基于可能性测度的计算树逻辑 CTL* 与可能性互模拟

邓 辉 薛 艳 李亚利 李永明

(陕西师范大学计算机科学学院 西安 710062)

摘 要 提出了基于可能性测度的计算树逻辑 CTL*(PoCTL*)的概念。给出了在可能的 Kripke 结构中可能性互模拟的定义并对其性质进行了详细的探讨。对商可能性 Kripke 结构及其相关构造进行了特别的研究。

关键词 可能的 Kripke 结构,可能性测度,可能性计算树逻辑 PoCTL*,可能性互模拟,商可能性 Kripke 结构

中图法分类号 TP301.2 **文献标识码** A

Computation Tree Logic CTL* Based on Possibility Measure and Possibilistic Bisimulation

DENG Hui XUE Yan LI Ya-li LI Yong-ming

(School of Computer Science, Shaanxi Normal University, Xi'an 710062, China)

Abstract The notion of computation tree logic CTL* based on possibility measure(PoCTL* in short) was proposed in this paper. Then the possibilistic bisimulation in possibilistic Kripke structure was defined and its properties were discussed. Finally, the quotient possibilistic Kripke structure and the related construction were studied particularly.

Keywords Possibilistic Kripke structure, Possibility measure, Possibilistic computation tree logic PoCTL*, Possibilistic bisimulation, Quotient possibilistic Kripke structure

1 引言

模型检测[1]作为一种形式化的技术和工具,在近20年日趋成熟,特别是在硬件和软件系统中有着广泛的应用。经典的模型检测要求系统模型及性质必须是精确无异义的,而现实系统及其性质描述往往具有不确定性,这既包括概率不确定性,也包括模糊不确定性。2008年 Baier 和 Katoen[1]以有穷的马尔可夫链(Markov Chain)为概率系统的模型,系统地介绍了基于概率测度的模型检测的原理和方法,使得模型检测技术在理论和应用上得到了极大的丰富。1965年美国控制论学者 Zadeh[2]提出了模糊集的概念,标志着一门新学科的诞生,而模糊数学最重要的应用领域之一就是计算机智能。如今在计算机科学与工程的各个领域中,模糊数学都发挥着非常重要的作用。

本文将模糊理论与模型检测理论相结合,用可能性测度[4]结合经典模型检测中的计算树逻辑 CTL* 建立基于可能性测度的计算树逻辑 PoCTL*。因为 LTL 和 CTL 是 CTL* 的子集,与经典的模型检测理论相似,所以 PoLTL 和 PoCTL[3]也作为 PoCTL* 的子集。

在经典模型检测理论中当状态数以指数的形式增加时,会发生状态爆炸[1],而互模拟是其中一种抑制状态爆炸的方法,因此为了解决模糊测度下的状态爆炸问题,模糊测度下互模拟的研究就显得十分重要。本文是这个方面的一个尝试。将通过一些定义、证明和实例说明在模糊测度下互模拟的概念及相关的性质。

2 预备知识

定义 1[3] 一个可能的 Kripke 结构是一个5元组 $M=(S,P,I,AP,L)$,其中

(1) S 是一个可数非空的状态集合;

(2) $P:S\times S\to[0,1]$ 是可能性转移函数,对于每个状态 s 满足 $\bigvee_{s'\in S}P(s,s')=1$;

(3) $I:S\to[0,1]$ 是可能性初始分布,并使得 $\bigvee_{s\in S}I(s)=1$;

(4) AP 是一组原子命题集合;

(5) $L:S\to 2^{AP}$ 是标记函数。

注1:若 $X\subseteq[0,1]$,用"$\vee X$"和"$\wedge X$"分别表示集合 X 的最小上界和最大下界。所有满足 $I(s)>0$ 的状态 s 被定义为初始状态。对于状态 $s\in S$ 和 $T\subseteq S$,$P(s,T)$ 表示从状态 s 出发经过一步转移到达 T 中的某些状态 t 的可能性,即 $P(s,T)=\bigvee_{t\in T}P(s,t)$。如果 S 和 AP 是有穷的,则称 M 是有穷的。

对于可能的 Kripke 结构 M,用有穷状态序列 $\overset{\wedge}{\pi}=s_0s_1\cdots s_n$,$(n\in N)$ 表示 M 中的有穷路径,用无穷状态序列 $\pi=s_0s_1s_2\cdots\in S^\omega$ 表示 M 中的无穷路径,其中对于所有的 $i\in N$,都满足 $P(s_i,s_{i+1})>0$。$Paths(M)$ 表示 M 中所有无穷路径的集合,$Paths_{fin}(M)$ 表示 M 中所有有穷路径的集合;$Paths(s)$ 表示 M 中从状态 s 出发的无穷路径的集合。$Paths_{fin}(s)$ 表示 M 中从状态 s 出发的有穷路径的集合。s 的后继表示为 $Post(s)=\{s'\in S|P(s,s')>0\}$,$s$ 的前驱表示为 $Pre(s)=\{s'\in S|P(s',s)>0\}$。

到稿日期:2012-01-08 返修日期:2012-03-07 本文受国家自然科学基金(60873119),中央高校基本科研费(GK201001003)资助。

邓 辉(1982—),男,硕士生,主要研究方向为模型检测,E-mail:marsdenghui@163.com.cn;薛 艳(1986—),女,硕士生,主要研究方向为模型检测;李亚利(1986—),女,硕士生,主要研究方向为模型检测;李永明(1966—),男,博士,教授,博士生导师,主要研究方向为计算智能、模糊系统分析、量子逻辑、量子计算、模型检测。

定义 2[4] 设 M 是可能的 Kripke 结构，$Paths(M)=\bigcup_{s\in S}Paths(s)$，定义映射 $Po:Paths(M)\to[0,1]$：对任意的 $\pi\in Paths(M)$，$\pi=s_0s_1\cdots$，$Po(\pi)=I(s_0)\wedge\bigwedge_{i=1}^{\infty}P(s_i,s_{i+1})$，而对 $A\subseteq Paths(M)$，若定义 $Po(A)=\vee\{Po(\pi)\mid\pi\in A\}$，可得扩张映射 $Po:2^{Paths(M)}\to[0,1]$，则称映射 Po 为 $\Omega=2^{Paths(M)}$ 上的可能性测度。

