概率实时时态认知逻辑模型检测中抽象技术的研究

刘志锋,孙 博,周从华
(江苏大学计算机科学与通信工程学院,江苏镇江 212013)

摘 要: 概率实时时态认知逻辑 PTACTLK 模型检测面临着与传统模型检测同样的挑战,即状态空间爆炸问题.抽象是缓解状态空间爆炸问题的最为有效的方法之一.为了缓解概率实时时态认知逻辑模型检测中的状态空间爆炸问题,我们给出了一种抽象技术:对于 PTACTLK 中的实时部分 PTACTL,采用抽象离散时钟赋值,把概率实时解释系统的无限状态空间转化成有限形式;对于 PTACTLK 中的认知算子 K,给出了抽象状态关于智体认知等价的定义.定义了概率实时解释系统的抽象模型,给出了抽象模型上概率实时时态认知逻辑的语义,并证明了由抽象技术演绎得到的抽象模型是原始模型的上近似.最后通过一个通信协议来说明抽象技术的有效性.

关键词: 模型检测; 概率实时时态认知逻辑; PTACTLK; 状态空间爆炸; 抽象
中图分类号: TP301 **文献标识码:** A **文章编号:** 0372-2112 (2013)07-1343-09
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2013.07.016

Abstraction in Model Checking Probabilistic Real-Time Temporal Logic of Knowledge

LIU Zhi-feng, SUN Bo, ZHOU Cong-hua
(*School of Computer Science and Telecommunication Engineering, Jiangsu University, Jiangsu, Zhenjiang* 212013, *China*)

Abstract: The same challengs facing model checkings in probabilistic real-time temporal logic of knowledge PTACTLK is the same as traditional model one. That is the state space explosion problem. Abstraction is one of the most effective methods to alleviate the state space explosion problem. In order to alleviate the problem of the state space explosion in model checking probabilistic real-time temporal logic of knowledge, an abstraction technique is presented. For the real time part of PTACTLK, that is PTACTL, we adopt the abstract discrete clock valuations, and the infinite state space of a probabilistic real time was interpreted into a finite form. For the epistemic operator K in PTACTLK, the definition of epistemic equivalent to an agent between abstract states is given. We define the abstract model of the interpreted system in a probabilistic real time and present the semantics of PTACTLK on the abstract model. We prove that the abstract model obtained by using the abstraction techniques is the upper approximation of the original model. At last, a simple communication protocol is adopted to illustrate the effectiveness of our abstraction techniques.

Key words: model checking; probabilistic real-time temporal logic of knowledge; PTACTLK; state space explosion; abstraction

1 引言

模型检测[1]是一种很重要的有限状态系统的自动验证技术,已经应用到了硬件检测、通信协议以及控制系统的验证中并受到了广泛的关注.在模型检测中,把多智体系统 S 建模成一个适当的模型 M_S,用逻辑公式 ϕ_p 来表示要检测的规范 P,这样检测一个多智体系统 S 是否满足一个规范 P 就转化成了验证 $M_S \models \phi_p$ 是否成立的模型检测问题.对知识进行推理[2]一直是人工智能中的焦点,为此,这些年来研究人员提出并改进了一些基于模态逻辑的规范形式,其中得到最广泛关注的是时态认知逻辑.时态认知逻辑是为多智体系统建模和推理的一个规范语言.然而,用模型检测对时态认知逻辑进行验证仍缺乏一些必要的功能,其中一个就是实时.A Lomuscio 等人在文献[3]中把实时结合进来,并提出了一个对多智体系统中的实时和知识进行推理的逻辑,即实时时态认知逻辑 TACTLK.在实时时态认知逻辑中加入概率因素则得到概率实时时态认知逻辑 PTACTLK.

收稿日期:2012-09-27;修回日期:2012-12-03;责任编辑:郭游
基金项目:国家自然科学基金 (No.61003288,No.6111130184);江苏省自然科学基金(No.BK2010192);教育部博士点基金(No.20093227110005);江苏大学高级人才科研启动基金(No.12JDG061)

概率实时时态认知逻辑 PTACTLK 模型检测与传统模型检测一样,也面临着状态空间爆炸问题,即状态空间随着并发分量的增加而呈指数级的增长.由于模型检测算法是在状态空间中穷举搜索来寻找满足所验证属性的状态,如果状态空间是无限的或太大,这就会严重影响模型检测的执行效率.为了缓解状态空间爆炸问题,学者们提出了一些技术,如偏序规约[4]、对称规约[5]、基于 OBDD 的符号化计算、抽象[6,7]以及限界模型检测[8,9]等.其中抽象是克服状态空间爆炸问题的最为有效的方法之一.抽象技术是利用抽象函数对原始模型的状态空间进行等价划分,从而得到原始模型的一个对应的抽象模型.这样就删除了原始模型中与验证属性无关的信息,属性验证在得到的抽象模型中进行,由于状态空间相对较小,使验证效率大为提高.

限界检测也是一种克服状态空间爆炸的有效技术,其基本思想是以一种递增的方式搜索属性成立的证据或者失效的反例,从而避免了全局空间的构造.目前学术界对同步多智体系统上的时态认知逻辑[10]以及概率实时认知逻辑均提出了有效的限界检测算法[11].而对于抽象技术,时态逻辑模型检测中已有关于抽象及求精技术的研究[7,12],概率时态认知逻辑模型检测已经建立了三值抽象技术,在实时系统中亦已有关于建立抽象模型的研究[13].但是就我们所知,在概率实时时态认知逻辑的模型检测中还没有任何关于抽象技术的探讨.因此,本文主要对概率实时时态认知逻辑模型检测中的抽象技术进行系统的研究.我们的主要工作有:(1)对概率实时时态认知逻辑 PTACTLK 中的实时部分 PTACTL,采用抽象离散时钟赋值[13]隐式构造概率实时解释系统状态空间的时钟区域(clock regions),从而得到概率实时解释系统状态空间的有限形式,对于 PTACTLK 中的认知算子 K,给出了两个抽象状态关于智体认知等价的定义,这样就可以把满足该定义中约束的抽象状态进行合并,使其成为一个等价类,从而进一步简化概率实时解释系统的状态空间;(2)利用上面给出的抽象技术,从概率实时解释系统的原始模型 M 推演出了对应的抽象模型 M^A,给出了抽象模型上概率实时时态认知逻辑的语义,并证明了抽象模型是原始模型的上近似;(3)通过对一个简单通信协议的状态空间的简化来说明我们抽象技术的有效性.

2 概率实时时态认知逻辑 PTACTLK 语法及其语义

概率实时时态认知逻辑 PTACTLK 是在实时时态认知逻辑 TACTLK 中加入概率因素 P 得到的,它用于为多智体系统进行建模和推理.其中,实时时态认知逻辑是由表示分支实时逻辑[14]的 TCTL 与表示知识操作符的模态逻辑[15]S5n 的结合.

