

嵌套谓词等式系与弱互模拟

林惠民

(中国科学院软件研究所计算机科学开放研究实验室 北京 100080)

摘要 带赋值符号迁移图是一般传值进程的语义模型,其强互模拟等价可以归结为谓词等式系的最大解.该文将这一结果推广到弱互模拟等价,为此,引入嵌套谓词等式系的概念,并提出算法,将带赋值符号迁移图的弱互模拟等价归结为形如 $E_2 \mu E_1$ 的嵌套谓词等式系的最大解.

关键词 传值进程,互模拟,谓词等式系.

中图法分类号 TP301

文献[1,2]中引入了带赋值的符号迁移图(symbolic transition graphs with assignment,简称 STGA)作为一般传值进程的计算模型.STGA 在符号迁移图^[3]的基础上扩充了赋值运算,可以表示进程内部状态的改变,因而很大一类传值进程都可以表示为有穷状态 STGA.以 CCS 为例,任一正则(即递归定义体中不出现并行复合)CCS 传值进程都对应于一有穷状态 STGA.有穷状态 STGA 的另一个优点是,在并行复合下封闭,即两个有穷状态 STGA 并行复合的结果仍然是有穷状态 STGA^[2],因此,STGA 足以表示并发进程网络(networks of parallel processes).两个不带赋值有穷符号迁移图的强互模拟等价可以用一阶公式刻画,即两个图强互模拟当且仅当相应的公式为真^[3].对带赋值的符号迁移图,这一结论一般不再成立,因此,文献[3]中引入谓词等式系的概念,在一阶谓词演算的正子集中引入不动点,并设计了算法,将有穷 STGA 的强互模拟归结为谓词等式系的最大解.

强互模拟等价主要具有理论上的意义,在实际上使用的等价关系是将表示内部通信的不可见动作 τ 抽象后得到的弱互模拟等价^[4].本文的目的是将文献[1]的结果推广到弱互模拟等价.由于简单的谓词等式系不足以刻画弱互模拟,为此,首先引入嵌套谓词等式系的概念,证明其极大、极小解的存在性,然后讨论如何将将有穷 STGA 的弱互模拟等价归结为交错深度为 2 的嵌套谓词等式系的最大解.

为节省篇幅,对文献[1]第 2 和第 3 节中的基本记号及定义,本文不再重复.

1 嵌套谓词等式系

假定数据变量集 $DV = \{x, y, z, \dots\}$,数据变量集上的数据表达式集 $DExp$ 和布尔表达式集 $BExp$,谓词变量集 $PV = \{X, Y, Z, \dots\}$,可如文献[1]第 3 节定义合式命题 Φ 和谓词 Λ .注意在命题和谓词的构造中没有使用否定词,并且谓词变量不在蕴涵式的左部出现.给定数值集 Val ,并令 $T = \{true, false\}$.对数据变量的赋值 ρ 将数据变量映射为 Val 中的元素. ρ 可延伸到 $DExp$ 和 $BExp$ 上;对任一 $e \in DExp, \rho(e) \in Val$;对任一 $b \in BExp, \rho(b) \in T$.对谓词变量的赋值 \mathcal{V} 将谓词变量映射为函数空间 $Val^n \rightarrow T$ 中的元素(n 为谓词变量的型).给定 ρ 和 \mathcal{V} ,可定义公式 Φ 和谓词 Λ 的语义,详见文献[1]中的第 3 节.令 $false < true$,序 $<$ 可逐点扩充到函数空间 $Val \rightarrow T$ 上,并进一步扩充到谓词变量的赋值,详见文献[1]中的第 3 节.容易验证,全体谓词变元赋值在序 $<$ 下构成完备格.设 $\{X_i | i \in I\}$ 是谓词变量的有限集,称 $E; \{X_i = \Lambda_i | i \in I\}$ 为一谓词等式系,若 Λ_i 与 X_i 有相同的型,且对 $i \neq j$ 有 $X_i \neq X_j$.用向量形式 $\{X_i = \Lambda_i | i \in I\}$ 可简写为 $\bar{X} = \bar{\Lambda}$.对 $k \in \{1, \dots, n\}$,设 $\sigma_k \in \{\mu, \mathcal{V}\}, \sigma_k \neq \sigma_{k-1} (k > 1), E_k:$

• 本文研究得到国家自然科学基金和中国科学院“九五”基础研究重点项目基金资助.作者林惠民,1947年生,博士,研究员,博士生导师,主要研究领域为形式语义学,通信并发系统的语义模型与验证工具,模态逻辑与时序逻辑.