定理 1[3] 可能性测度 Po 满足如下性质：

(1) $Po(\varnothing)=0$，$Po(Paths(M))=1$；

(2) 如果 $A_i\in\Omega$，$i\in I$，则 $Po(\bigcup_{i\in I}A_i)=\bigvee_{i\in I}Po(A_i)$；

(3) 如果 $A\subseteq B$，$A,B\in\Omega$，则 $Po(A)\leqslant Po(B)$；

但一般地，下列性质未必成立：

(4) 如果 $A_1\supseteq A_2\supseteq\cdots$ 为下降列，则

$Po(\bigcap_{i\in I}A_i)=\bigwedge_{i\in I}Po(A_i)$。

定义 3[1] 设 M_1，M_2 是两个在原子命题 AP 上的 Kripke 结构。(M_1，M_2) 的互模拟是一个二元关系 $R\subseteq S_1\times S_2$，并且满足以下条件：

(A) $\forall s_1\in I_1(\exists s_2\in I_2,(s_1,s_2)\in R)$ 并且 $\forall s_2\in I_2(\exists s_1\in I_1,(s_1,s_2)\in R)$。

(B) 所有的状态 $(s_1,s_2)\in R$ 满足：

(1) $L_1(s_1)=L_2(s_2)$；

(2) 如果 $s_1'\in post(s_1)$，那么存在 $s_2'\in post(s_2)$ 并且 $(s_1',s_2')\in R$；

(3) 如果 $s_2'\in post(s_2)$，那么存在 $s_1'\in post(s_1)$ 并且 $(s_1',s_2')\in R$。

如果在 M_1 和 M_2 上存在上述关系 R，则称 M_1 和 M_2 互模拟等价(或互模拟)，记作 $M_1\sim M_2$。

定义 4[1] 对于 Kripke 结构 M 和互模拟关系 $\sim_M$，转移系统的商 $M/\sim_M$ 定义如下：

$M/\sim_M=(S/\sim_M,I',R',AP,L')$，其中，$I'=\{[s]\sim\mid s\in I\}$，$R'\subseteq[s]\sim\times[s]\sim$，$L'([s]\sim)=L(s)$。

3 基于可能性测度的计算树逻辑 PoCTL*

基于上述基本概念，本节重点讨论基于可能性测度的计算树逻辑 PoCTL* 的相关定义。经典 CTL* 的相关概念可参见文献[1]。

定义 5(基于可能性测度的计算树逻辑 PoCTL* 的语构定义)

PoCTL* 的状态公式：

$\Phi::=\text{true}\mid a\mid\Phi_1\wedge\Phi_2\mid\neg\Phi\mid Po_J(\varphi)$

式中，$a\in AP$，φ 是路径公式并且 $J\subseteq[0,1]$。

PoCTL* 的路径公式：

$\varphi::=\Phi\mid\varphi_1\wedge\varphi_2\mid\neg\varphi\mid O\varphi\mid\varphi_1\cup\varphi_2$

式中，Φ 是状态公式。

布尔操作符以及时序操作符和 CTL* 一样适用 PoCTL*。为了方便在 PoCTL* 的路径公式中略去有界可达形式，采用另外一种形式去定义它，即 $\varphi_1U^{\leqslant n}\varphi_2=\bigvee_{0\leqslant i\leqslant n}\psi_i$，其中 $\psi_0=\varphi_2$ 并且 $\psi_{i+1}=\varphi_1\wedge O\psi_i$，$i\geqslant0$。因此，PoCTL 可以看作是 PoCTL* 的子逻辑。

定义 6 设 $\pi=s_0s_1s_2\cdots$ 是可能的 Kripke 结构 M 中以 s_0 为起点的路径，$\pi[i]=s_is_{i+1}s_{i+2}\cdots$ 表示以 s_i 为起点的路径，状态 $s\in S$，$a\in AP$ 是一个原子命题，Φ,Ψ 是 PoCTL* 的状态公式，并且 φ,φ_1 和 φ_2 是 PoCTL* 的路径公式。满足关系“$\mid=$”定义如下：

(1) $s\mid=a$ 当且仅当 $a\in L(s)$；

(2) $s\mid=\neg\Phi$ 当且仅当 $s\mid\neq\Phi$；

(3) $s\mid=\Phi\wedge\Psi$ 当且仅当 $(s\mid=\Phi)$ 并且 $(s\mid=\Psi)$；

(4) $s\mid=Po_J(\phi)$ 当且仅当 $Po(s=\phi)\in J$。

对于路径 π，满足关系“$\mid=$”定义如下：

(1) $\pi\mid=\Phi$ 当且仅当 $s_0\mid=\Phi$；

(2) $\pi\mid=\varphi_1\wedge\varphi_2$ 当且仅当 $\pi\mid=\varphi_1$ 并且 $\pi\mid=\varphi_2$；

(3) $\pi\mid=\neg\varphi$ 当且仅当 $\pi\mid\neq\varphi$；

(4) $\pi\mid=O\varphi$ 当且仅当 $\pi[1\cdots]\mid=\varphi$；

(5) $\pi\mid=\varphi_1U\varphi_2$ 当且仅当 $\exists j\geqslant0,(\pi[1\cdots]\mid=\varphi_2\wedge(\forall0\leqslant k\leqslant j,\pi[k\cdots]\mid=\varphi_1))$。

4 可能性互模拟

定义 7 设 $M=(S,P,I,AP,L)$ 是一个可能的 Kripke 结构，M 的可能性互模拟是 S 上的一个等价关系 R，那么对于所有的状态 $(s_1,s_2)\in R$，它满足以下条件：

1. $L_1(s_1)=L_2(s_2)$；

2. $Po(s_1,T)=Po(s_2,T)$，$T\in S/R$。

如果 M 中存在 $(s_1,s_2)\in R$ 这样的等价关系 R，那么称状态 s_1 和 s_2 是可能性互模拟等价的(或可能性互模拟)，记作 $s_1\sim_Ps_2$。

第一个条件指的是两个状态的标签函数要一样，第二个条件要求这两个状态转移到除去自己直接到达其他所有状态的可能性要相等，其中 $Po(s,T)=\bigvee_{t\in T}Po(s,t)$ 表示从状态 s 直接到 T 中的状态的可能性。