定义 1 (概率实时时态认知逻辑 PTACTLK 语法)

设 PV 是一命题变量的集合,其中包含表示常量 true 的符号 T,Ag 是 m 个智体(agent)的一个集合,I 是实数集 $\mathbf{R}$ 中一个时间间隔并且其边界均为整数.假设 $p\in PV$,$i\in Ag$ 且 $\Gamma\subseteq Ag$,则 PTACTLK 公式集合如下定义:

$$\varphi::=p\mid\neg p\mid\varphi\wedge\varphi\mid\varphi\vee\varphi\mid A(\varphi U_I^{\rhd p}\varphi)\mid A(\varphi R_I^{\rhd p}\varphi)\mid K_i^{\rhd p}\varphi\mid D_\Gamma^{\rhd p}\varphi\mid E_\Gamma^{\rhd p}\varphi\mid C_\Gamma^{\rhd p}\varphi,\rhd\in\{<,\leqslant,>,\geqslant\}$$

其中,$A(\varphi U_I^{\rhd p}\psi)$表示"对于所有的计算路径满足:在时间间隔 I 中的一个状态上 ψ 成立,并且在此之前的所有状态上 φ 成立.且所有这些路径的概率之和满足 $\rhd p$";$A(\varphi R_I^{\rhd p}\psi)$表示"对于所有的计算路径满足:在时间间隔 I 中一个状态上 φ 与 ψ 均成立,且在此之前的所有状态上 ψ 一直成立,或者 ψ 在时间间隔 I 中所有状态上一直成立.且所有这些路径的概率之和满足 $\rhd p$";$K_i^{\rhd p}\varphi$ 表示"智体 i 认为 φ 成立的概率为 $\rhd p$".

对于其他时态修饰符,有 $AG_I^{\rhd p}\varphi=A(\bot R_I^{\rhd p}\varphi)$,$AF_I^{\rhd p}\varphi=A(TU_I^{\rhd p}\varphi)$,$\bot=\neg T$,$\alpha\rightarrow\beta=\neg\alpha\vee\beta$ 以及 $\alpha\leftrightarrow\beta=(\alpha\rightarrow\beta)\wedge(\beta\rightarrow\alpha)$.

为了给出概率实时时态认知逻辑的语义,首先回顾一下关于时钟约束[16]、离散概率分布和概率时间自动机[17]的知识.

定义 2 (时钟约束[16])

时钟变量集合 C 上的一个时钟约束 g 是根据以下语法定义的:$g::=x<c\mid x\leqslant c\mid x>c\mid x\geqslant c\mid g\wedge g$.其中,$c\in N$,$x\in C$ 是一个时钟变量.我们用 $CC(C)$ 表示在时钟变量集合 C 上的所有时钟约束的集合.

定义 3 (离散概率分布[17])

在一个可数集合 Q 上的离散概率分布是一个函数 $\mu:Q\rightarrow[0,1]$,使 $\sum_{q\in Q}\mu(q)=1$.对于一个不可数集合 Q',用 $\mathrm{Dist}(Q')$表示 Q' 的可数子集上的概率分布的集合.

时间自动机[18,19]用于为时间关键系统(time critical systems)的行为进行建模,概率时间自动机是对时间自动机的概率扩展,其定义如下.

定义 4 (概率时间自动机[3])

一个概率时间自动机形式上可表示为一个元组:$PTA=(L,Act,C,l_0,prob,Inv)$.其中,$L$ 表示由位置(location)组成的一个有限集合,$l_0\in L$ 表示初始位置,Act 表示行为的有限集合,C 是时钟变量的有限集合,$prob$ 是概率边关系:$prob\subseteq L\times CC(C)\times Act\times Dist(2^C,L)$,$Inv$ 是一个位置不变函数 $Inv:L\rightarrow CC(C)$,它给每个位置都分配一个时钟约束,该时钟约束定义了概率时间自动机停留在该位置上必须要满足的条件.

若有一离散转换$(l,g,\alpha,p)\in prob$发生,即当前时钟赋值v要满足时钟约束g,则从位置l到达位置l'且集合D中的时钟变量的值重置为0的概率是$p(D,l')$.

由于一个多智体系统(MAS)是由n个智体组成的($n>0$,且n为整数),若每个智体$i(1\leqslant i\leqslant n)$是用一个概率时间自动机$PTA_i=(L_i,Act_i,C_i,l_0^i,prob_i,Inv_i)$来建模,则该多智体系统可建模成这$n$个概率时间自动机的平行组合(parallel composition).下面是多个概率时间自动机平行组合的定义.

定义5 (概率时间自动机的平行组合[3])

n个概率时间自动机$PTA_i(1\leqslant i\leqslant n)$的平行组合是一个全局概率时间自动机(global probabilistic timed automaton) $PTA=(L,Act,C,l_0,prob,Inv)$,其中,$L=\prod_{i=1}^{n}L_i$,即概率时间自动机$PTA$中的一个全局位置(global location)l是一个元组:$l=(l_1,l_2,\cdots,l_n)$,$l_i\in L_i(1\leqslant i\leqslant n)$;$Act=\bigcup_{i=1}^{n}Act_i$,$C=\bigcup_{i=1}^{n}C_i$,$l_0=(l_0^1,l_0^2,\cdots,l_0^n)$,$l_0^i(1\leqslant i\leqslant n)$表示第$i$个概率时间自动机$PTA_i$的初始位置;$Inv(l_1,l_2,\cdots,l_n)=\wedge_{i=1}^{n}Inv(l_i)$;若$((l_1,l_2,\cdots,l_n),g,\alpha,p)\in prob$,则从全局位置$(l_1,l_2,\cdots,l_n)$转换到另一全局位置$(l'_1,l'_2,\cdots,l'_n)$,且将$D=\sum_{i\in Act(\alpha)}D_i$中的时钟变量重置为0的概率为$p$.

上面的$Act(\alpha)$表示其行为的集合$Act_i(1\leqslant i\leqslant n)$中包含$\alpha$的概率时间自动机$PTA_i$的下标的集合,即$Act(\alpha)=\{1\leqslant i\leqslant n\mid \alpha\in Act_i\}$. $D(D\subseteq C)$是在全局转换中重置为0的时钟变量的集合.

由于实时时态认知逻辑的语义模型是实时解释系统[3],则概率实时时态认知逻辑的语义模型是概率实时解释系统,其定义如下.

定义6 (概率实时时态认知逻辑PTACTLK语义模型)

概率时间自动机$PTA=(L,Act,C,l_0,prob,Inv)$对应的概率实时解释系统是一个元组$M=(Q,q_0,P,\sim_1,\cdots,\sim_n,P_1,\cdots,P_n,V)$,其中:

(1)Q是状态的有限集合,是$L\times R^{|C|}$的子集,即$Q\subseteq L\times R^{|C|}$. $R^{|C|}$表示时钟变量集合C上的时钟赋值的集合,则Q中的每一个状态都是由一个位置l和一个时钟赋值v组成的元组:(l,v). Q中的所有状态都是可到达的;

(2)$q_0=(\ell_0,v_0)$是初始状态,且时钟赋值v_0满足:$\forall x\in C$,有$v_0(x)=0$;

(3)P为状态转换概率函数:$P:Q\times Q\to[0,1]$.两个状态集合之间的转换关系可表示为:$E\subseteq(L\times R^{|C|})\times(Act\cup R^+)\times(L\times R^{|C|})$,存在两种转换关系,

(a)时间转换:对$\delta\in R^+$,$(\ell,v)\xrightarrow{\delta}(\ell,v+\delta)$,当且仅当$v\mid=Inv(\ell)$,$v+\delta\mid=Inv(\ell)$;

(b)行为转换:对$a\in Act$,$(\ell,v)\xrightarrow{a}(\ell',v')$当且仅当$(\exists cc\in CC(C))(\exists D\subseteq C)$使:$\ell\xrightarrow{cc,a,D}\ell'\in E$,且$v\mid=cc$,$v'=v[D:=0]\mid=Inv(\ell')$;

其中,$v'=v[D:=0]$表示时钟赋值v'是这样得到的:$\forall x\in D,v'(x)=0$,$\forall x\in C\setminus D,v'(x)=v(x)$.其中$D$是在该转换发生时要重置为0的时钟变量的集合;

(4)$\sim_i\subseteq Q\times Q(1\leqslant i\leqslant n,n$为智体的个数)是一个认知等价关系:$(\ell,v)\sim_i(\ell',v')$当且仅当对智体$i(1\leqslant i\leqslant n)$,有$\ell_i(\ell)=\ell_i(\ell')$且$v\cong v'$.其中,$\ell_i(\ell)$表示智体$i$在全局位置$\ell$中的位置分量,$v\cong v'$表示时钟赋值$v$与$v'$是等价的.事实上,$\sim_i$是一个认知可访问关系;

(5)$P_i:Q\times Q\to[0,1](1\leqslant i\leqslant n)$是认知关系上的概率函数,满足$\forall q\in Q$,$\sum_{q'\in Q}P_i(q,q')=1$;

(6)$V:Q\to 2^{PV}$是一个赋值函数,有$V((\ell,v))=V_{PTA}(\ell)$;

其中,$V_{PTA}(\ell)$表示在概率时间自动机PTA的位置ℓ上成立的命题变量集合.

