映射 ELOTOS 到基于 FSM 的性能估价模型*

罗铁庚　陈火旺　龚正虎　齐治昌

(国防科技大学计算机系　长沙　410073)

摘要　ELOTOS 是协议描述规范语言 LOTOS 的扩展. 本文用标号转换系统 LTS(labeled transition system)给出了 ELOTOS 的语义. 然后,通过对 LTS 进行踪迹等价性分析,将 ELOTOS 映射到基于有穷状态机 FSM(finite state machine)的性能估价模型.

关键词　ELOTOS,概率规范,LTS,形式语义,FSM,踪迹等价,性能模型.

中图法分类号　TP311

LOTOS[1]是基于进程代数 CCS[2]的协议描述规范语言,已被 ISO 采纳为国际标准. 它面向协议验证,但是它不能描述实际协议的某些性质. 文献[3]给出了 LOTOS 的一种扩充语言 ET-LOTOS,并定义了它的语义,将 ET-LOTOS 按一对一关系映射到性能模型上. ET-LOTOS 是将时间规范和概率规范有机地结合起来的一种语言,它用优先级和权值解决了因延迟时间相同而导致的选择冲突,用事件的年龄转换刻画了系统时间的变迁. 我们在用 ET-LOTOS 进行协议验证(性能分析)和测试的过程中,发现一些不尽人意之处:我们觉得用全局不同的优先级能完全解决选择冲突问题,独立于时间的概率选择应当根据事件的概率密度函数计算,而不应当再用权值来描述;用行动的年龄来描述系统时间的变迁使得把握系统的全局时间非常困难,由于在 ET-LOTOS 中引入了存储时间语句,进行性能估价时,除了行动年龄外,还必须知道行动发生时间;语义中包含年龄转换,导致验证算法状态爆炸;将 ET-LOTOS 映射到性能模型上只是简单的一对一关系,没有严格的语义基础,会出现到达状态的非确定性. 因而,我们在文献[4]中给出了 LOTOS 的一种新的扩充语言 ELOTOS,该语言能有效地描述时间和随机事件的发生. 本文将用 LTS(labeted transition system)给出 ELOTOS 的严格语义. 在已有的工作中,人们对基于 FSM(finite state machine)模型的协议验证和一致性测试技术进行了深入的研究,提出了很多有效的方法,基于 Markov 过程模型进行性能分析已变得越来越逼近现实.[5,6]因此,我们将通过对 LTS 进行踪迹等价性

* 本文研究得到国家自然科学基金和国家 863 高科技项目基金资助. 作者**罗铁庚**,1970 年生,博士生,主要研究领域为协议验证,协议测试,CASE. **陈火旺**,1936 年生,教授,博士导师,主要研究领域为计算机科学理论,软件工程. **龚正虎**,1945 年生,教授,博士导师,主要研究领域为协议工程,计算机网络. **齐治昌**,1942 年生,教授,博士导师,主要研究领域为软件工程.

本文通讯联系人:罗铁庚,长沙 410073,国防科技大学计算机系

本文 1996-11-27 收到修改稿

分析,将 ELOTOS 映射到基于 FSM 的性能估价模型 TFSM.

1 基本定义和表示

我们规定 u 为时间变量,允许时间是离散的或者连续的,时间域是$[0,+\infty)$. 同时,我们用 $et(a)$表示行动 a 被使能的时间,用 $age(a)$表示 a 的年龄,用 $f(a)$表示 a 的延迟时间的概率密度函数,用 $p(a)$表示 a 的优先级,用 $ot(a)$表示 a 发生的时间.

定义 1. 标号转换系统(LTS). LTS 是一个四元偶$\langle S,\Sigma,\Delta,s_0\rangle$,其中 S 是一个非空状态集,$s_0\in S$ 是初始状态. Σ 是一个集合,$a\in\Sigma$ 是一个带有信息 $et(a),age(a),f(a)$和 $p(a)$的行动,叫作可观察行动(Observable Action),$\tau\notin\Sigma$ 是内部行动(Internal Action). Δ 是转换关系的集合,$\Delta\subseteq S\times(\Sigma\cup\{\tau\})\times T\times S$,它的元素是四元偶$(cur,a,u,next)$,也可以表示为:$cur\xrightarrow{a}_u next$.