例 1 如图 1 所示，$L_1(s_1)=L_2(s_2)=\{a\}$，$Po(s_1,T)=Po(s_1,s_3)=0.6$，根据可能性互模拟的定义 $Po(s_2,T)=\bigvee_{t\in T}Po(s_2,t)=Po(s_2,s_4)\vee Po(s_2,s_5)=0.5\vee0.6=0.6$，可得 $Po(s_1,T)=Po(s_2,T)$。可知状态 s_1 和 s_2 满足可能性互模拟的两个条件。那么存在 $(s_1,s_2)\in R$，状态 s_1 和 s_2 是可能性互模拟等价的(或可能性互模拟)，$s_1\sim_Ps_2$。

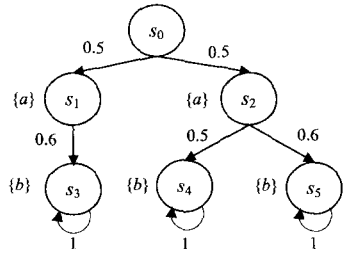

图 1 六状态的可能的 Kripke 结构

在概率模型检测中概率互模拟可以推广到两个马尔科夫链上，与概率互模拟相似，可能性互模拟也可以推广到两个可能的 Kripke 结构上。

定义 8 设 $M_i=(S_i,P_i,I_i,AP,L_i)(i=1,2)$ 是一组在原子命题 AP 上的可能的 Kripke 结构，(M_1，M_2) 的可能性互模拟是一个二元关系 $R\subseteq S_1\times S_2$，它满足以下条件：

1. $L_1(s_1)=L_2(s_2)$；

2. $Po_1(s_1,T)=Po_2(s_2,T)$，$T\in S/R$。

如果存在上述关系 R，那么 (M_1，M_2) 是可能性互模拟等

价的(或可能性互模拟),记作 $M_1 \sim_P M_2$。

假设 M_1, M_2 是两个拥有相同原子命题集合和各自的初始分布 I^1_{init} 和 I^2_{init} 的可能的 Kripke 结构,把这两个可能的 Kripke 结构 M_1, M_2 结合起来可以构造一个新的可能的 Kripke 结构 $M=M_1 \cup M_2$。如果对于 $M=M_1 \cup M_2$ 中每一个等价类 T,$I^1_{init}(T)=I^2_{init}(T)$,那么 M_1 和 M_2 是可能性互模拟的,其中 $I_{init}(T)=\bigvee_{t\in T} I_{init}(t)$。

例 2　可能性互模拟的合并及简化。

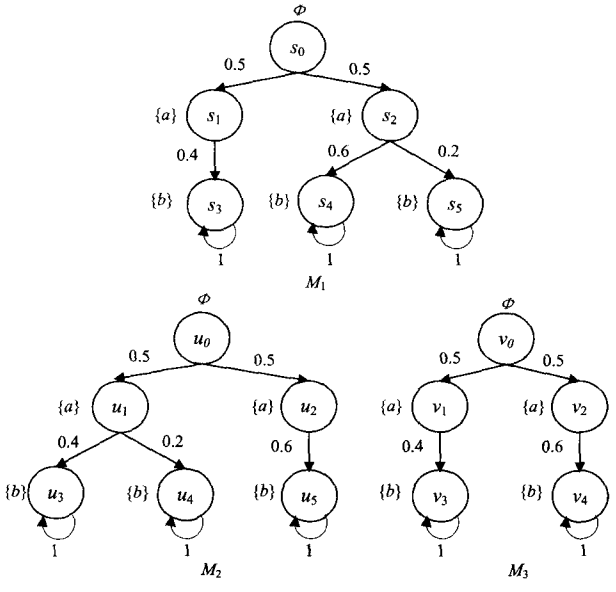

图 2　3 个可能的 Kripke 结构

如图 2 所示,有 3 个可能的 Kripke 结构 M_1, M_2 和 M_3,根据可能性互模拟的定义,可以看出:

$L(s_0)=L(u_0)=L(v_0)=\phi$

$L(s_1)=L(u_1)=L(v_1)=\{a\}$

$L(s_2)=L(u_2)=L(v_2)=\{a\}$

$L(s_3)=L(u_3)=L(u_4)=L(v_3)=\{b\}$

$L(s_4)=L(s_5)=L(u_5)=L(v_4)=\{b\}$

满足可能性互模拟定义的条件 1,其次有:

$$Po(s_0,T)=\bigcup_{t\in T} Po(s_0,t)=Po(s_0,s_1)\cup Po(s_0,s_2)=0.5\cup 0.5=0.5$$

$$Po(u_0,T)=\bigcup_{t\in T} Po(u_0,t)=Po(u_0,u_1)\cup Po(u_0,u_2)=0.5\cup 0.5=0.5$$

$$Po(v_0,T)=\bigcup_{t\in T} Po(v_0,t)=Po(v_0,v_1)\cup Po(v_0,v_2)=0.5\cup 0.5=0.5$$

$$Po(s_1,T)=\bigcup_{t\in T} Po(s_1,t)=Po(s_1,s_3)=0.4$$

$$Po(s_2,T)=\bigcup_{t\in T} Po(s_2,t)=Po(s_2,s_4)\cup Po(s_2,s_5)=0.5\cup 0.6=0.6$$

$$Po(u_1,T)=\bigcup_{t\in T} Po(u_1,t)=Po(u_1,u_3)\cup Po(u_1,u_4)=0.4\cup 0.2=0.4$$

$$Po(u_2,T)=\bigcup_{t\in T} Po(u_2,t)=Po(u_2,u_5)=0.6$$

$$Po(v_1,T)=\bigcup_{t\in T} Po(v_1,t)=Po(v_1,v_3)=0.4$$

$$Po(v_2,T)=\bigcup_{t\in T} Po(v_2,t)=Po(v_2,v_4)=0.6$$

式中,s_3、s_4、s_5、u_3、u_4、u_5 和 v_3、v_4 是终结状态,由上述可得:

$Po(s_0,T)=Po(u_0,T)=Po(v_0,T)=0.5$

$Po(s_1,T)=Po(u_1,T)=Po(v_1,T)=0.4$

$Po(s_2,T)=Po(u_2,T)=Po(v_2,T)=0.6$

满足可能性互模拟定义的条件 2。

所以 M_1, M_2 和 M_3 都是可能性互模拟等价关系。M_3 由 M_1, M_2 组成,即 $M_3=M_1 \cup M_2$。

基于上面的一些基本概念,下面给出可能性互模拟的一些性质。

定理 2　可能性互模拟满足自反性、对称性和传递性。

证明:(自反性)对于在状态空间 S 上的可能的 Kripke 结构,$R=\{(s,s)\mid s\in S\}$ 对于 (M,M) 是一个可能性互模拟关系。

(对称性)假设 R 是可能的 Kripke 结构 (M_1,M_2) 上的可能性互模拟关系,通过交换位置得到一个新的等价关系 $R^{-1}=\{(s_2,s_1)\mid(s_1,s_2)\in R\}$。显然等价关系 R^{-1} 满足可能性互模拟关系条件 1 $L_1(s_1)=L_2(s_2)$ 和条件 2 $Po(s_1,T)=Po(s_2,T), T\in S/R$。从而得到可能的 Kripke 结构 (M_1,M_2),R^{-1} 也是一个可能性互模拟关系。

(传递性)假设 $R_{1,2}$ 和 $R_{2,3}$ 分别是可能的 Kripke 结构 (M_1,M_2) 和 (M_2,M_3) 可能性互模拟关系。定义关系 $R=R_{1,2}\cdot R_{2,3}$,$R=\{(s_1,s_3)\mid \exists s_2\in S_2,(s_1,s_2)\in R_{1,2}\wedge(s_2,s_3)\in R_{2,3}\}$ 是可能的 Kripke 结构 (M_1,M_3) 的等价关系,S_2 为可能的 Kripke 结构 M_2 的状态集合。

下面检验 (M_1,M_3) 是否满足可能性互模拟关系的条件:

1. 通过对 R 的定义,存在 $(s_1,s_2)\in R_{1,2},(s_2,s_3)\in R_{2,3}$ 这两个可能性互模拟关系,那么 $L_1(s_1)=L_2(s_2)=L_3(s_3)$ (满足条件 1)。

2. 因为 $(s_1,s_2)\in R_{1,2}$,那么 $Po(s_1,T)=Po(s_2,T)$ (对于每个等价类 $T\in S/R$)。又因为 $(s_2,s_3)\in R_{2,3}$,那么 $Po(s_2,T)=Po(s_3,T)$ (对于每个等价类 $T\in S/R$),所以 $Po(s_1,T)=Po(s_3,T)$ (对于每个等价类 $T\in S/R$)。由以上两点说明其满足可能性互模拟关系的两个条件,故可能性互模拟满足传递性。

如果可能性互模拟满足上面的性质,则可以讨论可能性互模拟路径等价的问题。

定义 9(可能性互模拟路径等价)　在可能的 Kripke 结构 M 上存在无穷路径 $\pi_1=s_{0,1}s_{1,1}s_{2,1}\cdots$ 和 $\pi_2=s_{0,2}s_{1,2}s_{2,2}\cdots$,如果 $\pi_1\sim_P\pi_2$ 当且仅当 $s_{i,1}\sim_P s_{i,2}, i\geqslant 0$。

定理 3　设 M_1 和 M_2 是在原子命题 AP 上可能的 Kripke 结构,R 是 M_1 和 M_2 的可能性互模拟关系,M_1 的所有状态 s_1 和 M_2 的所有状态 s_2 满足 $(s_1,s_2)\in R$。那么对于 M_1 中的(有穷或无穷)路径 $\pi_1=s_{0,1}s_{1,1}s_{2,1}\cdots\in path(s_1)$,在 M_2 中一定也存在一条和 π_1 长度相等的路径 $\pi_2=s_{0,2}s_{1,2}s_{2,2}\cdots\in path(s_2)$ 使得 $(s_{j,1},s_{j,2})\in R, j\geqslant 0$。

证明:当 $j=0$ 时,$s_{0,1}$ 为终止状态,根据假设 $(s_1,s_2)\in R$ 及可能性互模拟条件 2,可得 $s_{0,2}$ 也一定为终止状态,并且 π_1 和 π_2 的路径长度相等。

当 $j>0$ 时,如果 π_1 的长度是 $i, 0<i<j$。$s_{i,1}$ 就是终止状态,根据假设 $(s_1,s_2)\in R$ 及可能性互模拟条件 2,可得 $Po(s_{i,1},s_{i,1})=Po(s_{i,2},s_{i,2})=1$。所以 $s_{i,2}$ 也一定为终止状态。因此存在一条和 $\pi_1=s_{0,1}s_{1,1}s_{2,1}\cdots s_{i,1}$ 长度一样的路径 $\pi_2=s_{0,2}s_{1,2}s_{2,2}\cdots s_{i,2}$。

不妨设 $s_{i,1}$ 不是终止状态,根据假设 $(s_1,s_2)\in R$ 及可能性互模拟条件 2,可得 $Po(s_{i,1},T)=Po(s_{i,2},T), T\in S/R$。又因

为 $Po(s_{i,1},T)=\bigvee_{t\in T}Po(s_{i,1},t)$ 和 $Po(s_{i,2},T)=\bigvee_{t\in T}Po(s_{i,2},t)$，所以必定存在 $s_{i,1}$ 的后继 $s_{i+1,1}$ 和 $s_{i,2}$ 的后继 $s_{i+1,2}$，使得 $Po(s_{i,1},s_{i+1,1})=Po(s_{i,2},s_{i+1,2})$，故 $s_{i,2}$ 也不是终止状态。因此在 M_2 中一定也存在一条和 π_1 长度相等的路径 π_2 使得 $(s_{j,1},s_{j,2})\in R, j\geqslant 0$。

定义 10 在可能的 Kripke 结构 M 上，定义 $trace(\pi)=L(s_0)L(s_1)L(s_2)\cdots$ 为无穷路径 $\pi=s_0s_1s_2\cdots$ 的迹，$trace(\overset{\wedge}{\pi})=L(s_0)L(s_1)L(s_2)\cdots L(s_n)$ 为有穷路径 $\pi=s_0s_1s_2\cdots s_n$ 的迹。