定义7 (概率实时时态认知逻辑PTACTLK语义:满足性关系)

设$M=(Q,q_0,P,\sim_1,\cdots,\sim_n,P_1,\cdots,P_n,V)$是一概率实时解释系统,$M,q\mid=\alpha$表示PTACTLK公式$\alpha$在$M$中的状态$q$上为真.在下面的满足性关系中,我们省略了符号$M$.假设下面的$p,q,\phi$和$\varphi$均为PTACTLK公式,满足性关系"$\mid=$"如下归纳定义:

$q\mid=p$当且仅当$p\in V(q)$,其中p为一原子命题;

$q\mid=\neg p$当且仅当$p\notin V(q)$,其中p为一原子命题;

$q\mid=\phi\vee\varphi$当且仅当$q\mid=\phi$或$q\mid=\varphi$;

$q\mid=\phi\wedge\varphi$当且仅当$q\mid=\phi$且$q\mid=\varphi$;

$q\mid=A(\phi U_I^{\rhd p}\varphi)$当且仅当$\forall\rho\in f_{PTA}(q)$,$\rho\mid=\phi U_I\varphi$且$\sum_{\rho\in f_{PTA}(q)}\mathrm{Prob}(\rho)\rhd p$.其中,$\rhd\in\{<,\leqslant,>,\geqslant\}$.

$q\mid=A(\phi R_I^{\rhd p}\varphi)$当且仅当$\forall\rho\in f_{PTA}(q)$,$\rho\mid=\phi R_I\varphi$,且$\sum_{\rho\in f_{PTA}(q)}\mathrm{Prob}(\rho)\rhd p$.

$q\mid=K_i^{\rhd p}\varphi$当且仅当$\sum_{q'\mid=\varphi}P_i(q,q')\rhd p$;

$q\mid=E_\Gamma^{\rhd p}\varphi$当且仅当$\sum_{q'\mid=\varphi}\sum_{i\in\Gamma}P_i(q,q')\rhd p$;

$q\mid=D_\Gamma^{\rhd p}\varphi$当且仅当$\sum_{q'\mid=\varphi}\prod_{i\in\Gamma}P_i(q,q')\rhd p$;

上面的$\forall\rho\in f_{PTA}(q)$表示从状态$q$开始的任意一条路径;$\rho\mid=\phi U_I\varphi$当且仅当$(\exists r\in I)(\pi_\rho(r)\mid=\varphi$且$(\forall r'<r)(\pi_\rho(r')\mid=\phi))$,表示在时间间隔$I$内存在一时刻$r$,路径$\rho$上该时刻对应的状态满足公式$\varphi$,并且在此之

前的所有状态均满足 $\phi;\rho \models \phi R_I \varphi$ 当且仅当($\forall r \in I$)($\pi_\rho(r) \models \varphi$ 或($\exists r' < r$)($\pi_\rho(r') \models \phi$)). $C_\Gamma^{\triangleright p}\varphi$ 是 $E_\Gamma^{\triangleright p}\varphi$ 的传递闭包,在此省略了 $C_\Gamma^{\triangleright p}\varphi$ 的满足性定义.

3 抽象

3.1 抽象技术

概率实时解释系统的状态集 Q 中的每一个状态可表示为(ℓ, v)的形式,ℓ 是一个全局位置,v 是对所有时钟变量的一个赋值.由于时间连续的属性,$v \in R^+$,因此概率实时解释系统的状态空间是无限的,从而对概率实时解释系统进行模型检测时不能利用现有的有限状态系统模型检测算法.为了将其转化为有限状态系统的模型检测问题,需要对概率实时解释系统的状态空间进行等价划分,以尽可能的简化其状态空间.

假设 $M=(Q, q_0, P, \sim_1, \cdots, \sim_n, P_1, \cdots, P_n, V)$是一概率实时解释系统的原始模型,我们的目标是给出一种抽象技术,通过抽象能够从该原始模型演绎出一个对应的抽象模型 $M^A=(Q', q_0', P', \sim_1', \cdots, \sim_n', P_1', \cdots, P_n', V')$,从而可以在保持原始模型的属性的条件下在得到的抽象模型中进行模型检测.

对于为多智体系统建模的概率时间自动机中的每个时钟变量 $x \in C$,用 I_x 表示它的整数部分变量,用 F_x 表示它的小数次序变量.I_x 表示 x 的整数部分,即如果 $x \leqslant c_x$,$I_x = \lfloor x \rfloor$,否则 $I_x = c_x$(c_x 是与 x 比较的最大时钟常数).因此 I_x 是一个取值范围为 0 到 c_x 的整数.对于在时钟赋值 v 下满足 $v(x) \leqslant c_x$ 的所有时钟变量 x,对它们的小数部分 $fract(x)$ 进行排序,用 F_x 表示每一个时钟变量 x 的小数部分在这个排序中的位置.对满足 $x \leqslant c_x$ 的时钟变量 x,$F_x=0$ 当且仅当 x 的小数部分 $fract(x)=0$.由此可知,F_x 是取值范围为 0 到 n 的整数,其中 n 为时钟变量的个数.

定义 8 (离散时钟赋值)

为一个多智体系统建模的概率时间自动机中出现的所有时钟变量的集合 C,它对应的一个离散时钟赋值是一个函数 v^d:对每一个时钟变量 $x \in C$,对它的 I_x 赋以集合$\{0, \cdots, c_x\}$中的一个值,对其 F_x 赋以集合$\{0, \cdots, n\}$中一个值,用 $v^d(x)$表示$(v^d(I_x), v^d(F_x))$.

由于一个时钟区域(clock region)是满足同一个时钟约束的时钟赋值的集合,则可知每一个离散时钟赋值对应于一个唯一的时钟区域,反之,每一个时钟区域也对应一个唯一的离散时钟赋值.例如,对时钟变量集合 $C=\{x, y\}$ 且 $c_x=2$, $c_y=1$ 的一个离散时钟赋值 $v^d(x, y)=((0,1),(0,))$,它对应于图 1 中阴影部分所示的时钟区域.

两个时钟赋值 v 和 v' 是等价的条件中有这样一个要求:每对时钟变量的小数部分的次序关系在时钟赋值 v、v'下是相同的.例如,对任意的两个时钟变量 $x, y \in C$,如果在 v 下有 $frac(v(x)) \leqslant frac(v(y))$,则在 v'下必须有 $frac(v'(x)) \leqslant frac(v'(y))$.然而,如果为一个多智体系统建模的概率时间自动机中有 n 个时钟变量,则这些时钟变量的小数部分的次序关系有 $n!$ 种可能,这就对应于 $n!$ 个不同的时钟区域,从而导致概率实时解释系统的状态空间的指数增长.所以,如果将只是某些时钟变量的小数部分次序不同的离散时钟赋值进行合并,能极大的减少时钟区域的数目,从而也就简化了概率实时解释系统的状态空间.