考虑到非确定性,在 LTS 中,执行同样的可观察行动序列,可能会到达 LTS 中的不同状态. 针对每一个可观察行动序列,为了避免到达状态的非确定性,我们引用了多状态(Multi-state)的概念,每个多状态包含了一个可观察行动序列所有可达的最后状态.

定义 2. 多状态集(Multi-state Set). LTS $L=\langle S,\Sigma,\Delta,s_0\rangle$的多状态集是这样的一个集合:$\coprod_S=\{S_i\subseteq S\mid$存在 $a_1,\ldots,a_n\in\Sigma$,对于任意 $s\in S_i$,$\exists\ q_1,\ldots,q_n(=s)\in S$,使得 $s_0\xrightarrow{a_1}_u q_1,\ldots,q_{n-1}\xrightarrow{a_n}_u q_n\}$.

定义 3. 基于 FSM 的性能模型 PMBFSM(performance model based on FSM). PMBFSM 是一个六元偶$\langle S,X,Y,\Delta,s_0,E\rangle$,其中 S 是非空有穷集,它的元素是状态,$s_0\in S$ 是初始状态. X 是一个集合,它的元素是一个带有信息 $et(a),age(a),f(a)$和 $p(a)$的行动,叫作可观察行动. Y 是一个集合,它的元素是一个带有信息 $ot(a)$的行动,叫作被观察行动(Observed Action). Y 中还包括一个用来表示空行动(没有行动发生)的 Θ. Δ 是一个转换关系的集合,$\Delta\subseteq S\times X\to S\times Y$. 每个元素是一个四元偶 $(cur,a)\to(next,b)$,也可表示为 $cur\xrightarrow{a/b}next$. 映射 $E:S\to P(\Delta)$ ($P(\Delta)$是 Δ 的幂集),定义每个状态中被使能的转换的集合.

在协议验证和测试技术中,最重要的一种方法是等价性分析. 等价性分析方法包括观察等价、测试等价、踪迹等价和实现等价. 我们定义踪迹等价为 ELOTOS 规范和基于 FSM 的性能模型之间的等价关系.

定义 4. 踪迹(Trace). 在 LTS $L=\langle S,\Sigma,\Delta,s_0\rangle$中,对于任意 $p\in S$,p 的踪迹是 $Tr(p)=\{\sigma\in\Sigma^*\mid$存在 $q_1,\ldots,q_n(q)\in S,a_1,\ldots,a_n\in\Sigma$,使得 $p\xrightarrow{a_1}_u q_1,\ldots,q_{n-1}\xrightarrow{a_n}_u q_n,\sigma=a_1,\ldots,a_n\}$,同时,$Tr(L)=Tr(s_0)$. 在 PMBFSM $F=\langle S,X,Y,\Delta,s_0,E\rangle$中,对于任意 $p\in S$,p 的踪迹是 $Tr(p)=\{\sigma\in Y^*\mid$存在 $q_1,\ldots,q_n(q)\in S,a_1,\ldots,a_n\in X,b_1,\ldots,b_n\in Y\backslash\{\Theta\}$,使得 $p\xrightarrow{a_1/b_1}q_1,\ldots,q_{n-1}\xrightarrow[a]{a_n/b_n}q_n,\sigma=b_1,\ldots,b_n\}$,同时 $Tr(F)=Tr(s_0)$.

定义 5. 踪迹等价(Trace Equivalence). 两个 LTS L 和 M 之间的踪迹等价关系(记为 $L=_tM$)当且仅当 $Tr(L)=Tr(M)$ 时成立. 两个 PMBFSM F 和 H 之间的踪迹等价关系(记为 $F=_tH$)当且仅当 $Tr(F)=Tr(H)$ 时成立. 一个 LTS L 和一个 PMBFSM F 之间的踪迹

等价关系(记为 $L\approx_u F$)当且仅当 $Tr(L)=Tr(F)$ 时成立.