定理 4(可能性互模拟迹相等) 由 $M_1\sim_P M_2$ 可得到 $Traces(M_1)=Traces(M_2)$。

证明：R 是可能的 Kripke 结构 M_1，M_2 的可能性互模拟关系。由定理 3 可知，任何在 M_1 中的路径 $\pi_1=s_{0,1}s_{1,1}s_{2,1}\cdots\in path(s_1)$ 都可以在 M_2 中找到一条路径 $\pi_2=s_{0,2}s_{1,2}s_{2,2}\cdots\in path(s_2)$ 使得 $(s_{j,1},s_{j,2})\in R, j\geqslant 0$。所以 $L_1(s_{j,1})=L_2(s_{j,2})$，$j\geqslant 0$，并且 $Traces(M_1)=Traces(M_2)$，故 $Traces(M_1)\subseteq Traces(M_2)$。然后根据可能性互模拟的对称性可得 $Traces(M_2)\subseteq Traces(M_1)$。所以关于可能的 Kripke 结构 M_1，M_2 是迹相等的。

定义 11 设 $M=(S,P,I,AP,L)$ 是一个可能的 Kripke 结构，商可能的 Kripke 结构 $M/\sim_P$ 定义如下：

$M/\sim_P(S/\sim_P,Po',I'_{init},AP,L')$ 其中，

$Po([s]\sim,[t]\sim)=Po(s,[t]\sim)$，$I'_{init}([s]\sim)=\bigcup_{s'\in[s]}I_{init}(s)$ 且 $L'([s]\sim)=L(s)$。

商可能的 Kripke 结构的状态空间 $M/\sim_P$ 是关于可能性互模拟 $\sim_P$ 的等价类的集合。从等价类 $[s]\sim$ 到等价类 $[t]\sim$ 的转移的可能性为 $Po(s,[t]\sim)$。

在一个状态数目非常大的模糊系统中，如果把所有的状态都定义在一个可能的 Kripke 结构中，那么它的状态空间将很有可能会发生状态爆炸。商可能的 Kripke 结构通过将模型最小化来有效地抑制状态爆炸问题的发生，从而减少了时间的花费和空间的开销。

例 3 由定义 11 知，图 1 中商可能的 Kripke 结构的状态空间为 $([s_0]\sim,[s_1]\sim,[s_3]\sim)$，$[s_0]\sim=\{s_0\}$，$[s_1]\sim=\{s_1,s_2\}$，$[s_3]\sim=\{s_3,s_4,s_5\}$，$L[s_0]\sim=\phi$，$L[s_1]\sim=\{a\}$，$L[s_3]\sim=\{b\}$，$Po([s_0]\sim,[s_1]\sim)=Po(s_0,[s_1]\sim)=0.5$，$Po([s_1]\sim,[s_3]\sim)=Po(s_1,[s_3]\sim)=0.5$。商可能的 Kripke 结构如图 3 所示。

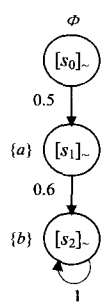

图 3 三状态商可能的 Kripke 结构

定义 12 设 M 是一个关于状态空间 S 的可能的 Kripke 结构并且 $T_0T_1T_2\cdots T_n\in S/\sim_P$ 是可能性互模拟 $\sim_P$ 的等价类。那么可能性互模拟闭包的 σ-代数 $\xi^M_{\sim P}$ 是通过柱集 $Cyl(T_0T_1T_2\cdots T_n)$ 表示 σ-代数，其中 $Cyl(T_0T_1T_2\cdots T_n)$ 是所有路径 $t_0t_1t_2\cdots t_nt_{n+1}t_{n+2}\cdots$ 的集合 $(t_i\in T_i, 0\leqslant i\leqslant n)$。

σ-代数相关定义参见文献[1]。

可能性互模拟闭包 σ-代数 $\xi^M_{\sim P}$ 的所有集合关于经典的 σ-代数都是可测的，这也就是说 $\xi^M_{\sim P}\subseteq\xi^M$。这种包含关系说明关于 σ-代数 $\xi^M_{\sim P}$ 基本事件 $Cyl(T_0T_1T_2\cdots T_n)$ 是可能的 Kripke 结构 M 上 σ-代数 ξ^M 的柱集的并集，表示如下：

$$Cyl(T_0T_1\cdots T_n)=\bigcup_{\substack{t_0t_1\cdots t_n\in Paths_{fin}(M)\\ t_i\in T,0\leqslant i\leqslant n}}Cyl(t_0t_1\cdots t_n)$$

式中，$T_0T_1\cdots T_n\in S/\sim_P$ 是互模拟的等价类，因此可能性互模拟闭包 σ-代数 $\xi^M_{\sim P}$ 叫做 σ-代数 ξ^M 的子代数。

习惯上将 $\xi^M_{\sim P}$ 的事件称作互模拟闭包事件。互模拟闭包 σ-代数 $\xi^M_{\sim P}$ 的事件是 σ-代数 ξ^M 上可测路径的集合。令 $\Pi\in\xi^M$ 是可测路径的集合，若对任何 $\pi_1\in\Pi$，$\pi_1\sim_P\pi_2$，可得到 $\pi_2\in\Pi$，那么集合 Π 是可能性互模拟闭包的。即：

$\xi^M_{\sim P}=\{\Pi\in\xi^M\mid \Pi$ 是可能性互模拟闭包的$\}$

引理 1 设 M 是一个可能的 Kripke 结构，对于所有的互模拟闭包事件 $\Pi\in paths(M)$，M 中的状态 s_1 和 s_2 如果满足 $s_1\sim_P s_2$，那么 $Pos^M_1(\Pi)=Pos^M_2(\Pi)$。

证明：根据不动点理论 $f:(S/\sim M)^+\to[0,1]$ 假设存在一个可能性测度 μ 在可能性互模拟闭包 σ-代数 $\xi^M_{\sim M}$ 上，那么对于所有的互模拟等价类 $T_i, 0\leqslant i\leqslant n$。有：

$\mu(Cyl(T_0T_1T_2\cdots T_n))=f(T_0T_1T_2\cdots T_n)$

式中，T,U 为 M 中的互模拟等价类，$Po(T,U)$ 的值为 $Po(t,U)$ 对于所有的 $t\in T$ 的值。

1. 如果 $s_1,s_2\in T_0$，则

$Pos^M_1(Cyl(T_0T_1\cdots T_n))=Po(T_0,T_1)\wedge Po(T_1,T_2)\wedge\cdots\wedge Po(T_{n-1},T_n)$