本文通讯联系人:林惠民,北京 100080,中国科学院软件研究所计算机科学开放研究实验室

本文 1998-08-20 收到原稿,1998-12-25 收到修改稿

$\bar{X}_k = \bar{X}_k$ 是谓词等式系, 且对 $k \neq j, \{\bar{X}_k\} \cap \{\bar{X}_j\} = \emptyset$, 则称

$$\mathcal{E}: E_n \sigma_{n-1} E_{n-1} \dots \sigma_1 E_1$$

是交错深度为 n 的嵌套谓词等式系. 为方便书写, 我们用 \mathcal{E}_k 表示 $E_k \sigma_{k-1} E_{k-1} \dots \sigma_1 E_1$. 给定 ρ 和 \mathcal{V} , \mathcal{E}_n 的解 ζ 归纳定义如下:

$$\zeta(\bar{X}_1) = \|\bar{A}_1\|_{\rho, \mathcal{V}(\zeta)},$$

$$\zeta(X_n) = \|\Lambda_n\|_{\rho, \mathcal{V}(\eta_\zeta)},$$

$$\eta_\zeta = \|\sigma_{n-1} \mathcal{E}_{n-1}\|_{\rho, \mathcal{V}(\zeta)}.$$

这里, $\|\sigma \mathcal{E}\|_{\rho, \mathcal{V}}$ 表示 \mathcal{E} 相对于 ρ 和 \mathcal{V} 的最大解(若 $\sigma \equiv \mathcal{V}$)或最小解(若 $\sigma \equiv \mathcal{V}$), \mathcal{E}_n 的解也就是泛函 $\lambda \zeta \|\bar{A}_n\|_{\rho, \mathcal{V}(\eta_\zeta)}$ 的不动点. 这个定义的合理性由下述命题保证.

命题 1.1. 给定 ρ 和 \mathcal{V} , 任意嵌套谓词等式系存在最大解和最小解.

证明: 由于全体对谓词变量的赋值在下 $<$ 构成完备格, 完备格上的单调函数有最大和最小不动点^[5], 所以只需证明泛函 $\lambda \zeta \|\bar{A}_n\|_{\rho, \mathcal{V}(\eta_\zeta)}$ 关于序 $<$ 单调, 其中 $\eta_n = \|\sigma_{n-1} \mathcal{E}_{n-1}\|_{\rho, \mathcal{V}(\zeta)}$. 我们假定 $\zeta' < \zeta''$, 往证 $\|\bar{A}_n\|_{\rho, \mathcal{V}(\eta_{\zeta'})} < \|\bar{A}_n\|_{\rho, \mathcal{V}(\eta_{\zeta''})}$, 对 n 施归纳.

(基始步) $n=1$. 这时等式系非嵌套, η_ζ 和 $\eta_{\zeta'}$ 都是空解, 所以, $\mathcal{V}(\eta_\zeta)\{\zeta'\} = \mathcal{V}\{\zeta'\}, \mathcal{V}(\eta_{\zeta'})\{\zeta''\} = \mathcal{V}\{\zeta''\}$. 由 $\zeta' < \zeta''$ 知, $\mathcal{V}\{\zeta'\} < \mathcal{V}\{\zeta''\}$. 由于 $\|\bar{A}_1\|$ 中谓词变量不出现于蕴涵式左部, 所以, $\|\bar{A}_1\|_{\rho, \mathcal{V}(\zeta')} < \|\bar{A}_1\|_{\rho, \mathcal{V}(\zeta'')}$.

(归纳步) 设结论对嵌套深度为 $n-1$ 的等式系成立, 考虑 $\mathcal{E}_n = E_n \sigma_{n-1} \mathcal{E}_{n-1}$, 不妨设 $\sigma_{n-1} \equiv \mu$. 由归纳假设 $\lambda \zeta \|\bar{A}_{n-1}\|_{\rho, \mathcal{V}(\eta_\zeta)}$ 关于 $<$ 单调, 因此, \mathcal{E}_{n-1} 有关于 $\rho, \mathcal{V}\{\zeta'\}$ 的最小不动点 $\eta_{\zeta'} = \|\mu \mathcal{E}_{n-1}\|_{\rho, \mathcal{V}(\zeta')}$ 和关于 $\rho, \mathcal{V}\{\zeta''\}$ 的最小不动点 $\eta_{\zeta''} = \|\mu \mathcal{E}_{n-1}\|_{\rho, \mathcal{V}(\zeta'')}$, 从 $\zeta' < \zeta''$ 知, $\mathcal{V}\{\zeta'\} < \mathcal{V}\{\zeta''\}, \eta_{\zeta'} < \eta_{\zeta''}$, 故有 $\mathcal{V}(\eta_{\zeta'})\{\zeta'\} < \mathcal{V}(\eta_{\zeta''})\{\zeta''\}$. 由于 $\|\bar{A}_n\|$ 中谓词变量不在蕴涵式左部出现, 得 $\|\bar{A}_n\|_{\rho, \mathcal{V}(\eta_{\zeta'})} < \|\bar{A}_n\|_{\rho, \mathcal{V}(\eta_{\zeta''})}$. □

预备定理 1.1. 设有谓词等式系 $E(Y_i = (X_i) (\Phi_i \vee \bigvee_{j \in J_i} (b_j \wedge Y_j(\bar{e}_j)))) \mid i \in I$, Φ_i 不含 Y 中的谓词变元, η 是 E 相对于 ρ 和 \mathcal{V} 的最小解. 则 $\eta(Y_{i_0})(\bar{u}_{i_0}) = true, i_0 \in I$, 当且仅当存在 $i_1, \dots, i_k, k \geq 0 (i_1, \dots, i_k$ 不必互不相同), 满足 $i_l \in J_{i_{l-1}}$,

$$\rho_l(b_{i_l}) \wedge \eta(Y_{i_l})(u_{i_l}) = true, 1 \leq l \leq k,$$

$$\|\Phi_{i_k}\|_{\rho_k, \mathcal{V}} = true,$$

其中 $\rho_0 = \rho, \rho_{l+1} = \rho_l(\bar{u}_{i_l} \vdash \bar{x}_{i_l}), \bar{u}_{i_l} = \rho_l(\bar{e}_{i_l})$.

