\}\models b\wedge b_1$，从而 $\rho\{v/x\}\models\vee B$. 故必有 $b'\in B$，$\rho\{v/x\}\models b'$，对此 b'，存在 $u\xrightarrow{b_2,c?x}_E u'$，$b'\models b_2$ 且 $(t',u')\in S^{b'}$. 由于 $\rho\{v/x\}\models b_2$，由预理 2.5(2)，有 $q\equiv_a u'\rho\{v/x\}$，$u\rho\{v/x\}\xrightarrow{c?v}_c q$. 由于 $x\notin fv(u)$，$u\rho\{v/x\}=u\rho$，即 $u\rho\xrightarrow{c?v}_c q\equiv_a u'\rho\{v/x\}$. 由 $(t',u')\in S^{b'}$ 及 $\rho\{v/x\}\models b'$，有 $(t'\rho\{v/x\},u'\rho\{v/x\})\in R_S$. 再由预理 2.1，$(p,q)\in R_S$.

· $t\rho\xrightarrow{c!v}_c p$. 类似可证存在 $u\rho\xrightarrow{c!v}_c q$ 且 $(p,q)\in R_S$.

对称地可证，对任一 $u\rho\xrightarrow{a}_c q$ 存在 $t\rho\xrightarrow{a}_c p$ 且 $(p,q)\in R_S$. □

命题 3.2. 设 R 是互模拟. 定义

$$S_R^b=\{(t,u)\mid\rho\models b\Rightarrow(t\rho,u\rho)\in R\}$$

则 $S=\{S_R^b\}$ 是符号互模拟.

证明:设$(t,u)\in S^b_R$,考虑三种类型的符号迁移:

• $t\xrightarrow{b_1,\tau}_E t'$. 我们要构造$b\wedge b_1$－分割$B$,使其具有所要求的性质. 为此将从$u$出发的所有$\tau$－符号迁移编号,记为$u\xrightarrow{b'_i,\tau}_E u^i$,$0<i\leqslant k$. 对每一$i$,令$b''_i$是满足如下条件的布尔表达式.

$$fv(b''_i)\subseteq fv(t,u),\ b''_i\vDash b\wedge b_1$$

$$\rho\vDash b''_i \text{ 当且仅当}(t'\rho,u^i\rho)\in R.$$

令$b'_i=b'_i\wedge b''_i$,$B=\{b'_i\mid 0<i\leqslant k\}$. 我们首先证明$B$是个$b\wedge b_1$－分割,即$\vee B=b\wedge b_1$. 由$B$的定义知$\vee B\vDash b\wedge b_1$. 下面证$b\wedge b_1\vDash\vee B$.

设$\rho\vDash b\wedge b_1$,则$(t\rho,u\rho)\in R$. 由预理 2.3(2),$t\rho\xrightarrow{\tau}_e p\equiv_a t'\rho$. 于是存在$u\rho\xrightarrow{\tau}_e q$,$(p,q)\in R$. 由预理 2.3(1),存在$b'_2$,$u'$,满足$\rho\vDash b'_2$,$q\equiv_a u'\rho$,且$u\xrightarrow{b'_2,\tau}_E u^i$. 由预理 1.1,$(t'\rho,u^i\rho)\in R$. 由$b''_i$的定义,$\rho\vDash b''_i$. 从而$\rho\vDash b'_i$,$\rho\vDash\vee B$.

由B的定义易知它具有符号互模拟所要求的性质:对任一$b'_i\in B$,存在$u\xrightarrow{b'_2,\tau}_E u^i$,由定义$b'_i\vDash b'_2$,由$b''_i$和$b'_i$的定义,$(t',u')\in S^{b'_i}_{R'}$.