2 ELOTOS 的语义

类似于 ISO 组织定义 LOTOS 语义的方法[1],我们在本节给出一个 ELOTOS 标准规范(Canonical ELOTOS Specification)[1]的推导系统,用于定义 LTS 中的转换关系 Δ. 其中字串 $[t_1/x_1,\ldots,t_n/x_n]B$ 表示 B 中 $x_1,\ldots,x_n$ 的所有出现被相应的 $t_1,\ldots,t_n$ 代替. 同时,我们用 δ 专门表示进程的成功终止. 在 LTS 中,变量 u 用来表示全局时间. 根据前一行动的发生时间、该行动的年龄和行动类型(是否使用存储计时),可以计算出 u 的值.

$A_1>\tau;B \xrightarrow{\tau}_u B$ $\quad A_2>\mathrm{exit}(E_1,\ldots,E_n)\xrightarrow{\delta}_u \mathrm{stop}$

$A_3>ty_i=y_i$ iff $d_j=?\ y_i(1\leqslant i\leqslant n,1\leqslant j\leqslant m)$,

$g\ d_1,\ldots,d_m;B \xrightarrow{g}_u [\ ty_1/y_1,\ldots,ty_n/y_n]B$

如果 SP 为真,$g\ d_1,\ldots,d_m[SP];B \xrightarrow{g}_u [\ ty_1/y_1,\ldots,ty_n/y_n]B$

$R_1>$ $\dfrac{[t_1/x_1,\ldots,t_n/x_n]B_1 \xrightarrow{a}_u B_2}{}$ $\quad R_2>\dfrac{B_1\xrightarrow{a}_u B_2, name(a)\in\{g_1,\ldots,g_n\}}{}$

let $x_1=t_1,\ldots,x_n=t_n$ in $B_1\xrightarrow{a}_u B_2$ $\quad$ hide $g_1,\ldots,g_n$ in $B_1\xrightarrow{\tau}_u$ hide $g_1,\ldots,g_n$ in B_2

$R_3>$ $\dfrac{B_1\xrightarrow{a}_u B'_1,\ name(a)\neq\delta}{}$

$B_1>>\mathrm{accept}\ x_1,\ldots,x_n$ in $B_2\xrightarrow{a}_u B'_1>>\mathrm{accept}\ x_1,\ldots,x_n$ in B_2

$B_1\xrightarrow{\delta}_u B'_1, v_1,\ldots,v_n$ 是 $x_1,\ldots,x_n$ 的项实例值

$B_1>>\mathrm{accept}\ x_1,\ldots,x_n$ in $B_2\xrightarrow{\tau}_u [v_1/x_1,\ldots,v_n/x_n]B_2$

$R_4>$ $\dfrac{B_1\xrightarrow{a}_u B'_1, name(a)\neq\delta}{}$ $\quad \dfrac{B_1\xrightarrow{\delta}_u B'_1}{}$ $\quad \dfrac{B_2\xrightarrow{a}_u B'_2}{}$

$B_1[>B_2\xrightarrow{a}_u B'_1[>B_2$ $\quad B_1[>B_2\xrightarrow{\tau}_u B'_1\ B_1[>B_2\xrightarrow{a}_u B'_2$

$R_5>$ $\dfrac{B_1\xrightarrow{a}_u B'_1, name(a)\notin\{g_1,\ldots,g_n,\delta\}}{}$

$B_1|[g_1,\ldots,g_n]|B_2\xrightarrow{a}_u B'_1|[g_1,\ldots,g_n]|B_2$

$B_2\xrightarrow{a}_u B'_2, name(a)\notin\{g_1,\ldots,g_n,\delta\}$

$B_1|[g_1,\ldots,g_n]|B_2\xrightarrow{a}_u B_1|[g_1,\ldots,g_n]|B'_2$

$B_1\xrightarrow{a}_u B'_1, B_2\xrightarrow{a}_u B'_2, name(a)\in\{g_1,\ldots,g_n,\delta\}$

$B_1|[g_1,\ldots,g_n]|B_2\xrightarrow{a}_u B'_1|[g_1,\ldots,g_n]|B_2$

$B_1|[]|B_2\xrightarrow{a}_u B'$ $\quad B_1|[g_1,\ldots,g_n]|B_2\xrightarrow{a}_u B', g_1,\ldots,g_n$ 包括了所有事件