$=Pos^M_2(Cyl(T_0T_1\cdots T_n))$。

2. 如果 $s_1,s_2\notin T_0$，则

$Pos^M_1(Cyl(T_0T_1\cdots T_n))=Pos^M_2(Cyl(T_0T_1\cdots T_n))=0$。

定理 5(PoCTL/PoCTL* 与可能性互模拟的等价关系) 设 M 是一个可能的 Kripke 结构，s_1 和 s_2 是 M 中的状态。那么下述条件等价：

(a) $s_1\sim_P s_2$；

(b) s_1 和 s_2 是 PoCTL* 等价，即满足一样的 PoCTL* 公式；

(c) s_1 和 s_2 是 PoCTL 等价，即满足一样的 PoCTL 公式。

证明：从上述的表达可知 3 种表述都包含了可能性的因素，那么证明从两方面着手。一方面证明在 PoCTL* 与 PoCTL 公式中不包含可能性的部分的等价关系，那么这里的证明就转换为 CTL* / CTL 与互模拟的等价关系。另一方面证明在 PoCTL* 与 PoCTL 公式中包含可能性的部分的等价关系。

1. 首先证明在非可能性情况下的等价。

采用夹逼法则，分为 3 步。第一步，证明 CTL 等价相比互模拟等价的优越性，即 $\equiv_{CTL}\subseteq\sim_{TS}$；接下来，证明互模拟等价相比 CTL* 的优越性，即，$\sim_{TS}\subseteq\equiv_{CTL^*}$；显而易见 CTL* 等价比 CTL 更优越(因为 CTL* 包含 CTL) 那么具有以下的关系 $\sim\subseteq\equiv_{CTL^*}$ 且 $\equiv_{CTL^*}\subseteq\equiv_{CTL}$ 且 $\equiv_{CTL}\subseteq\sim$。

(1)首先证明 CTL 等价相比互模拟的优越性，使得 $R=\{(s_1,s_2)\mid s\in S/s_1\equiv_{CTL}s_2\}$ 是 Kripke 结构 M 上的互模拟等价

关系。通过互模拟的两个满足条件来检验它。

a. 考虑在原子命题 AP 上的 CTL 状态公式 Φ：

$$\Phi=\bigwedge_{a\in L(s_1)} a\wedge\bigwedge_{a\in AP\setminus L(s_1)}\neg a$$

很明显，因为 $s_1\models\Phi$，并且 $s_1\equiv_{CTL}s_2$，可知 $s_2\models\Phi$。因为 Φ 限定了状态 s_1 的标签函数，立即可得到 $L(s_1)=L(s_2)$，所以，互模拟的条件 1 满足。

b. 对于任意的等价类 $C\in S/R$，令 CTL 状态公式 Φ_C 满足 $Sat(\Phi_C)=C$。Φ_C 的描述如下。对每一对等价类 (C,D)，$(C,D)\in S/R$ 并且 $C\neq D$，令 CTL 状态公式 $\Phi_{C,D}$ 满足 $Sat(\Phi_{C,D})\supseteq C$ 并且 $Sat(\Phi_{C,D})\cap D=\phi$。因为 M 是有限的，那么在 R 中仅存在有限个等价类，Φ_C 被定义成所有的状态公式 $\Phi_{C,D}$ 的交集，有

$$\Phi_C=\bigwedge_{\substack{D\in S/R\\ D\notin C}}\Phi_{C,D}$$

显然，条件 $Sat(\Phi_C)=C$ 满足。令 $B\in S/R$ 并且 $s_1,s_2\in B$，即 $s_1,s_2\in R$ 并且 B 是关于 s_1,s_2 在 R 上的等价类。令 $s_1'\in post(s_1)$ 并且 C 是关于 s_1' 在 R 上的等价类即 $C=[s_1']_R$。那么存在一个转移 $s_2\to s_2'$ 关于 $(s_1',s_2')\in R$。因 $s_1'\in post(s_1)\cap C$ 且 $Sat(\Phi_C)=C$，则有 $s_1\models\exists O\Phi_C$。由 $s_1\equiv_{CTL}s_2$，得到 $s_2\models\exists O\Phi_C$。存在 $s_2'\in post(s_2)$ 关于 $s_2'\models\Phi_C$。但是 $Sat(\Phi_C)=C$，那么 $s_2'\in C$。又因为 $C=[s_t']_R$，可得 $(s_1',s_2')\in R$。因此，互模拟的条件 2 满足。

(2) 接下来证明互模拟等价相比 CTL* 的优越性，令 M 是一个在原子命题 AP 上的没有终结状态的 Kripke 结构，s_1，s_2 是 M 中的状态，并且 π_1,π_2 是 M 中的无限路径片段。那么，

(a) 如果 $s_1\sim s_2$，那么对于任意 CTL* 状态公式 Φ：$s_1\models\Phi$ 当且仅当 $s_2\models\Phi$。

(b) 如果 $\pi_1\sim\pi_2$，那么对于任意 CTL* 路径公式 φ：$\pi_1\models\varphi$ 当且仅当 $\pi_2\models\varphi$。

通过归纳法证明(a)和(b)成立。

第一步　令 $s_1\sim s_2$ 因 $\Phi=$true，(a)明显成立。因 $L_1(s_1)=L_2(s_2)$，于是 $\Phi=a\in AP$：$s_1\models a$ 当且仅当 $a\in L(s_1)$ 当且仅当 $a\in L(s_2)$ 当且仅当 $s_2\models a$。

第二步　假设 Φ_1,Φ_2,Ψ 是 CTL* 满足(a)的状态公式，φ 满足(b)路径公式。令 $s_1\sim s_2$。那么对于状态公式 Φ：

情况 1　$\Phi=\Phi_1\wedge\Phi_2$，由假设可知：

$s_1\models\Phi_1\wedge\Phi_2$ 当且仅当 $s_1\models\Phi_1$，$s_1\models\Phi_2$ 当且仅当 $s_2\models\Phi_2$，$s_2\models\Phi_1$ 当且仅当 $s_2\models\Phi_1\wedge\Phi_2$。

情况 2　$\Phi=\neg\Psi$，由假设可知：

$s_1\models\neg\Psi$ 当且仅当 $s_1\not\models\Psi$ 当且仅当 $s_2\not\models\Psi$ 当且仅当 $s_2\models\neg\Psi$。