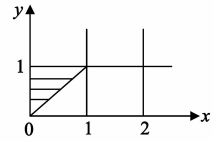

图1 离散时钟赋值((0,1),(0,2))对应的时钟区域

对只是某些时钟变量的小数部分次序不同的离散时钟赋值,我们这样来合并它们.用抽象小数次序变量 F_x^a 来替换小数次序变量 F_x,且令抽象小数次序变量的值域为 $F^a=\{0, \alpha\}$.其中,0 表示小数部分为 0 的时钟变量,α 表示所有其它可能的小数次序值.例如,对离散时钟赋值 $v^d(x, y, z)=((0,3),(1,1),(2,2))$,其对应的抽象离散时钟赋值为 $v^a(x, y, z)=((0, \alpha),(1, \alpha),(2, \alpha))$;对 $v^d(x, y, z)=((1,0),(2,0),(3,0))$,其对应的抽象离散时钟赋值为 $v^a(x, y, z)=((1,0),(2,0),(3,0))$.用 $V^a(C)$表示一个时钟变量集合 C 上的抽象时钟赋值的集合,对任一 $x \in C$,用 $v^a(x)$表示 $v^a(v^d(I_x), v^d(F_x^a))$.

定义 9 (抽象离散时钟赋值)

给定一个时钟变量集合 C,它的一个抽象离散时钟赋值是一函数 v^a:对每一时钟变量 $x \in C$,把集合$\{0, \cdots, c_x\}$中的一个值赋给 I_x,把 F^a 中一个值赋给 F_x^a.

定义 10 (两个具体状态关于智体 i 认知等价: $\sim_i$)

对概率实时解释系统中的两个具体状态(l, v),(l', v'),它们关于智体 $i(1 \leqslant i \leqslant n)$是认知等价的,表示为:$(l, v) \sim_i (l', v')$当且仅当 $l_i(l)=l_i(l')$且 $v \cong v'$.即智体 i 在全局位置 l 中的位置分量与其在全局位置 l'中的位置分量相同,且两个具体状态中的时钟赋值 v 与 v'是等价的.

定义 11 (两个抽象状态关于智体 i 认知等价: $\sim_i'$)

若(l, v),(l', v')是两个抽象状态,我们如下定义它们关于智体 $i(1 \leqslant i \leqslant n)$的认知等价关系:

抽象状态(l, v),(l', v')是关于智体 i 认知等价的,记为$(l, v) \sim_i' (l', v')$,当且仅当对(l, v)中任意一个具体状态 s_1,对(l', v')中任意一个具体状态 s_2,有 s_1

$\sim_i s_2$ 总是成立的,即这两个具体状态 s_1 与 s_2 是关于智体 i 认知等价的.

例如,假设概率实时解释系统中有 3 个智体:智体 1,2,3,即 $Ag=\{1,2,3\}$,有 2 个时钟变量 x,y,即 $C=\{x,y\}$,且 $C_x=C_y=2$. 假设抽象状态 $s=(l,((1,\alpha),(1,\alpha)))$ 中有 3 个具体状态:$s_{11}:((l_1,l_2,l_3),(1.5,1.1))$,$s_{12}:((l_1,l_2,l_3'),(1.5,1.2))$ 以及 $s_{13}:((l_1,l_2,l_3'),(1.5,1.3))$;抽象状态 $s'=(l',((1,\alpha),(1,\alpha)))$ 中有 4 个具体状态:$s_{21}:((l_1,l_2',l_3),(1.8,1.4))$,$s_{22}:((l_1,l_2',l_3),(1.8,1.5))$,$s_{23}:((l_1,l_2',l_3'),(1.8,1.6))$ 和 $s_{24}:((l_1,l'_2,l_3'),(1.8,1.7))$. 则根据上面的定义可知,抽象状态 s 与 s' 是关于智体 1 认知等价的:$s\sim_1' s'$,因为对 s 中任意一个具体状态 $s_{1i}(1\leqslant i\leqslant 3)$,$s'$ 中任意一个具体状态 $s_{2j}(1\leqslant j\leqslant 4)$,均有:$s_{1i}\sim_1 s_{2j}$. 所以,抽象状态 s 与 s' 是关于智体 1 认知等价的:$s\sim_1' s'$.

有了两个抽象状态关于智体 $i(1\leqslant i\leqslant n)$ 认知等价的定义后,我们就可以把符合这样条件的抽象状态进行合并,使它们成为一个抽象状态,即一个等价类,从而可以进一步简化概率实时解释系统的状态空间.

3.2　建立抽象模型

根据上面给出的抽象技术,即抽象离散时钟赋值和两个抽象状态关于智体认知等价,我们现在可以从概率实时解释系统的原始模型 M 演绎出对应的抽象模型 M^A,该抽象模型 M^A 如下定义.

定义 12　(概率实时解释系统的抽象模型)

概率实时解释系统的原始模型 $M=(Q,q_0,P,\sim_1,\cdots,\sim_n,P_1,\cdots,P_n,V)$ 对应的抽象模型 M^A 是一个元组 $M^A=(Q',q_0',P',\sim_1',\cdots,\sim_n',P_1',\cdots,P_n',V')$,其中:

$Q'=L'\times R_C^A$ 表示抽象模型中的状态集,其中 L' 表示抽象全局位置的集合,R_C^A 表示时钟变量集合 C 上的抽象离散时钟赋值的集合;

$q_0'=(l_0',v_0')$ 表示初始抽象状态,对它的一个具体初始状态 $q_0=(\ell_0,v_0)$,有 $l_0\in L_0$,对 $\forall x\in C$,有 $v_0(x)=0$;

$P':Q'\times Q'\to[0,1]$ 是抽象状态之间的转换概率函数,且满足对任意的抽象状态 $\forall q_1,q_2\in Q'$,有 $P'(q_1,q_2)=\min_{s\in q_1}P(s,q_2)=\min_{s\in q_1}\sum_{s_2\in q_2}P(s,s_2)$.

抽象模型中的状态转换关系表示为:$E'\subseteq(L'\times R_C^A)\times(Act\cup R^+)\times(L'\times R_C^A)$,有两种转换:

(1)时间转换:$(\ell,v^a)\xrightarrow{d}(\ell,v^a+d)$,$\forall d>0$,当且仅当 $v^a\models Inv(\ell)$ 且 $v^a+d\models Inv(\ell)(\forall d>0)$;

(2)行为转换:$(\ell,v^a)\xrightarrow{a}(\ell',v_a')(a\in Act)$,当且仅当 $(\exists cc\in CC(C))(\exists D\subseteq C)$,有 $\ell\xrightarrow{cc,a,D}\ell'$,$v^a\models cc$ 且 $v_a'=v^a(D=0)\models Inv(\ell')$. 其中,$v_a'=v^a(D=0)$ 表示在抽象时钟赋值 v^a 中,将时钟变量集合 $D\subseteq C$ 中每个时钟变量 x 的整数部分变量 I_x 和抽象小数次序变量 F_x^a 均置为 0,其余时钟变量的值仍遵循抽象时钟赋值 v^a.

$\sim_i'\subseteq Q'\times Q'(1\leqslant i\leqslant n)$ 是抽象状态之间的认知等价关系,具体参加定义 11.