• $t\xrightarrow{b_1,c?x}_E t'$. 不妨设$x\notin fv(u)$. 同样我们将从$u$出发的所有$c?x$迁移编号,记为$u\xrightarrow{b'_2,c?x}_E u^i$,$0<i\leqslant k$. 对每个$i$,令$b''_i$是满足下列条件的布尔表达式:

$$fv(b''_i)\subseteq fv(t,u)\cup\{x\},\ b''_i\vDash b\wedge b_1,$$

$$\text{对任一 } v,\rho\{v/x\}\vDash b''_i \text{ 当且仅当}(t'\rho\{v/x\},u^i\rho\{v/x\})\in R.$$

令$b'_i=b'_2\wedge b''_i$,$B=\{b'_i\mid 0<i\leqslant k\}$. 同样我们先来证明$B$是个$b\wedge b_1$－分割. 由$B$的定义知$\vee B\vDash b\wedge b_1$. 为证$b\wedge b_1\vDash\vee B$,设$\rho\vDash b\wedge b_1$,则$(t\rho,u\rho)\in R$. 由预理 2.5(2)对任意$v\in val$,$t\rho\xrightarrow{c?v}_e P\equiv_a t'\rho\{v/x\}$. 于是有$u\rho\xrightarrow{c?v}_e q$,$(p,q)\in R$. 再由预理 2.5(1),存在$i$,$\rho\vDash b'_2$,$u\xrightarrow{b'_2,c?x}_E u^i$,满足$q\equiv_a u^i\rho\{v/x\}$. 由预理 1.1,$(t'\rho\{v/x\},u^i\rho\{v/x\})\in R$. 所以$\rho\{v/x\}\vDash b''_i$,由此$\rho\{v/x\}\vDash b'_i$,从而$\rho\{v/x\}\vDash\vee B$. 由于$v$是任意的,$\rho\vDash\vee B$.

由B的构造易见它具有所要求的性质:对任一$b'_i\in B$,有$u\xrightarrow{b'_2,c?x}_E u^i$,$b'_i\vDash b'_2$. 设$\rho\vDash b'_i$,则$\rho\vDash b''_i$. 令$v=\rho(x)$,则$\rho\{v/x\}=\rho$,于是$(t'\rho,u^i\rho)\in R$. 由$S^b_R$的定义,$(t',u')\in S^{b'_i}_{R'}$. □

• $t\xrightarrow{b_1,c!e}_E t'$. 类似.

综合上面两个定理,我们得到本节的主要结果:

定理 3.3. $t\sim^b_E u$ 当且仅当对任意$\rho\vDash b$,$t\rho\sim_e u\rho$.

特别地对闭项p,q,$p\sim_e q$ 当且仅当 $p\sim^{true}_E q$. 这表明符号互模拟确实刻划了传统互模拟.

4　弱互模拟

在CCS中τ代表内部通讯,是不可见的动作. 考虑到τ的这种特殊性,就导致弱互模拟的概念.

我们首先定义传统的双箭头迁移$\overset{a}{\Rightarrow}_e, a\in\{\varepsilon,\tau,c?v,c!v\}$，它是由下列规则生成的最小关系：

- $p\overset{\varepsilon}{\Rightarrow}_e p$
- 若 $p\overset{a}{\rightarrow}_e q$ 则 $p\overset{a}{\Rightarrow}_e q$
- 若 $p\overset{\tau}{\rightarrow}_e\overset{a}{\Rightarrow}_e q$ 则 $p\overset{a}{\Rightarrow}_e q$
- 若 $p\overset{a}{\Rightarrow}_e\overset{\tau}{\rightarrow}_e q$ 则 p 若 $p\overset{a}{\Rightarrow}_e q$

我们还要用到记号 $\hat{a}=\begin{cases}\varepsilon & \text{若 } a=\tau\\ a & \text{否则}\end{cases}$

定义 4.1. 称闭项上的对称关系 R 为弱互模拟，若对任意$(p,q)\in R$，只要 $p\overset{a}{\rightarrow}_e p'$，就有 $q\overset{\hat{a}}{\Rightarrow}_e q'$ 且$(p',q')\in R$.

用$\approx_e$表示最大的弱互模拟关系. □

由于$\approx_e$关于＋不同余，需进一步定义观察等价：

定义 4.2. 称闭项 p,q 观察等价，记为 $p\simeq_e q$，若对任意 $a\in\{\tau,c!v,c?v\}$都有

- 若 $p\overset{a}{\rightarrow}_e p'$，则 $q\overset{a}{\Rightarrow}_e q'$ 且 $p'\approx_e q'$.
- 若 $q\overset{a}{\rightarrow}_e q'$，则 $p\overset{a}{\Rightarrow}_e p'$ 且 $p'\approx_e q'$.

观察等价是同余关系[2].

类似地，我们可定义符号双箭头迁移和符号观察等价.