$B_1\|\|B_2\xrightarrow{a}_u B'$ $\quad B_1\|B_2\xrightarrow{a}_u B'$

$R_6>$ $\dfrac{B_1\xrightarrow{a}_u B'_1}{}$ $\quad \dfrac{B_2\xrightarrow{a}_u B'_2}{}$

$B_1[]B_2\xrightarrow{a}_u B'_1$ $\quad B_1[]B_2\xrightarrow{a}_u B'_2$

$R_7>$ $\dfrac{B_1\xrightarrow{a}_u B'_1, SP\text{ 为真}}{}$

$[SP]\to B_1\xrightarrow{a}_u B'_1$

R_8> B_p 是 P 的行为表达式,$h_1,\ldots,h_n$ 是 p 的形式化门径参数,$x_1,\ldots,x_n$ 是 p 的形式化变量参数.

$$\frac{(\lceil t_1/x_1,\ldots,t_n/x_n\rceil B_p)\lceil g_1/h_1,\ldots,g_n/h_n\rceil \xrightarrow{a}_u B' \qquad B_1 \xrightarrow{a}_u B_2}{p\lceil g_1,\ldots,g_n\rceil(t_1,\ldots,t_m) \xrightarrow{a}_u B' \qquad (B_1) \xrightarrow{a}_u B_2}$$

R_9> $\dfrac{B_1 \xrightarrow{a}_u B_2, t_1 \leqslant age(a) \leqslant t_2}{\text{delay\_attr } a(t_1,t_2,f,p) \text{ in } B_1 \xrightarrow{a}_u \text{delay\_attr } a\langle t_1,t_2,f,p\rangle \text{ in } B_2}$

$$\frac{B_1 \xrightarrow{b}_u B_2, b \neq a}{\text{delay\_attr } a(t_1,t_2,f,p) \text{ in } B_1 \xrightarrow{b}_u \text{delay\_attr } a(t_1,t_2,f,p) \text{ in } B_2}$$

R_{10}> $\dfrac{B_1 \xrightarrow{a}_u B_2, t_1 \leqslant age(a) \leqslant t_2}{\text{p\_delay\_attr } a\langle t_1,t_2,f,p\rangle \text{ in } B_1 \xrightarrow{a}_u \text{p\_delay\_attr } a\langle t_1,t_2,f,p\rangle \text{ in } B_2}$

R_{11}> $\dfrac{B_1 \xrightarrow{a}_u B_2, t_1 \leqslant age(a) \leqslant t_2}{\text{m\_delay\_attr } a\langle t_1,t_2,f,p\rangle \text{ in } B_1 \xrightarrow{a}_u \text{m\_delay\_attr } a\langle t_1,t_2,f,p\rangle \text{ in } B_2}$

3　将 LTS 映射到 TFSM

ELOTOS 的表达能力不弱于图灵机(Turing Machine),只有加以限制的 ELOTOS 才能被有穷状态转换系统模拟.我们给出了下面一组充分条件,确保存在等价于受限 ELOTOS 的有穷状态转换系统.

(1).门径中不含数值传递.

(2).每个表达示"*choice* x []B"x 的取值范围为一个有穷元素集合.

(3).每个进程 $p:=A|[G]|B$ 中的 A 和 B 不能用 p 作为子表达式.

给定一个 LTS L,我们要构造出一个产生 LTS 的所有踪迹的 PMBFSM F.如果在 L 中,对于某一个输入行动,L 不能形成一条有效的踪迹,那么在 F 中我们用 Θ 表示空输出.从 L 转换到 F 包括将 L 的多状态映射到 F 的状态.在 F 中,下沉状态 s_Θ 表示在相应的 LTS 中发生了死锁并且还没有被解除时的情况.我们把这样的一个 PMBFSM F 叫作踪迹有穷状态机 TFSM(trace finite state machines).定义 6 给出了 L 到 F 的映射算法.