$P_i':Q'\times Q'\to[0,1](1\leqslant i\leqslant n)$ 是认知关系上抽象转换概率函数,且满足对任意的抽象状态 $\forall q_1,q_2\in Q'$,有 $P_i'(q_1,q_2)=\min_{s\in q_1}P_i(s,q_2)=\min_{s\in q_1}\sum_{s_2\in q_2}P_i(s,s_2)$.

$V':Q'\to 2^{Ap}$ 是一赋值函数,对于一个抽象状态 (ℓ,v),有 $V((\ell,v))=\bigcap_{i=1}^n V_{PTA}(\ell_i)$ (ℓ_i 表示该抽象状态的第 i 个具体状态的全局位置). 即在一个抽象状态上成立的命题变量集合是在它的每个具体状态上成立的命题变量集合的交集.

定义 13　(抽象模型上 PTACTLK 的语义)

$M^A=(Q',q_0',P',\sim_1',\cdots,\sim_n',P_1',\cdots,P_n',V')$ 是概率实时解释系统 M 的一个抽象模型,$M^A,q\models\alpha$ 表示 PTACTLK 公式 α 在抽象模型 M^A 的抽象状态 q 上为真. 在下面的满足性关系中我们省略了符号 M^A. 假设下面的 p,q,ϕ 和 φ 均为 PTACTLK 公式,满足性关系"$\models$"如下归纳定义:

$q\models p$ 当且仅当 $p\in V'(q)$,即 $\forall s\in q$,$p\in V(s)$,其中,$p\in Ap$;

$q\models\neg p$ 当且仅当 $p\notin V'(q)$,即 $\forall s\in q$,$p\notin V(s)$,其中,$p\in Ap$;

$q\models\phi\vee\varphi$,当且仅当 $q\models\phi$ 或 $q\models\varphi$;

$q\models\phi\wedge\varphi$,当且仅当 $q\models\phi$ 且 $q\models\varphi$;

$q\models A(\phi U_I^{\geqslant p}\varphi)$,当且仅当 $\forall\rho'\in f_{PTA}(q)$,$\rho'\models\phi U_I\varphi$,且 $\sum_{\rho'\in f_{PTA}(q)}\mathrm{Prob}(\rho')\geqslant p$;

$q\models A(\phi R_I^{\geqslant p}\varphi)$,当且仅当 $(\forall\rho'\in f_{PTA}(q))$,$\rho'\models\phi R_I\varphi$,且 $\sum_{\rho'\in f_{PTA}(q)}\mathrm{Prob}(\rho')\geqslant p$;

$q\models K_i^{\geqslant p}\varphi$,当且仅当 $\sum_{q'\models\varphi}P_i'(q,q')\geqslant p$;

$q\models E_\Gamma^{\geqslant p}\varphi$,当且仅当 $\sum_{q'\models\varphi}\sum_{i\in\Gamma}P_i'(q,q')\geqslant p$;

$q\models D_\Gamma^{\geqslant p}\varphi$,当且仅当 $\sum_{q'\models\varphi}\prod_{i\in\Gamma}P_i'(q,q')\geqslant p$;

由于 $C_\Gamma^{\geqslant p}\varphi$ 是 $E_\Gamma^{\geqslant p}\varphi$ 的传递闭包,在此我们省略了 $C_\Gamma^{\geqslant p}\varphi$ 在抽象模型上的满足性定义.

3.3　属性保持关系

抽象的目的就是在保持属性的条件下对系统的原始模型进行简化,下面我们证明 PTACTLK 公式的满足性在抽象模型下的保持关系. 即若抽象模型 M^A 满足一个 PTACTLK 公式 ϕ,则可推出原始模型 M 也要满足 ϕ. 也就是说,抽象模型 M^A 是原始模型 M 的上近似.

定理 1 令 $M=(Q,q_0,P,\sim_1,\cdots,\sim_n,P_1,\cdots,P_n,V)$是一个概率实时解释系统,$M^A=(Q',q_0',P',\sim_1',\cdots,\sim_n',P_1',\cdots,P_n',V)$是根据上面的抽象技术演绎得到的 M 的抽象模型,ϕ 是一个 PTACTLK 公式.我们有:若 $M^A,s'\models\phi$,则有 $M,s\models\phi$.

证明 通过对公式 ϕ 的结构进行归纳来证明.对于原子命题,$\neg$ 算子,$\wedge$ 与 $\vee$ 算子,结论显然成立.我们主要考察下面的几种形式.

(1)$\phi=A(\varphi U_I^{\geqslant p}\psi)$

根据定义 13,若 $M^A,s'\models A(\varphi U_I^{\geqslant p}\psi)$,则 $\forall\rho'\in f_{PTA}(s'),\rho'\models\varphi U_I\psi$,且 $\sum_{\rho'\in f_{PTA}(s')}\mathrm{Prob}(\rho')\geqslant p$.而 $\sum_{\rho'\in f_{PTA}(s')}\mathrm{Prob}(\rho')=\sum_{\rho'\in f_{PTA}(s')}\prod_{i\geqslant 0}P(s_i',s_{i+1}')$,且 $s_0'=s'$.由于 $\rho'=s_0's_1'\cdots s_n'\cdots$满足 $\varphi U_I\psi$,则在时间间隔 I 内存在一时刻 r,使时刻 r 在该路径上对应的状态满足 ψ,不妨设该状态是 s_n',则 $s_n'\models\psi$,且该状态之前的所有状态都满足 φ:$s_i'\models\varphi(0\leqslant i<n)$.由对原子命题的归纳假设可得,$\forall s_n\in s_n',s_n\models\psi,\forall s_i\in s_i',s_i\models\varphi(0\leqslant i<n)$,其中 $s_0=s$,且 s_n 是时间间隔 I 中的一个具体状态.从而路径 $s_0s_1\cdots s_n\cdots$满足 $\varphi U_I\psi$,即 $\forall\rho\in f_{PTA}(s),\rho\models\varphi U_I\psi$.于是 $p\leqslant\sum_{\rho'\in f_{PTA}(s')}\prod_{i\geqslant 0}P(s_i',s_{i+1}')\leqslant\sum_{\rho\in f_{PTA}(s)}\prod_{i\geqslant 0}P(s_i,s_{i+1})=\sum_{\rho\in f_{PTA}(s)}\mathrm{Prob}(\rho)$.从而我们可以得出 $M,s\models A(\varphi\bigcup_I^{\geqslant p}\psi)$.

(2)$\phi=A(\varphi R_I^{\geqslant p}\psi)$

根据定义 13,若 $M^A,s'\models A(\varphi R_I^{\geqslant p}\psi)$,则 $\forall\rho'\in f_{PTA}(s'),\rho'\models\varphi R_I\psi$,且 $\sum_{\rho'\in f_{PTA}(s')}\mathrm{Prob}(\rho')\geqslant p$.而 $\sum_{\rho'\in f_{PTA}(s')}\mathrm{Prob}(\rho')=\sum_{\rho'\in f_{PTA}(s')}\prod_{i\geqslant 0}P'(s_i',s_{i+1}')$,其中 $s_0'=s'$,由于 $s_0's_1'\cdots s_n'\cdots$满足 $\varphi R_I\psi$,则可得:(a)对时间间隔 I 内的任一时刻 r,存在小于 r 的时刻 r',使该路径上时刻 r' 对应的状态满足 φ 和 ψ,且所有之前的状态均满足 ψ.不妨设路径上时刻 r' 对应的状态为 s_n',则有 $s_n'\models\varphi\wedge\psi,s_i'\models\psi(0\leqslant i<n)$.或者($b$)对时间间隔 I 内的任一时刻 r,该路径上时刻 r 对应的状态均满足 ψ.不妨设所有这些状态为 $s_i'(0\leqslant i\leqslant n)$,则 $s_i'\models\psi$.