符号双箭头迁移$\overset{b,a}{\Rightarrow}_E, a\in\{\varepsilon,\tau,c?x,c!e\}$，由下列规则定义：

- $t\overset{true,\varepsilon}{\Rightarrow}_E t$
- 若 $t\overset{b,a}{\rightarrow}_E u$，则 $t\overset{b,a}{\Rightarrow}_E u$
- 若 $t\overset{b,\tau}{\rightarrow}_E\overset{b',a}{\Rightarrow}_E u$ 则 $t\overset{b\wedge b',a}{\Rightarrow}_E u$
- 若 $t\overset{b,a}{\Rightarrow}_E\overset{b',\tau}{\rightarrow}_E u$ 则 $t\overset{b\wedge b',a}{\Rightarrow}_E u$

定义 4.3. 称以布尔表达式加标的项上关系族 $S=\{S^b\mid b\in BExp\}$为符号弱互模拟，如果对任意$(t,u)\in S^b$，只要 $t\overset{b_1,a}{\rightarrow}_E t'$，$bv(a)\cap fv(b,t,u)=\varnothing$，就存在 $b\wedge b_1$－分割 B，对任一 $b'\in B$，有 $u\overset{b_2,\hat{a}}{\Rightarrow}_E u'$，$b'\vdash b_2$，$a=^{b'}a'$ 且$(t',u')\in S^{b'}$.

记$\approx_E=\{\approx_E^b\}$为最大的符号弱互模拟.

定义 4.4. 称项 t,u 符号观察等价，记作 $t\simeq_E u$，如果只要 $t\overset{b_1,a}{\rightarrow}_E t'$，$bv(a)\cap fv(b,t,u)=\varnothing$，就存在$b\wedge b_1$－分割 B，对任一 $b'\in B$，有 $u\overset{b_2,a'}{\Rightarrow}u'$，$b'\vdash b_2$，$a=^{b'}a'$ 且 $t'\approx_E^{b'}u'$.

关于 u 成立对称的条件.

下面的定理说明符号弱互模拟和符号观察等价分别刻划了弱互模拟和观察等价. 它们的证明与定理 3.3 的证明类似，限于篇幅略去.

定理 4.1. $t\approx_E^b u$，当且仅当对任意 $\rho\vdash b$，$t\rho\approx_e u\rho$.

定理 4.2. $t \simeq_E^b u$,当且仅当对任意 $\rho \models b$, $t\rho \approx_e u\rho$.

参考文献

1 Hoare C A R. Communicating sequential processes. Prentice—Hall, 1985.

2 Milner R. Communication and concurrecy. Prentice—Hall, 1989.

3 Cleaveland R, Parrow J, Steffen B. A semantics based verification tool for finite state systems. Proc. 9th IFIP Symposium on Protocol Specification, Testing and Verification, North—Holland, 1989.

4 Denicola R, Inverardi P, Nesi M. Using the axiomatic presentation of behavioral equivalences for manipulating CCS specifications. Proc. Workshop on Automatic Verification for Finite State Systems, LNCS 407, 1989.

5 Lin H. PAM: a process algebra manipulator. Proc. International Workshop on Computer Aided Verification, LNCS 575, Spinger—Verlag, 1991.

6 Simone R De, Verganimi D. Aboard auto. Report RT111, INRIA 1989.

7 Dijkstra E W. A discipline of programming. Prentice—Hall, 1976.

8 Milner R, Parrow J, Walker D. A calculus of mobile processes. Information and Computation, 1992, **100**(1): 1—40.

9 Plotkin G. A structural approach to operational semantics. Technical Report DAIMI FN—19, Dept. of Computer Science, Aarhus University, 1981.

SYMBOLIC BISIMULATION FOR VALUE—PASSING PROCESSES

Lin Huimin

(*Institute of Software, The Chinese Academy of Sciences, Beijing* 100080)

Abstract　A symbolic transitional semantics for value—passing process algebras is proposed and the notion of symbolic bisimulation is introduced. It is proved that two processes are bisimilar in the traditional sense if and only if they are symbolicaly bisimilar. Since the transition graphs of value—passing processes over infinite data domains are infinite, while the symbolic transition graphs of many such processes are finite, the article's result makes it possible to decide bisimulation—based equivalences for such these processes in finite amount of time and space.

Key words　Communicating processes, process algebra, bisimulation.