证明: 由 $\eta(Y_{i_0})(\bar{u}_{i_0}) = true$ 知,

$$\Phi_{i_0} \vee \bigvee_{j \in J_{i_0}} (b_j \wedge Y_j(\bar{e}_j)) \|\rho_1, \mathcal{V}(\eta)\| = true.$$

若 $\|\Phi_{i_0}\|_{\rho_1, \mathcal{V}(\eta)} = true$, 则预备定理已得证(由于 Φ_i 不含 \bar{Y} 中的谓词变元, $\|\Phi_{i_0}\|_{\rho_1, \mathcal{V}(\eta)} = \|\Phi_{i_0}\|_{\rho_1, \mathcal{V}}$). 否则, 有 $i_1 \in J_{i_0}$ 使得 $\|b_{i_1} \wedge Y_{i_1}(\bar{e}_{i_1})\|_{\rho_1, \mathcal{V}(\eta)} = true$. 即

$$\rho_1(b_{i_1}) \wedge \eta(Y_{i_1})(\bar{u}_{i_1}) = true.$$

对 $\eta(Y_{i_1})(\bar{u}_{i_1}) = true$ 可继续同样推理. 由最小不动点的性质, 必有某个 k , 使得 $\|\Phi_{i_k}\|_{\rho_k, \mathcal{V}} = true$, 且对所有 $1 \leq l < k$, 都有 $\rho_l(b_{i_l}) \wedge \eta(Y_{i_l})(\bar{u}_{i_l}) = true$. □

2 STGA 的弱互模拟及其逻辑刻画

关于带赋值符号迁移图的详细定义请参看文献[1]第2节.

定义 2.1. 带赋值符号迁移图(简称 STGA)是一个有向图, 其每个结点 n 标有自由变量的有穷集 $fv(n)$, 每条边标有由布尔表达式、赋值和动作组成的三元组, 满足: 如果 $n \xrightarrow{b, \bar{x}_i = \bar{e}, \alpha} m$ 是从 n 到 m 的一条边, 则有 $fv(b, \bar{e}) \subseteq fv(n), fv(\alpha) \subseteq \{\bar{x}\}, fv(m) \subseteq \{\bar{x}\} \cup fv(\alpha)$. □

这里, b 是布尔表达式, \bar{e} 是数据表达式, $\alpha \in \{\tau, c? x, c! e \mid c$ 是通道, $c? x$ 称为输入动作, $c! e$ 称为输出动作, τ 是表示内部通信的不可见动作. 给定一个带赋值的符号迁移图 \mathcal{G}, \mathcal{G} 上的状态空间 $\mathcal{S} = \{n_p \mid n$ 是 \mathcal{G} 的结点,

$\rho \in Eval$). STGA 的迟操作语义是状态上的迁移关系,由下列规则给出.

$$\frac{m \xrightarrow{b, \theta, \tau} n}{m_\rho \xrightarrow{\tau} n_{\theta\rho}} \rho \models b \quad \frac{m \xrightarrow{b, \theta, c!e} n}{m_\rho \xrightarrow{c! \rho(c!e)} n_{\theta\rho}} \rho \models b \quad \frac{m \xrightarrow{b, \theta, c!\gamma} n}{m_\rho \xrightarrow{c!\gamma} n_{\theta\rho}} \rho \models b.$$

为了定义迟弱互模拟,先引入双箭头迁移. 令 $\Rightarrow = \xrightarrow{\tau}^*$; $m_\rho \Rightarrow n_\rho$ 当且仅当 $m_\rho \xrightarrow{c!x} n_\rho$, 对 $a \in \{\tau', c! \nu\}$ $m_\rho \xrightarrow{a} n_\rho$ 当且仅当 $m_\rho \xrightarrow{a} n_\rho$; $\Rightarrow = \xrightarrow{\tau}^*$, 对 $a \neq \tau$, $\xrightarrow{a} = \xrightarrow{a}$.

定义 2.2. 称状态上的对称二元关系 R 是迟弱互模拟, 如果 $\{m_\rho, n_e\} \in R$ 蕴涵,

- 只要 $m_\rho \xrightarrow{c!x} m'_\rho$, 就有 $n_e \xrightarrow{c!\gamma} n'_e$, 并且对任意 $v \in Val$, 存在 $n'_e[v/y] \Rightarrow n'_e$, 满足 $(m_\rho[v/x], n'_e) \in R$.
- 对其他动作 a , 只要 $m_\rho \xrightarrow{a} m'_\rho$, 就有 $n_e \xrightarrow{a} n'_e$, 满足 $(m'_\rho, n'_e) \in R$.

令 $\approx = \cup \{R \mid R \text{ 是一个迟弱互模拟.}\}$

刻画弱互模拟需要交错深度为 2 的嵌套谓词等式系 $E_2 \mu E_1$, 直观地说, 外层等式系 E_2 刻画互模拟, 内层等式系 E_1 则用于吸收 τ 动作.