假设(a)成立,由归纳假设可得,$\forall s_n\in s_n',s_n\models\varphi\wedge\psi,\forall s_i\in s_i',s_i\models\psi(0\leqslant i<n)$,(其中 $s_0'=s'$),且 s_n 是时间间隔 I 内的一个状态.从而可知路径 $ss_1\cdots s_n\cdots$满足 $\varphi R_I\psi$,其中 s 是 s' 的任一具体状态.于是我们得到 $\forall\rho\in f_{PTA}(s),\rho\models\varphi R_I\psi$.

假设(b)成立,由归纳假设可得,$\forall s_i\in s_i',s_i\models\psi(0\leqslant i\leqslant n)$,其中 $s_0'=s'$,且 $s_i'(0\leqslant i\leqslant n)$是时间间隔 I 中对应的状态.则路径 $s_0s_1\cdots s_n\cdots$满足 $\varphi R_I\psi$,其中 s 是 s' 的任一具体状态.即 $\forall\rho\in f_{PTA}(s),\rho\models\varphi R_I\psi$.

由以上可得,

$$p\leqslant\sum_{\rho'\in f_{PTA}(s')}\prod_{i\geqslant 0}P'(s_i',s_{i+1}')\leqslant\sum_{\rho\in f_{PTA}(s)}\prod_{i\geqslant 0}P(s_i,s_{i+1})=\sum_{\rho\in f_{PTA}(s)}\mathrm{Prob}(\rho),$$

从而 $M,s\models A(\varphi R_I^{\geqslant p}\psi)$.

(3)$\phi=K_i^{\geqslant p}\varphi$

根据定义 13,若 $M^A,s'\models K_i^{\geqslant p}\varphi,\sum_{s'\models\varphi}P_i'(s',s'')\geqslant p$.而

$$\sum_{s''\models\varphi}P_i'(s',s'')=\sum_{s''\models\varphi}\min_{s_1\in s'}P_i(s_1,s'')=\sum_{s''\models\varphi}\min_{s_1\in s'}\sum_{s_2\in s''}P_i(s_1,s_2)\leqslant\sum_{s''\models\varphi}\sum_{s_2\in s''}P_i(s,s_2),$$

其中 s 是 s' 的任意一个具体状态.由归纳假设可得,$\forall s_2\in s'',s_2\models\varphi$.于是有

$$p\leqslant\sum_{s'\models\varphi}\sum_{s_2\in s''}P_i(s,s_2)\leqslant\sum_{s_2\models\varphi}P_i(s,s_2),$$

其中s 是 s'的任一具体状态.即$\forall s\in s',\sum_{s_2\models\varphi}P_i(s,s_2)\geqslant p$.从而有 $M,s\models K_i^{\geqslant p}\varphi$ 成立.

(4)$\phi=E_I^{\geqslant p}\varphi$

根据定义 13,若 $M^A,s'\models E_I^{\geqslant p}\varphi$,则 $\sum_{s'\models\varphi}\sum_{i\in I}P_i'(s',s'')\geqslant p$.而

$$\sum_{s'\models\varphi}\sum_{i\in I}P_i'(s',s'')=\sum_{s'\models\varphi}\sum_{i\in I}\min_{s_1\in s'}P_i(s_1,s'')=\sum_{s'\models\varphi}\sum_{i\in I}\min_{s_1\in s'}\sum_{s_2\in s''}P_i(s_1,s_2)\leqslant\sum_{s'\models\varphi}\sum_{i\in I}\sum_{s_2\in s''}P_i(s,s_2),$$

其中 s 是 s' 的任意一个具体状态.由归纳假设可得,$\forall s_2\in s'',s_2\models\varphi$.于是 $p\leqslant\sum_{s'\models\varphi}\sum_{i\in I}\sum_{s_2\in s''}P_i(s,s_2)\leqslant\sum_{s_2\models\varphi}\sum_{i\in I}P_i(s,s_2)$,其中 s 是 s' 的任一具体状态.从而可得,$\forall s\in s',\sum_{s_2\models\varphi}\sum_{i\in I}P_i(s,s_2)\geqslant p$,即 $M,s\models E_I^{\geqslant p}\varphi$.

(5)$\phi=D_I^{\geqslant p}\varphi$

根据定义 13,若 $M^A,s'\models D_I^{\geqslant p}\varphi$,则 $\sum_{s'\models\varphi}\prod_{i\in I}P_i'(s',s'')\geqslant p$.而 $\sum_{s'\models\varphi}\prod_{i\in I}P_i'(s',s'')=\sum_{s'\models\varphi}\prod_{i\in I}\min_{s_1\in s'}\sum_{s_2\in s''}P_i(s_1,s_2)\leqslant\sum_{s'\models\varphi}\prod_{i\in I}\sum_{s_2\in s''}P_i(s,s_2)$,其中 s 是 s' 的任一具体状态.由归纳假设可得,$\forall s_2\in s'',s_2\models\varphi$.于是,$p\leqslant\sum_{s'\models\varphi}\prod_{i\in I}\sum_{s_2\in s''}P_i(s,s_2)\leqslant\sum_{s_2\models\varphi}\prod_{i\in I}P_i(s,s_2)$,其中 s 是 s' 的任一具体状态.即$\forall s\in s',\sum_{s_2\models\varphi}\prod_{i\in I}P_i(s,s_2)\geqslant p$.从而有 $M,s\models D_I^{\geqslant p}\varphi$.

由于 $C_I^{\geqslant p}\varphi$ 是 $E_I^{\geqslant p}\varphi$ 的传递闭包,在此我们省略了对 $C_I^{\geqslant p}\varphi$ 的证明.

4 实例分析

这里我们给出一个简单的通信协议,通过对该协议的状态空间的简化来说明我们抽象技术的有效性.

4.1 一个简单的通信协议

在我们的通信协议中,存在两个智体:发送器(sender)和接收器(receiver),它们通过一条通信信道相连接.发送器负责从环境中收集数据并将其通过信道发送给接收器;接收器接收来自发送器的数据.发送器和接收器对应的概率时间自动机分别如图 2、3 所示.这里我们假设信道是可靠的,即数据在传输过程中不会丢失.协议具体描述如下.

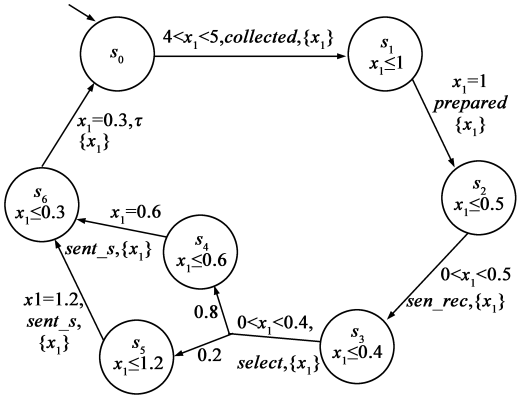

图2　概率时间自动机 Sender

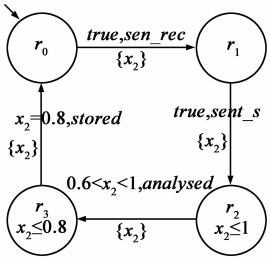

图3　概率时间自动机 Receiver

智体发送器有一个时钟变量 x_1,用于标识其在各个位置(location)上停留的时间.在初始位置 s_0 上,x_1 的值为 0.当发送器收集 4 ~ 5s 的数据后,到达位置 s_1,行为 collected 表示发送器完成收集数据的工作.为了将收集的数据发送给接收器,发送器用 1s 的时间准备通信,然后到达位置 s_2,行为 prepared 表示准备通信的工作完成.在 s_2 上,发送器在 0.5s 内向接收器发送同步信号 sen_rec,然后到达位置 s_3.假设发送器向接收器发送数据时需用两个特殊的发送端口:端口 1、端口 2,每个端口都与信道相连接,但每次发送数据时,发送器只能随机的选择使用一个端口.选择端口 1 的概率为 0.8,选择端口 2 的概率为 0.2.若选择的是端口 1,需要等待 0.6s 的时间,然后将数据通过端口 1 发送出去;若选择的是端口 2,则需要等待 1.2s.在 s_3 时,发送器在 0.4s 内随机选择一个端口,若选的是端口 1,则到达位置 s_4,否则到达位置 s_5.不论发送器选择用哪个端口发送数据,发送完后都会到达位置 s_6.在 s_6 上等待 0.3s 后返回初始位置.