情况 3　$\Phi=\exists\varphi$，由对称性知

$s_1\models\exists\varphi\Rightarrow s_2\models\exists\varphi$。

假设 $s_1\models\exists\varphi$，那么存在 $\pi_1=s_{0,1}s_{1,1}s_{2,1}\cdots\in path(s_1)$ 起点为 $s_1\models s_{0,1}$，并且 $\pi_1\models\varphi$。由于互模拟的路径等价，那么存在 $\pi_2=s_{0,2}s_{1,2}s_{2,2}\cdots\in path(s_2)$ 起点为 $s_2\models s_{0,2}$，以至于 $\pi_1\sim\pi_2$。(在(b)上)，得到 $\pi_2\models\varphi$。故，$s_1\models\exists\varphi$，$s_2\models\exists\varphi$。

假设 φ_1,φ_2 和 Ψ 分别满足 CTL* 路径公式和状态公式。令 $\pi_1\sim\pi_2$。$\pi_i[j\cdots]$ 表示下标为 $s_{ji}s_{ji+1}s_{ji+2}\cdots$ 的路径 π_i。

情况 1　$\varphi=\Phi$，由假设可知：

$\pi_1\models\varphi$ 当且仅当 $s_{0,1}\models\Phi$ 当且仅当 $s_{0,2}\models\Phi$ 当且仅当 $\pi_2\models\varphi$。

情况 2　$\varphi\models\varphi_1\wedge\varphi_2$，由假设知：

$\pi_1\models\varphi_1\wedge\varphi_2$ 当且仅当 $\pi_1\models\varphi_1$，$\pi_1\models\varphi_2$ 当且仅当 $\pi_2\models\varphi_1$，$\pi_2\models\varphi_2$ 当且仅当 $\pi_2\models\varphi_1\wedge\varphi_2$。

情况 3　$\varphi\models\neg\Psi$，由假设知：

$\pi_1\models\neg\Psi$ 当且仅当 $\pi_1\not\models\Psi$ 当且仅当 $\pi_2\not\models\Psi$ 当且仅当 $\pi_2\models\neg\Psi$。

情况 4　$\varphi\models O\Psi$，由假设知：

$\pi_1\models O\Psi$ 当且仅当 $\pi_1[1\cdots]\models\Psi$ 当且仅当 $\pi_2[1\cdots]\models\Psi$ 当且仅当 $\pi_2\models O\Psi$。

情况 5　$\varphi\models\varphi_1\cup\varphi_2$，由假设知：

$\pi_1\models\varphi_1\cup\varphi_2$ 当且仅当下标 $j\in N$，$\pi_1[j\cdots]\models\varphi_2$ 并且 $\pi_1[i\cdots]\models\varphi_1$，$i=0,1,\cdots,j-1$，当且仅当下标 $j\in N$，$\pi_2[j\cdots]\models\varphi_2$ 并且 $\pi_2[i\cdots]\models\varphi_1$，$i=0,1,\cdots,j-1$，当且仅当 $\pi_2\models\varphi_1\cup\varphi_2$。

2. 接下来证明包含可能性的部分，假设对于可能的 Kripke 结构 M 中的路径 π_1,π_2 如果 $\pi_1\sim_P\pi_2$，那么 $\pi_1\models\varphi$ 并且 $\pi_2\models\varphi$。令 $s_1\sim_P s_2$ 并且 $\prod$ 是 M 上满足 φ 的路径的集合，即，$\prod=\{\pi\in path(M)\mid\pi\models\varphi\}$。由假设和引理 1 得到：

$$Po(s_1\models\varphi)=Pos_1^M(\prod)=Pos_2^M(\prod)=Po(s_2\models\varphi)$$

显然(1)⇒(2)，又因为 PoCTL 是 PoCTL* 的子逻辑，故(1)⇒(2)，(3)。

(3)⇒(1)：$R=\{(s_1,s_2)\in S\times S\mid s_1\equiv_{PoCTL}s_2\}$ 是一个 PoCTL 等价关系。令 $(s_1,s_2)\in R$。因为 s_1,s_2 满足一样的原子命题，于是 $L_1(s_1)=L_2(s_2)$，满足可能性互模拟条件 1。令 T,U 是等价类并且 $T\neq U$，对于 PoCTL 公式 $\Phi_{T,U}$ 有 $Sat(\Phi_{T,U})\supseteq T$ 并且 $Sat(\Phi_{T,U})\cup T=\phi$。定义：

$$\Phi_T=\bigwedge_{\substack{U\in S/\sim_M\\ U\neq T}}\Phi_{T,U}$$

显然 $Sat(\Phi_T)=T$。假设 $Po(s_1,T)\leqslant Po(s_2,T)$，令 $s_1\models Po_{\leqslant P}(\Phi_T)$，$P=Po(s_1,T)$。因为 $s_1\equiv_{PCTL}s_2$，故 $s_2\models Po_{\leqslant P}(\Phi_T)$，$P=Po(s_1,T)\leqslant Po(s_2,T)\leqslant p$，由上不等式得到 $Po(s_1,T)=Po(s_2,T)=P$ 满足可能性互模拟条件 2。

(2)⇒(1)同理。

所以可能的 Kripke 结构如果满足可能性互模拟，那么一定满足 PoCTL* 等价并且满足 PoCTL 等价。

例 4　在图 1 中，M_1 的两个状态 $s_1\not\sim_P s_2$，存在一个 PoCTL 公式 $Po_{\leqslant 0.2}(Ob)$，显然只有 s_2 满足该公式，而 s_1 并不满足该公式。

结束语　本文是在可能的 Kripke 结构、PoLTL 和 PoCTL 的基础上提出了 POCTL* 的定义。在经典互模拟和可能性测度的基础上建立了可能性互模拟理论，给出了对于两个满足可能性互模拟的可能的 Kripke 结构的相互表示以及可能性互模拟的化简；证明了可能性互模拟满足自反性、对称性和传递性，以及可能性互模拟迹相等、可能性互模拟闭包事件保可能性；最后证明了 PoCTL 和 PoCTL* 与可能性互模拟的等价关系。因为可能性互模拟可以用来简化模糊环境下的状态空间，所以可能性互模拟有着很好的应用前景，比如抑制状态爆炸。