设 \mathcal{S} 和 \mathcal{X} 是两个变量名字空间不相交的 STGA, \mathcal{S} 的结点用 m, m', m_i, \dots 表示; \mathcal{X} 的结点用 n, n', n_j, \dots 表示; m, m', m_i, \dots 的变量记为 $\bar{x}, \bar{x}', \bar{x}_i, \dots$; n, n', n_j, \dots 的变量记为 $\bar{y}, \bar{y}', \bar{y}_j, \dots$. 下面的算法 1 中的算法生成形如 $E_2 \mu E_1$ 的等式系. 算法中用集合 $Visited, Visited_{\tau, m, n}, Visited_{\theta, c!e, m, n}, Visited_{c!\gamma, m, n}$ 保证对每一相应的环路只访问一次. 这些集合由过程 $init()$ 置为空集. 另外, 在匹配输入动作时使用函数 $newVar()$ 生成一个新的数据变量. 过程 $emit$ 产生谓词等式. id 表示恒等替换.

由上述算法产生的谓词等式有 4 类, 分别如

$$\begin{aligned} X_{m, n}(\bar{x}, \bar{y}) &= \nu \Phi && \text{(由 close 产生)} \\ Y_{m, n}(\bar{x}, \bar{y}) &= \rho \Phi \vee \bigvee_i (b_i \wedge Y_{m, n}(\bar{x}, \bar{f}_i)) && \text{(由 close}_\tau \text{ 产生)} \\ Y_{\theta, c!e, m, n}(\bar{x}, \bar{y}) &= \mu \Phi \vee \bigvee_i (b_i \wedge Y_{\theta, c!e, m, n_i}(\bar{x}, \bar{f}_i)) && \text{(由 match'}_{c!} \text{ 产生)} \\ Y_{c!\gamma, m, n}(\bar{x}, \bar{y}) &= \nu \Phi \vee \bigvee_i (b_i \wedge Y_{c!\gamma, m, n_i}(\bar{x}, \bar{f}_i)) && \text{(由 match'}_{c!\gamma} \text{ 产生)} \end{aligned}$$

令 E_2 为由第 1 类等式组成的等式系, E_1 为由其余 3 类等式组成的等式系. 称 $E_2 \mu E_1$ 为上述算法产生的嵌套谓词等式系. 不难看出, $E_2 \mu E_1$ 是闭的, 并且在 E_1 的各等式中, 右边的第 1 个析取项 Φ 中不含在 E_1 左部出现的谓词变元.

算法 1. 迟弱互模拟算法

```

bisim(m, θ, n, σ) = init()
                    close(m, θ, n, σ)
close(m, θ, n, σ) =
  if (m, n) ∈ Visited then {
    Visited = {⟨m, n⟩} ∪ Visited
    emit(Xm, n =ν match(m, n))
  }
  return Xm, n(θ, σ)
match(m, n) =  $\bigwedge_{r \in \{\tau, c!, c!\gamma\}}$  matchr(m, n) ∧ matchr(n, m)
matchr(m, n) =  $\bigwedge_{\substack{b_i, \theta_i, \tau_i \\ n_i \xrightarrow{b_i, \theta_i, \tau_i} m_i}} b_i \Rightarrow match'_i(\theta_i, m_i, n'_i)$ 
closeτ(m, θ, n, σ) =
  B = close(m, θ, n, σ)
  for each ni |  $\xrightarrow{b_i, \theta_i, \tau_i} n_i$ 
    if (m, ni) ∈ Visitedτ, m, n then {
      Visitedτ, m, n = {⟨m, ni⟩} ∪ Visitedτ, m, n
      emit(Ym, ni =ρ closeτ(m, θ, ni, id))
    }
  return (B ∨  $\bigvee_i b_i \wedge Y_{m, n_i}(\text{id}, \sigma_i)$ )
match'_i(m, n) = closeτ(m, θ, n, id)

```

$$\begin{aligned}
\text{match}_{c_1}(m, n) &= \bigwedge_{\substack{b_i, \theta_i, c_1!e_i \\ m \vdash \rightarrow n_i}} b_i \Rightarrow \text{match}'_{c_1}(\theta_i, m_i, n) \\
\text{match}'_{c_1}(\theta, m, n) &= \\
&\text{for each } n \xrightarrow{b_j, \sigma_j, c_1!e_j} n_j \\
&\quad B_j := \text{close}_r(m, \theta, n_j, \sigma_j) \\
&\quad \text{for each } n \xrightarrow{b'_i, \sigma'_i, \tau} n'_i \\
&\quad \text{if } (m, n'_i) \notin \text{Visited}_{\theta, c_1!e, m, n} \text{ then } \{ \\
&\quad \quad \text{Visited}_{\theta, c_1!e, m, n} = \{ (m, n'_i) \} \cup \text{Visited}_{\theta, c_1!e, m, n} \\
&\quad \quad \text{emit}(Y_{\theta, c_1!e, m, n'_i} = \text{match}'_{c_1}(\theta, c_1!e, m, n'_i)) \\
&\quad \text{return}(\bigvee b_j \wedge e\theta = e'_j \sigma_j \wedge B_j) \vee (\bigvee b'_i \wedge Y_{\theta, c_1!e, m, n'_i}(\text{id}, \sigma'_i)) \\
\text{match}_{c_1}(m, n) &= \bigwedge_{\substack{b_i, \theta_i, c_1!e_i \\ m \vdash \rightarrow n_i}} b_i \Rightarrow \text{match}'_{c_1}(\theta_i, x, m_i, n) \\
\text{match}'_{c_1}(\theta, x, m, n) &= \\
&\text{for each } n \xrightarrow{b_j, \sigma_j, c_1!e_j} n_j \\
&\quad z = \text{new Var}() \\
&\quad B'_j := \text{close}_r(m, \theta[x \mapsto z], n_j, \sigma_j[x \mapsto z]) \\
&\quad B_j := \forall B'_j \\
&\quad \text{for each } n \xrightarrow{b'_i, \sigma'_i, \tau} n'_i \\
&\quad \text{if } (m, n'_i) \notin \text{Visited}_{\theta, c_1!e, m, n} \text{ then } \{ \\
&\quad \quad \text{Visited}_{\theta, c_1!e, m, n} = \{ (m, n'_i) \} \cup \text{Visited}_{\theta, c_1!e, m, n} \\
&\quad \quad \text{emit}(Y_{\theta, c_1!e, m, n'_i} = \text{match}'_{c_1}(\theta, x, m, n'_i)) \\
&\quad \text{return}((\bigvee b_j \wedge B_j) \vee (\bigvee b'_i \wedge Y_{\theta, c_1!e, m, n'_i}(\text{id}, \sigma'_i)))
\end{aligned}$$