智体接收器有一个时钟变量 x_2,初始位置是 r_0.当它收到来自发送器的同步信号 sen_rec 后会从初始位置到达位置 r_1.当接收完发送器的数据后从位置 r_1 到达 r_2.然后接收器用 0.6 ~ 1s 的时间对收到的数据进行分析处理,而后到达位置 r_3,行为 analysed 表示接收器已完成分析数据的工作.再用 0.8s 的时间将处理完的数据存储起来,行为 stored 表示接收器完成了存储数据的工作,最后返回初始位置 r_0.

在两个概率时间自动机中,除了在边上标出的转换关系的概率外,其余的转换概率均为 1.

在我们的通信协议中,一个具体状态应形如$((i,j),(v_{x_1},v_{x_2}))$,$(0\leqslant i\leqslant 6, 0\leqslant j\leqslant 3)$.其中$(i,j)$是该状态的全局位置,它的两个分量 i,j 表示智体 Sender、Receiver 所在的位置分量分别是 s_i,r_j;(v_{x_1},v_{x_2})是对协议中时钟变量集合 $C=\{x_1,x_2\}$ 的一个赋值,表示在该状态下时钟变量 x_1,x_2 的值分别是 v_{x_1},v_{x_2}.由于在该协议中时钟变量 x_1,x_2 的取值范围分别是 $0\leqslant v_{x_1}\leqslant 5, 0\leqslant x_2\leqslant 1$,且均为实数,这就使该协议中有无数个具体状态,即该协议的状态空间是无限的.

4.2 构造通信协议的抽象模型

为了将通信协议的无限状态空间简化成有限形式,我们利用第三节给出的抽象技术构造协议的抽象模型.对协议中每个具体状态$((i,j),(v_{x_1},v_{x_2}))$的时钟赋值$(v_{x_1},v_{x_2})$,用对应的抽象离散时钟赋值来表示,这样就可以把全局位置相同且时钟赋值对应同一抽象离散时钟赋值的所有具体状态合并成一个抽象状态.从而极大的简化通信协议的状态空间,得到状态空间的有限形式.在得到的有限状态空间中,再利用两个抽象状态关于智体 Sender(或 Receiver)认知等价的定义,将

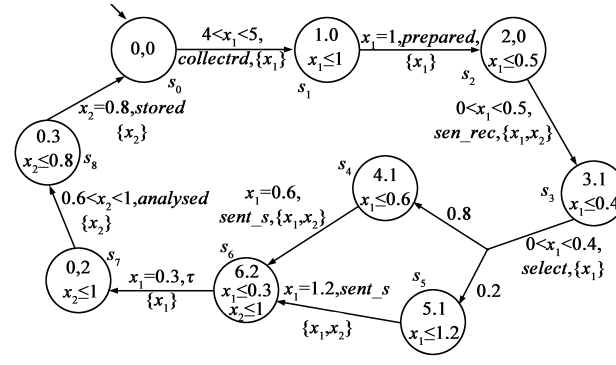

图4　通信协议的抽象模型

所有认知等价的抽象状态合并,进一步简化状态空间.最后,就得到通信协议的抽象模型.图 4 给出了利用抽象技术得到的通信协议的抽象模型,该抽象模型给出了所有可到达的抽象状态.

从得到的抽象模型中可以看出,我们的抽象技术把通信协议的无限状态空间简化成只包含 9 个抽象状态的有限形式.

抽象模型 M^A 的状态空间 Q' 中的每个状态及该状态上的位置不变条件如下所示:

$S_0:((0,0),((0,0),(0,0))),Inv(0,0)=\text{true};$

$S_1:((1,0),((0,0),(4,\alpha))),Inv(1,0)=x_1\leqslant 1;$

$S_2:((2,0),((0,0),(5,\alpha))),Inv(2,0)=x_1\leqslant 0.5;$

$S_3:((3,1),((0,0),(0,0))),Inv(3,1)=x_1\leqslant 0.4;$

$S_4:((4,1),((0,0),(0,\alpha))),Inv(4,1)=x_1\leqslant 0.6;$

$S_5:((5,1),((0,0),(0,\alpha))),Inv(5,1)=x_1\leqslant 1.2;$

$S_6:((6,2),((0,0),(0,0))),Inv(6,2)=x_1\leqslant 0.3\wedge x_2\leqslant 1;$

$S_7:((0,2),((0,0),(0,\alpha))),Inv(0,2)=x_2\leqslant 1;$

$S_8:((0,3),((0,\alpha),(0,0))),Inv(0,3)=x_2\leqslant 0.8.$

从而,在得到的通信协议的抽象模型 $M^A=(Q',q_0',P',\sim_1',\cdots,\sim_n',P_1',\cdots,P_n',V')$ 中,有

系统抽象状态空间:$Q'=\{S_0,S_1,S_2,S_3,S_4,S_5,S_6,S_7,S_8\}$;

初始抽象状态:$q_0'=S_0$;

状态转换概率:$P'(S_3,S_4)=0.8$,$P'(S_3,S_5)=0.2$.即从抽象状态 S_3 到 S_4 的转换概率为 0.8,从 S_3 到 S_5 的概率为 0.2.抽象模型中其余相邻状态之间的转换概率均为 1.

每个抽象状态和自己是关于智体 Sender 认知等价的,即对任一状态 $S_i\in Q'(0\leqslant i\leqslant 8)$,有 $S_i\sim'_{\text{Sender}}S_i$ 成立,同理这对于智体 Receiver 也是成立的.

4.3 模型检测通信协议

我们要验证的属性是:在通信协议中,智体发送器认为这样一个行为成立的概率大于等于 0.6,该行为中在发送器向接收器发送了一个同步信号 sen_rec 后,智体接收器会在 0.5~1s 内收到来自发送器的数据.该属性可用 PTACTLK 公式表示为:$\phi=K^{\geqslant 0.6}_{\text{Sender}}(sen\_rec\wedge AF_{(0.5,1)}receive)$,*receive* 表示接收器收到了来自发送器的数据.

在得到的抽象模型 M^A 中,由于发送器向接收器发送了同步信号后到达全局状态 S_3,接收器收到数据后到达全局状态 S_6,则只需看状态 S_3 和 S_6 之间的时间间隔是否在 0.5~1s 之间,且此时两个状态之间的转换概率是否大于等于 0.6.如果这两个条件均成立,则可判断属性 ϕ 是成立的.