定义 6. 踪迹有穷状态机(TFSM).给定一个 LTS $L=\langle S,\Sigma,\Delta,s_0\rangle$,它的踪迹有穷状态机是一个 PMBFSM $F=\langle S',X,Y,\Delta',s'_0,E\rangle$ 使得 $X=\Sigma$. $Y=\Sigma\cup\{\Theta\}$. S' 是一个有穷状态集,并且 $s_\Theta\in S'$.映射 $E:S\to P(\Delta)$($P(\Delta)$是 Δ 的幂集),定义每个状态中被使能的转换的集合.令 Π_S 为 S 的多状态集,那么存在一对一的影射关系 $\Psi:\Pi_S\to S'\setminus\{s_\Theta\}$,并且对于所有的 s_i, $s_j\in\Pi_S$ 和所有的 $a\in X$,

$(\Psi(s_j),a)\in\Delta'(\Psi(s_i),a)$且 $ot(a)=u$ 当且仅当 $s_i \xrightarrow{a}_u S_j$,

$(s_\Theta,\Theta)\in\Delta'(\Psi(s_i),a)$ 当且仅当 $a\notin Tr(s_i)$;

$\{(s_\Theta,\Theta)\}=\Delta'(s_\Theta,a)$,　如果 $s_0\in s_i, s'_0=\Psi(s_j)$.

定理 1. 给定一个 LTS L 和它的相应的 TFSM F,对于所有的 $\sigma\in\Sigma^*$ 和所有的 $\gamma=\sigma\in Y^*$,$\sigma\in Tr(L)$ 当且仅当 $\gamma\in Tr(F)$,即 $L\approx_{tr}F$.

定理 2. 对于任意两个 LTS L,M 和它们相应的 TFSM F,G,$L=_{tr}M$ 当且仅当 $F=_{tr}G$.

4 小 结

我们已经成功地给出了ELOTOS的语义,并且给出了将ELOTOS映射到TFSM的算法.和文献[3]比较,我们的贡献主要在以下几个方面:①省略权值,用不同优先级予以处理,简化了问题求解复杂度.②计算全局时间变量比年龄转换更容易控制状态爆炸.③由于在ELOTOS中引入了存储时间语句,因此引入了行动发生时间,从而能够进行性能估价.④根据踪迹语义将LTS映射到TFSM上.

基于FSM的性能模型上的性质和算法有待进一步地深入研究.我们目前正在进行的工作是可达性分析算法[7]和模型检验算法[8]的研究.

参考文献

1 Brinksma ED. Information processing systems——open systems interconnection——LOTOS——a formal description technique based on the temporal ordering of observational behaviour. International Standard, ISO 8807.

2 Milner R. Communication and concurrency. Prentice-Hall, 1989.

3 Marson M A, Bianco A *et al*. A LOTOS extension for the performance analysis of distributed systems. IEEE/ACM Transactions on Networking, April 1994,**2**(2):151~165.

4 Luo T G, Chen H W, Qi Z C *et al*. A specification language for formal development environment of practical protocols. In: Proc. of Changsha Inter. CASE Symp.'95, Oct. 1995.

5 Alur R, Courcoubetis C, Dill D. Model-checking for probabilistic real-time systems. Proc. 18th Int. Coll. on Automata, Language and Programming, Madrid, Spain, July 1991, LNCS 510.

6 Hansson H A. Modeling real-time and reliability. Formal Technique in Real-time and Fault-tolerant System. J. Vytopil[Ed.], 1993.

7 龚正虎.计算机网络协议工程.长沙:国防科大出版社,1993.

8 Clarke E M, Emerson E A, Sistla A P. Automatic verification of finite-state concurrent systems using temporal logic specifications. ACM Transaction on Programming Languages and Systems, April 1986,**8**(2):244~263.

MODELING ELOTOS BY PERFORMANCE EVALUATION MODEL BASED ON FSM

LUO Tiegeng CHEN Huowang GONG Zhenghu QI Zhichang

(*Department of Computer Science Changsha Institute of Technology Changsha* 410073)

Abstract ELOTOS is an extension of protocol specification language LOTOS which is an ISO standard. In this paper, the authors try to give the semantics of ELOTOS by defining a derivation system (like LOTOS). Then, from LTS (labeled transition system) of restricted ELOTOS, they construct the TFSM(trace finite state machine) for trace semantics, and TFSM is a kind of performance evaluation model.

Key words ELOTOS, probabilistic specification, labeled transition system, formal semantics, finite state machine, trace semantics, performance model.

Class number TP311