预备定理 2.1. 设 η 是 E_1 相对于 ζ 的最小解, 若 $\| Y_{M, n}(\bar{x}, \bar{f}) \|_{[\bar{x}/\bar{v}, \bar{v}/\bar{y}], \zeta(\eta)} = \text{true}$, M 形如 m 或 $\theta.c!e, m$ 或 $c?$ $x, m, \bar{v}_0 = \bar{f}[\bar{v}/\bar{y}]$, 则存在 n', \bar{v}', \bar{y}' 和 E_1 中等式

$$Y_{M, n'}(\bar{x}, \bar{y}') = \Phi' \vee \bigvee (b_l \wedge Y_{M, n_l}(\bar{x}, \bar{f}_l))$$

使得 $n_{[\bar{x}_0/\bar{y}_1]} \Rightarrow n'_{[\bar{v}'/\bar{y}]}$, 且 $\| \Phi \|_{[\bar{v}/\bar{x}, \bar{v}/\bar{y}], \zeta(\eta)} = \text{true}$.

证明: 以 $M \equiv m$ 为例, 其余情形类似. 由题设条件和预备定理 1.1, 有 $l_j, 0 \leq j < k, k \geq 0, n_0 = n$ 和 E_1 中等式

$$Y_{M, n_0}(\bar{x}, \bar{y}_0) = \Phi_0 \vee \bigvee_{l \in J_0} (b_l \wedge Y_{M, n_l}(\bar{x}, \bar{f}_l))$$

满足 $l_j \in j_{j-1}, j \geq 1$,

$$\begin{aligned}
b_{l_j}[\bar{v}_j/\bar{y}_{l_j}] &= \text{true}, \\
\eta(Y_{M, n_{l_j}})(\bar{u}, \bar{v}_{l_j}) &= \text{true}, \\
\| \Phi_{l_j} \|_{[\bar{u}/\bar{x}, \bar{v}_k/\bar{y}_k], \zeta(\eta)} &= \text{true},
\end{aligned}$$

其中 $\bar{v}_{l_j} = \bar{v}, \bar{v}_{l_j} = \bar{f}_{l_j}[\bar{v}_{l_j-1}/\bar{y}_{l_j-1}]$. 又由函数 close_r 知,

$$\begin{array}{ccc}
b_{l_1, \sigma_{l_1}, \tau} & & b_{l_k, \sigma_{l_k}, \tau} \\
n_0 \xrightarrow{\quad} & n_1 \dots & \xrightarrow{\quad} n_k
\end{array}$$

所以 $n_{i_0[\bar{u}/\bar{x}, \bar{v}/\bar{y}]} \xrightarrow{c} n_{i_1[\bar{u}/\bar{x}, \bar{v}_1/\bar{y}_1]} \dots \xrightarrow{c} n_{i_k[\bar{u}/\bar{x}, \bar{v}_k/\bar{y}_k]}$. 令 $n' = n_k, \bar{v}' = \bar{v}_k, \bar{y}' = \bar{y}_k, \Phi' = \Phi_k$ 即得所欲证. □

定理 2.1. 设 $E_2 \mu E_1$ 是由算法 1 产生的嵌套谓词等式系, ζ 是 $E_2 \mu E_1$ 的解. $\zeta(X_{m, n})(\bar{u}, \bar{v}) = \text{true}$ 当且仅当 $m_{[\bar{u}/\bar{x}]} \sim n_{[\bar{v}/\bar{y}]}$, 其中 \bar{x}, \bar{y} 分别是 m 和 n 的自由变量.