在上面的抽象模型中,状态 S_3 到 S_6 有两条路径:一条是 S_3 经过 S_4 到达 S_6,即 $S_3\rightarrow S_4\rightarrow S_6$;另一条是 S_3 经过 S_5 到达 S_6,即 $S_3\rightarrow S_5\rightarrow S_6$.首先考察路径 $S_3\rightarrow S_4\rightarrow S_6$.状态 S_3 到 S_4 的时间间隔是(0,0.4),S_4 到 S_6 的时间间隔是 0.6,从而可推出在这条路径上状态 S_3 到达 S_6 的时间间隔是(0.6,1).又由于状态 S_3 到 S_4 的转换概率是 0.8,S_4 到 S_6 的概率是 1,则可得出由该路径从状态 S_3 到达 S_6 的转换概率是 $0.8\times 1=0.8$;再考察路径 $S_3\rightarrow S_5\rightarrow S_6$.状态 S_3 到 S_5 的时间间隔是(0,0.4),S_5 到 S_6 的时间间隔是 1.2,从而可推出此路径上状态 S_3 到 S_6 的时间间隔是(1.2,1.6).由于状态 S_3 到 S_5 的转换概率是 0.2,S_5 到 S_6 的概率是 1,则可得出从状态 S_3 经过 S_5 到达 S_6 的转换概率是 $0.2\times 1=0.2$.

由于第一条路径上状态 S_3 到达 S_6 的时间间隔(0.6,1)包含在间隔(0.5,1)中,且从状态 S_3 到达 S_6 的转换概率是 0.8.即发送器向接收器发送了同步信号后,接收器在 0.6~1s 内收到数据的概率为 0.8.从而可得出,属性 ϕ 在抽象模型 M^A 中是成立的:$M^A\models\phi$.

由于在 3.3 节中已经证明了利用抽象技术演绎得到的抽象模型 M^A 是原始模型 M 的上近似,从而可以得出我们的通信协议是满足该属性的,即 $M\models\phi$.我们的抽象技术将系统规模从原始系统的无限多个状态降低到了抽象模型中的 9 个状态,由此可见我们的抽象技术是有效的.

5 结论与展望

为了缓解概率实时时态认知逻辑 PTACTLK 模型检测中的状态空间爆炸问题,我们给出了一种抽象技术:用抽象离散时钟赋值可将概率实时解释系统的无限状态空间简化成有限形式;用两个抽象状态关于智体认知等价可演绎出相应的等价关系,利用等价关系对抽象状态进行合并,从而进一步简化概率实时解释系统的状态空间.定义了概率实时解释系统的抽象模型,给出了抽象模型上概率实时时态认知逻辑的语义,并证明了利用抽象技术演绎得到的抽象模型是原始模型的上近似.最后,通过对一个简单的通信协议的状态空间的简化,说明了我们的抽象技术是有效的.

利用抽象技术演绎得到的抽象模型只是原始模型的上近似,如果抽象模型不满足待验证的属性,不能推导出原始模型也不满足该属性.因此,在抽象技术中引入除真和假之外表示不确定性的第三值是进一步研究的一个方向.

参考文献

[1] 林惠民,张文辉.模型检测:理论、方法与应用[J].电子学报,2002,30(12A):1907-1912.

Lin Huimin, Zhang Wenhui. Model checking: theories, techniques and applications[J]. Acta Electronica Sinica, 2002, 30(12A): 9 – 14. (in Chinese)

[2] 万长林,韩旭,牛温佳,王文杰,史忠植.基于动态描述逻辑的服务组合及质量模型[J].电子学报,2010,38(8):1923 – 1928.
Wan Changlin, Han Xu, Niu Wenjia, Wang Wenjie, Shi Zhongzhi. Dynamic description logic based web service composition and QoS model[J]. Acta Electronica Sinica, 2010, 38(8): 1923 – 1928. (in Chinese)

[3] A Lomuscio, W Penczek, B Wozna. Bounded model checking for knowledge and real time[J]. presented at Artif Intell, 2007. 1011 – 1038.

[4] Cormac Flanagan, Patrice Godefroid. Dynamic partial-order reduction for model checking software[A]. Proceedings of the 32nd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages[C]. NY, USA: ACM, Volume 40 Issue 1, January 2005. 110 – 121.

[5] A Prasad Sistla, Patrice Godefroid. Symmetry and reduced symmetry in model checking[J]. ACM Transactions on Programming Languages and Systems, 2004, 26(4): 702 – 734.

[6] Conghua Zhou, Bo Sun, Zhifeng Liu. Abstraction for model checking multi-agent systems[J]. Frontiers Of Computer Science in China, 2010, 5(1): 14 – 25.

[7] Edmund M Clarke, Orna Grumberg, David E Long. Model checking and abstraction[J]. ACM Transactions on Programming Languages and Systems, 1992, 16(5): 1512 – 1542.

[8] Biere A, Cimatti A, Clarke EM, Zhu Y. Symbolic model checking without BDDs[J]. Lecture Notes in Computer Science, 1999, 1579: 193 – 207.

[9] 杨晋吉,苏开乐,骆翔宇,林瀚,肖茵茵.有界模型检测的优化[J].软件学报,2009,20(8):2005 – 2014.
Yang JinJi, Su KaiLe, Luo Xiangyu, Lin Han, Xiao Yinyin. Optimization of bounded model checking[J]. Journal of Software, 2009, 20(8): 2005 – 2014. (in Chinese)

[10] 骆翔宇,苏开乐,杨晋吉.有界模型检测同步多智体系统的时态认知逻辑[J].软件学报,2006,17(12):2585 – 2498.
Luo Xiangyu, Su Kaile, Yang Jinji. Bounded model checking for temporal epistemic logic in synchronous multi-agent systems[J]. Journal of Software, 2006, 17(12): 2485 – 2498. (in Chinese)

[11] 周从华,孙博,刘志锋,葛云.概率时态认知逻辑模型检测中三值抽象技术的研究[J].电子学报,2012,40(10):2052 – 2061.
Zhou Conghua, Sun Bo, Liu Zhi-feng, Ge Yun. Three-valued abstraction for model checking the probabilistic temporal logic of knowledge[J]. Acta Electronica Sinica, 2012, 40(10): 2052 – 2061. (in Chinese)

[12] Orna Grumberg. Abstraction and refinement in model checking[J]. Lecture Notes in Computer Science, 2006, 4111: 219 – 242.

[13] Edmund M Clarke, Flavio Lerda, Muralidhar Talupur. An abstraction technique for real-time verification[J]. Next Generation Design and Verification Methodologies for Distributed Embedded Control Systems, 2007. 1 – 17.

[14] Sascha Konrad, Betty H C Cheng. Real-time specification patterns[A]. Proceedings of the 27th International Conference on Software Engineering[C]. USA: IEEE, 2005. 372 – 381.

[15] Carlos Areces, Guillaume Hoffmann, Alexandre Denis. Modal logics with counting[J]. Lecture Notes in Computer Science, 2010, 6188: 98 – 109.

[16] Christel Baier, Joost- Pieter Katoen. Principles of Model Checking[M]. USA: The MIT Press, 2008.

[17] M Kwiatkowska, G Norman, R Segala, J Sproston. Automatic verification of real-time systems with discrete probability distributions[J]. Theoretical Computer Science, 2002, 282: 101 – 150.

[18] Johan Bengtsson, Wang Yi. Timed automata: semantics, algorithms and tools[J]. Lecture Notes in Computer Science, 2004, 3098: 87 – 124.

[19] R Alur, D Dill. A theory of timed automata[J]. Theoret Comput Sci, 1994, 126: 183 – 235.

作者简介

刘志锋　男,1981 年生,江苏无锡人.2011 年在南京大学获得博士学位,现为江苏大学计算机科学与通信工程学院讲师.主要研究方向为模型检测,形式化方法,模态逻辑.
E-mail: liuzf@ujs.edu.cn