参 考 文 献

[1] Baier C, Katoen J P. Principles of Model Checking [M]. The

MIT Press,2007
[2] Zadeh L A. Fuzzy sets[J]. Information and Control,1965,8:338-353
[3] 薛艳,雷红轩,李永明. 基于可能性测度的计算树逻辑[J]. 计算机工程与科学,2011,33(9):70-75
[4] Drakopoulos J A. Probabilities, possibilities, and fuzzy sets[J]. Fuzzy Sets and Systems,1995,75:1-15
[5] 李永明. 模糊系统分析[M]. 北京:科学出版社,2005
[6] 欧阳丹彤,欧阳继红. 基于模型的诊断方法[J]. 南京大学学报,2000,36:187-192
[7] 雷丽晖,段振华. 使用扩展区间时序逻辑为并发工作流建模[J]. 西安电子科技大学学报,2007,34(4):673-680
[8] 赵林,吴尽昭. 基于吴方法的多值模型检验[J]. 系统科学与数学,2008,28(8):1020-1029
[9] 杨军,葛海通,郑飞君,等. 一种形式化验证方法:模型检验[J]. 浙江大学学报,2006,33(4):403-407
[10] 哈明虎,吴从炘. 模糊测度与模糊积分[M]. 北京:科学出版社,1998
[11] Clarke E, Grumberg O, Peled D. Model Checking [M]. MIT Press,1999
[12] Jenhani I,Benferhat S,Elouedi Z. Learning and Evaluating Possibilistic DecisionTrees using Information Affinity[J]. World Academy of Science, Engineering and Technology,2010,63:599-605
[13] Droste M,Kuich W,Vogler H,et al. Handbook of Weighted Automata[M]. An EATCS Series, Birlin-Heidelberg: Springer-Verlag,2009
[14] Kwiatkowska M. Quantitative Verification: Models, Techniques and Tools[C]//ESEC-FSE '07. 2007:449-458
[15] Hart S,Sharir M. Probabilistic propositional temporal logics[J]. Information and Control,1986,70(2/3):97-155
[16] Boutouhami S,Mokhtari A. Possibilistic Explanation[J]. International Journal of Computer Sicence and Applicatongs,2006,3(2):57-73

(上接第 239 页)

高了算法的计算效率。此外,通过购房综合评价的实例表明,该算法是可行且有效的。另外,该文提出的'删除不重要覆盖的策略'也可以用来加速其它基于信息量的约简算法,例如文献[16,18]中的约简算法。

相对于 Pawlak 粗糙集中的高效约简算法,该文提出的完备覆盖约简算法的时间复杂度可能仍有下降的空间,因此继续提出一些有效的措施以提高本文算法的运行效率是很有必要的。对于这方面的研究,可以借鉴 Pawlak 粗糙集中已取得的成熟经验,例如先排序,再求论域的划分。与此同时,困难也是存在的,比如"先排序,再求论域的划分"这种策略,它在一定程度上依赖于对象在各属性下的取值情况,而以覆盖族进行表示的数据集中对象在各属性下的取值有些并不唯一,故直接利用属性值进行排序存在一定的困难。因此,这个问题还有待于进一步研究,也是本文后继工作的一部分。此外,继续讨论覆盖决策系统[21,22]下的启发式加速约简算法是本文的另一个后继工作,将另文发表。

参 考 文 献

[1] Pawlak Z. Rough sets [J]. International Journal of Computer and Information Sciences,1982,11(5):341-356
[2] Pawlak Z,Skowron A. Rudiments of rough sets [J]. Information Sciences,2006,177(1):3-27
[3] 张文修,梁怡,吴伟志. 信息系统与知识发现[M]. 北京:科学出版社,2003
[4] 张文修,吴伟志. 粗糙集理论介绍和研究综述[J]. 模糊系统与数学,2000,14(4):1-12
[5] 王国胤,姚一豫,于洪. 粗糙集理论与应用研究综述[J]. 计算机学报,2009,32(7):1229-1246
[6] 李金海,吕跃进. 决策系统的快速属性约简算法[J]. 电子科技大学学报,2007,36(6):1237-1240
[7] Zakowski W. Approximations in the Space(u,π)[J]. Demonstratio Mathematica,1983,16:761-769
[8] Bonikowski Z, Bryniarski E, Wybraniec U. Extensions and intensions in the rough set theory [J]. Information Sciences,1998,107:149-167
[9] Pomykala J A. Approximation operations in approximation space [J]. Bulletin of the Polish Academy of Sciences,1987,35:653-662
[10] Tsang E,Chen D G,Lee J,et al. On the upper approximations of covering generalized rough sets [C]// IEEE Proceedings of the Third International Conference on Machine Learning and Cybernetics. Shanghai,2004:4200-4203
[11] Zhu W,Wang F Y. On three types of covering-based rough sets [J]. IEEE Transactions on Knowledge and Data Engineering,2007,19:1131-1144
[12] 魏荣,刘保仓,史开泉. 基于覆盖广义粗集的模糊性[J]. 计算机科学,2007,34(1):153-155
[13] 杨勇,朱晓钟,李廉. 覆盖粗糙集的公理化[J]. 计算机科学,2009,36(5):181-182
[14] Zhu W, Wang F Y. Reduction and axiomization of covering generalized rough sets [J]. Information Sciences,2003,152:217-230
[15] 胡军,张闽. 覆盖近似空间的约简理论[J]. 计算机工程与应用,2007,43(28):86-88
[16] 张燕兰,李进金. 广义覆盖粗集的约简[J]. 模糊系统与数学,2010,24(3):138-143
[17] Tsang E,Chen D G,Yeung D. Approximations and reducts with covering generalized rough sets [J]. Computers and Mathematics with Applications,2008,56:279-289
[18] 梁吉业,曲开社,徐宗本. 信息系统的属性约简[J]. 系统工程理论与实践,2001,21(12):76-80
[19] 王国胤,于洪,杨大春. 基于条件信息熵的决策表约简[J]. 计算机学报,2002,25(7):759-766
[20] 苗夺谦,胡桂荣. 知识约简的一种启发式算法[J]. 计算机研究与发展,1999,36(6):681-684
[21] Li F,Yin Y Q. Approaches to knowledge reduction of covering decision systems based on information theory [J]. Information Sciences,2009,179:1694-1704
[22] Chen D G,Wang C Z,Hu Q H. A new approach to attribute reduction of consistent and inconsistent covering decision systems [J]. Information Sciences,2007,177:3500-3518