证明: (\Rightarrow) 令 $S = \{ (m_{[\bar{u}/\bar{x}]}, n_{[\bar{v}/\bar{y}]}) \mid \zeta(X_{m, n})(\bar{u}, \bar{v}) = \text{true} \}$, 往证 S 是弱互模拟. 设 $(m_{[\bar{u}/\bar{x}]}, n_{[\bar{v}/\bar{y}]}) \in S$, 则 $\zeta(X_{m, n})(\bar{u}, \bar{v}) = \| \Phi_{m, n} \|_{[\bar{u}/\bar{x}, \bar{v}/\bar{y}], \eta(\zeta)} = \text{true}$, 这里, η 是 E_1 相对于 $[\bar{u}/\bar{x}, \bar{v}/\bar{y}]$ 和 ζ 的最小解. 分别考虑从 $m_{[\bar{u}/\bar{x}]}$ 出发的 3 种迁移.

(1) $m_{[\bar{u}/\bar{x}]} \xrightarrow{c!m} m'$, 则有边 $m \xrightarrow{b_i, \theta_i, c!e_i} m$, 满足 $b_i[\bar{u}/\bar{x}] = \text{true}, (e_i, \theta_i)[\bar{u}/\bar{x}] = \bar{v}, m_i = m, \Phi_{m, n}$ 含一合取项 $b_i \Rightarrow \Phi$. 由

$b_i[\bar{u}/\bar{x}] = true$ 得 $\| \Phi_i \|_{[\bar{u}/\bar{x}, \bar{v}/\bar{y}], \eta(\zeta)} = true$. Φ_i 形如 $\bigvee_j (b'_j \wedge e_i \theta_j = e'_j \sigma_j \wedge B_j) \vee \bigvee_j (b''_j \wedge Y_{\theta_j, c1e_j, m_j, n_j}(\bar{x}, \bar{f}_j))$.

(1.1) 若有 j , $\| b'_j \wedge e_i \theta_j = e'_j \sigma_j \wedge B_j \|_{[\bar{u}/\bar{x}, \bar{v}/\bar{y}], \eta(\zeta)} = true$, 则有边 $n \xrightarrow{b'_j, \sigma_j, c1e'_j} n_j, \sigma_j = [\bar{y}_j; = \bar{f}_j]$, 且 $b'_j[\bar{v}/\bar{y}] = true$, $(e'_j \sigma_j)[\bar{v}/\bar{y}] = (e_i \theta_i)[\bar{u}/\bar{x}] = v$. 从而 $n_{[\bar{v}/\bar{y}]} \xrightarrow{c1v} n_j[\bar{v}_j/\bar{y}_j], \bar{v}_j = \bar{f}_j[\bar{v}/\bar{y}]$, 同时, $\| B_j \|_{[\bar{u}/\bar{x}, \bar{v}/\bar{y}], \eta(\zeta)} = true$. B_j 形如 $X_{m_j, n_j}(\bar{e}_j, \bar{f}_j) \vee \bigvee_l (b_l \wedge Y_{m_l, n_l}(\bar{x}, \bar{f}_l))$. 记 $\theta_i = [\bar{x}_i; = \bar{e}_i], \bar{u}_i = \bar{e}[\bar{u}/\bar{x}]$. 若 $\zeta(X_{m_j, n_j})(\bar{u}_i, \bar{v}_j) = true$, 则 $(m_{i[\bar{v}_j/\bar{y}_j]}, n_{j[\bar{v}_j/\bar{y}_j]}) \in S$. 否则存在 l , $\| b_l \wedge Y_{m_l, n_l}(\bar{x}, \bar{f}_l) \|_{[\bar{u}/\bar{x}, \bar{v}/\bar{y}], \eta(\zeta)} = true$, 从而 $n_{j[\bar{v}_j/\bar{y}_j]} \xrightarrow{\tau} n_{[\bar{v}_l/\bar{y}_l]}, v_l = \bar{f}_l[\bar{v}_j/\bar{y}_j]$. 因为 η 是 E_2 相对于 ζ 的最小解, 由预备定理 2.1, 存在 n', \bar{v}', \bar{y}' 和 E_1 中等式

$$Y_{m_j, n'}(\bar{x}, \bar{y}') = X_{m_j, n'}(\bar{x}, \bar{f}') \vee \dots$$

使得 $n_{i[\bar{v}_j/\bar{y}_j]} \Rightarrow n'[\bar{v}'/\bar{y}']$, $\| X_{m_j, n'}(\bar{x}, \bar{f}') \|_{[\bar{u}/\bar{x}, \bar{v}'/\bar{y}'], \eta(\zeta)} = true$. 因此有 $n_{\bar{v}/\bar{y}} \xrightarrow{c1v} n_{j[\bar{v}_j/\bar{y}_j]} \xrightarrow{\tau} n_{[\bar{v}'/\bar{y}']},$ 且 $(m_{i[\bar{u}/\bar{x}]}, n_{\bar{v}'/\bar{y}'}) \in S$.

(1.2) 若不存在(1.1)中的 j , 则有 l ,

$$\| b''_l \wedge Y_{\theta_l, c1e_l, m_l, n_l}(\bar{x}_l, \bar{f}_l) \|_{[\bar{u}/\bar{x}, \bar{v}/\bar{y}], \eta(\zeta)} = true,$$

从而 $n_{[\bar{v}/\bar{y}]} \xrightarrow{\tau} n_{[\bar{v}_l/\bar{y}_l]}, \bar{v}_l = \bar{f}_l[\bar{v}/\bar{y}]$. 又由预备定理 2.1, 存在 $n'', \bar{v}'', \bar{y}''$ 和 E_1 中等式

$$Y_{\theta_l, c1e_l, m_l, n_l}(\bar{x}_l, \bar{y}'') = \bigvee_j (b'_j \wedge e \setminus \theta_l = e'_j \sigma_j \wedge B_j) \vee \bigvee_{j'} (b''_{j'} \wedge Y_{\theta_{j'}, c1e_{j'}, m_{j'}, n_{j'}}(\bar{x}_l, \bar{f}_{j'}))$$

满足

$$n_{[\bar{v}_l/\bar{y}_l]} \Rightarrow n''[\bar{v}''/\bar{y}''], \| \bigvee_j (b'_j \wedge e \setminus \theta_l = e'_j \sigma_j \wedge B_j) \|_{[\bar{u}/\bar{x}, \bar{v}''/\bar{y}''], \eta(\zeta)} = true.$$

应用(1.1)中的论证方法, 可得 n', \bar{v}' 和 $\bar{y}', n''[\bar{v}''/\bar{y}''] \xrightarrow{c1v} n'[\bar{v}'/\bar{y}']$ 且 $(m_{i[\bar{u}/\bar{x}]}, n'[\bar{v}'/\bar{y}']) \in S$. 这就完成了(1)的证明.

(2) 对于 τ 迁移和输入迁移可类似证明. 对输入迁移的证明要用到如下事实: 函数 $match'_{c?}$ 中在匹配 $c? x$ 和 $c? y$ 时将 x 和 y 替换为新变量 z , 由于 z 不在 θ 和 σ_j 中出现, 对任意 $v \in Val$ 均有

$$\begin{aligned} (\theta[x \mapsto z])\rho(z \mapsto v) &= \theta_\rho[x \mapsto v], \\ (\sigma_j[y \mapsto z])\rho(z \mapsto v) &= \sigma_j\rho[y \mapsto v]. \end{aligned}$$

(\Leftarrow) 设 S 是包含 $(m_{i[\bar{u}/\bar{x}]}, n_{[\bar{v}/\bar{y}]})$ 的弱互模拟. 定义 ζ 如下:

• 对每一 $X_{m, n}$, 令

$$\zeta(X_{m, n})(\bar{u}, \bar{v}) = \begin{cases} true, & \text{若 } (m_{[\bar{u}/\bar{x}]}, n_{[\bar{v}/\bar{y}]}) \in S; \\ false, & \text{否则.} \end{cases}$$

• 对每一 $Y_{m, n}$, 令 $\zeta(Y_{m, n})(\bar{u}, \bar{v}) = true$ 当且仅当存在 $m'[\bar{u}'/\bar{x}']$ 和 $n'[\bar{v}'/\bar{y}']$, 使得 $(m'[\bar{u}'/\bar{x}'], n'[\bar{v}'/\bar{y}']) \in S, m'[\bar{u}'/\bar{x}'] \xrightarrow{c1v} m_{[\bar{u}/\bar{x}]}, n_{[\bar{v}/\bar{y}]} \Rightarrow n'[\bar{v}'/\bar{y}']$ 且 $(m_{[\bar{u}/\bar{x}]}, n'[\bar{v}'/\bar{y}']) \in S$.

• 对每一 $Y_{\theta, c1e, m, n}$, 令 $\zeta(Y_{\theta, c1e, m, n})(\bar{u}, \bar{v}) = true$ 当且仅当存在 $m'[\bar{u}'/\bar{x}']$ 和 $n'[\bar{v}'/\bar{y}']$, 使得 $(m'[\bar{u}'/\bar{x}'], n'[\bar{v}'/\bar{y}']) \in S,$

$m'[\bar{u}'/\bar{x}'] \xrightarrow{c1v} m_{[\bar{u}/\bar{x}]}, (e\theta)[\bar{u}'/\bar{x}'] = v, n_{[\bar{v}/\bar{y}]} \Rightarrow n'[\bar{v}'/\bar{y}']$ 且 $(m_{[\bar{u}/\bar{x}]}, n'[\bar{v}'/\bar{y}']) \in S$.

• 对每一 $Y_{c1x, m, n}$, 令 $\zeta(Y_{c1x, m, n})(\bar{u}, \bar{v}) = true$ 当且仅当存在 $m'[\bar{u}'/\bar{x}'], n''[\bar{v}''/\bar{y}'']$ 和 $n'[\bar{v}'/\bar{y}']$, 使得 $(m'[\bar{u}'/\bar{x}'], n_{[\bar{v}/\bar{y}]}) \in S,$

$m'[\bar{u}'/\bar{x}'] \xrightarrow{c1x} m_{[\bar{u}/\bar{x}]}, n_{[\bar{v}/\bar{y}]} \xrightarrow{c1y} n''[\bar{v}''/\bar{y}''],$ 对任意 $v \in Val, n''[\bar{v}''/\bar{y}''] \xrightarrow{\tau} n'[\bar{v}'/\bar{y}'],$ 且 $(m_{[\bar{u}/\bar{x}]} \xrightarrow{c1v} v, n'[\bar{v}'/\bar{y}']) \in S$.

则可证 ζ 是 $E_2 \mu E_1$ 的解. 细节从略. □

例: 将本算法用在图 1 中的两个符号迁移图, 生成如下嵌套等式系:

$$\begin{aligned} E_2: X_{m_1, n_1} &= (x=0 \Rightarrow 0=x \wedge X_{m_2, n_2}(x/x, y/y)) \wedge \\ &\quad (true \Rightarrow x=0 \wedge 0=x \wedge X_{n_2, m_2}(y/y, x/x)) \vee \\ &\quad (x>0 \wedge Y_{[x/x, c10, n_2, m_2]}(y/y, x-2/x)) \wedge \\ &\quad (x>0 \Rightarrow X_{m_3, n_1}(x-2/x, y/y)) \\ X_{m_2, n_2} &= true \\ X_{n_2, m_2} &= true \end{aligned}$$

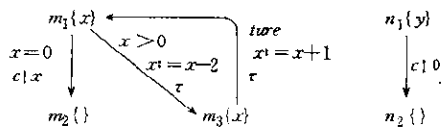


图1 例子

$$X_{n_3, n_1} = X_{n_1, n_1}(x+1/x, y/y) \wedge Y_{[y/y], c10, n_2, m_1}(y/y, x-1/x)$$

$$E_1: Y_{[y/y], c10, n_2, m_3} = Y_{[y/y], c10, n_2, m_1}(y/y, x+1/x)$$

$$Y_{[y/y], c10, n_2, m_1} = (x=0 \wedge 0-x \wedge X_{n_2, m_2}(x/x, y/x)) \vee (x>0 \wedge Y_{[y/y], c10, n_2, m_3}(y/y, x-2/x))$$

简化整理得

$$E_2: X_{n_1, n_1}(x, y) = (x=0) \vee ((x>0 \wedge Y_{[y/y], c10, n_2, m_1}(y, x-1))$$

$$E_1: Y_{[y/y], c10, n_2, m_1}(y, x) = (x=0) \vee (x>0 \wedge Y_{[y/y], c10, n_2, m_1}(y, x-1))$$

使用数学归纳法容易证明 $X_{n_1, n_1}(x, y)$ 为真(即两个图弱互模拟)当且仅当 $x \geq 0$.

3 早弱互模拟

对第 2 节中迟弱互模拟定义中输入迁移部分作如下修改,即得早弱互模拟的定义:

- 只要 $m_\rho \xrightarrow{c\tau} m'_\rho$, 则对任意 $v \in Val$, 都有 $n_c \xrightarrow{c\tau} n'_c, n''_c \xrightarrow{v[\sigma]} n'_c$, 且 $(m_{\rho[v\sigma]}, n'_c) \in R$.

将算法 1 中函数 $match'_{c\tau}$ 涉及到 $newVar$ 的部分改为

```

match'_{c\tau}(\theta, x, m, n) =
  z = new Var()
  for each  $n \xrightarrow{b_j, \sigma_j, c\tau} n_j$ 
     $B'_j = close_\tau(m, \theta[x \mapsto z], n_j, \sigma_j[y \mapsto z])$ 
  for each  $n \xrightarrow{b'_i, \sigma'_i, \tau} n'_i$ 
    if  $(m, n'_i) \notin Visited_{c\tau, m, n}$  then {
       $Visited_{c\tau, m, n} = \{(m, n'_i)\} \cup Visited_{\delta, c\tau, m, n}$ 
      emit( $Y_{c\tau, m, n'_i} = match'_{c\tau}(\theta, x, m, n'_i)$ )
    }
  return( $\forall z((\bigvee_j B_j \wedge B_j) \vee (\bigvee_i B'_i \wedge Y_{c\tau, m, n'_i}(id, \sigma'_i)))$ )

```

就得到计算早弱互模拟的算法.

对符号迁移图做简单的变换就可用本文的算法计算迟、早观察等价,此处不再赘述.

参考文献

- 1 林惠民. 传值系统的互模拟与谓词等式系. 计算机学报, 1998, 21(2): 97~102
(Lin Hui-min. Bisimulations of value-passing systems and predicate equation systems. Chinese Journal of Computers, 1998, 21(2): 97~102)
- 2 Lin H. Symbolic transition graph with assignment. In: Montanari, Sassone eds. Proceedings of the 7th International Conference on Concurrency Theory. Lecture Note in Computer Science 1119, Berlin: Springer-Verlag, 1996. 50~65
- 3 Hennessy M, Lin H. Symbolic bisimulations. Theoretical Computer Science, 1995, 138: 353~389
- 4 Milner R. Communication and Concurrency. Hemel Hempstead; Prentice-Hall, Inc., 1989
- 5 Tarski A. A lattice-theoretical fixpoint theorem and its applications. Pacific Journal of Mathematics, 1955, 5: 285~309

Nesting Predicate Equation Systems and Weak Bisimulations

LIN Hui-min

(Laboratory of Computer Science Institute of Software The Chinese Academy of Sciences Beijing 100080)

Abstract Symbolic transition graphs with assignment is a general semantical model for value-passing processes. Strong bisimulation equivalences between such graphs can be reduced to the greatest solutions to simple predicate equation systems. The aim of this paper is to generalise this result to weak bisimulation equivalences. For this purpose, the notion of nesting predicate equation systems is introduced, and algorithms are presented to reduce weak bisimulation equivalences to the greatest solutions to nesting predicate equation systems of the form $E_2 \mu E_1$.

Key words Value-passing processes, bisimulation, predicate equation systems.