软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2011,22(6):1169−1184 [doi: 10.3724/SP.J.1001.2011.04020]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

循环对称化简及在三值模型上的扩展*

魏 欧[1,2+], 袁 泳[2], 蔡昕烨[1], 黄志球[1], 徐丙凤[1]

[1](南京航空航天大学 计算机科学与技术学院,江苏 南京 210016)

[2](Department of Computer Science, University of Toronto, Ontario Canada M5S 3G4)

Cycle Symmetry Reduction and Its Extension on Three-Valued Models

WEI Ou[1,2+], YUAN Yong[2], CAI Xin-Ye[1], HUANG Zhi-Qiu[1], XU Bing-Feng[1]

[1](College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)

[2](Department of Computer Science, University of Toronto, Ontario Canada M5S 3G4)

+ Corresponding author: E-mail: owei@nuaa.edu.cn

Wei O, Yuan Y, Cai XY, Huang ZQ, Xu BF. Cycle symmetry reduction and its extension on three-valued models. *Journal of Software*, 2011,22(6):1169−1184. http://www.jos.org.cn/1000-9825/4020.htm

Abstract: This paper defines the notion of cycle symmetry, which extends the traditional automorphism-based symmetry and enables application of symmetry reduction to a broader class of asymmetric systems. The study also shows that both cycle symmetry group and cycle symmetry generated group can be used to produce a quotient structure that is bisimilar to the original model. Furthermore, the extension of symmetry reduction over three-valued models is investigated. The quotient structure of a three-valued model is defined and induced by a permutation group and extends to both automorphism-based symmetry reduction and cycle symmetry reduction to three-valued models. Finally, the study analyzes the relationship between symmetry reduction of a three-valued model and classical models induced by it. Both approaches can lead to the same reduced quotient structure of the original model.

Key words: model checking; symmetry reduction; cycle symmetry; three-valued model

摘 要: 为了将对称化简扩展到更多的非对称系统上,扩展了传统的基于自同构的对称性,提出了一种称为循环对称的新的对称性.证明了采用循环对称置换群或者由一组循环对称置换所生成的置换群仍可得到与原模型互模拟的对称商结构,从而达到化简系统规模的目的.进一步地,研究如何将对称化简应用于多值模型.多值模型可以有效地表示系统中的不确定信息,正越来越多地用于软件系统的建模与分析中.针对一种具体的多值模型——三值模型,定义传统的对称化简和循环对称化简在其上面的扩展.最后,分析三值模型的商结构与由约简得到的二值模型商结构之间的关系,证明了两种途径的等价性.

关键词: 模型检测;对称化简;循环对称;三值模型

中图法分类号: TP301 **文献标识码**: A

* 基金项目: 国家高技术研究发展计划(863)(2009AA010307); 中国博士后科学基金(20100471338); 南京航空航天大学基本科研业务费专项科研项目(NS2010110)

收稿时间: 2010-07-10; 定稿时间: 2011-03-29

模型检测[1,2]是一种对有限状态的计算机系统进行自动验证的方法.这种方法一般通过对系统状态空间的穷尽搜索来判断系统属性的成立与否.模型检测技术已经成功地应用于对集成电路、通信协议等并发系统的验证.制约模型检测技术在实际中进一步得到应用的主要障碍是状态爆炸问题,并发系统的状态空间往往随着系统中的变量以及进程的增加而呈指数级增长.这时候,由于需要使用过多的存储或计算资源,直接采用模型检测方法对系统进行验证的效率非常低,甚至无法在实际中实现.为解决这个问题,一系列相关的方法已经被提出,主要包括符号化方法[3]、抽象方法[4,5]、偏序规约[6]、对称化简[7−9]等.其中,Clarke 和 Emerson 等人提出的对称化简是一种通过避免对系统中对称状态的重复搜索而有效减少验证规模的方法.对称性经常表现在包含多个相同进程的并发系统中,例如互斥协议(MUTEX).由于交换相同的进程不会影响系统的整体行为,因此可以采用自同构置换群刻画进程之间的对称性,并基于此将系统的状态空间划分为若干个等价类.进一步,在所有的等价类上定义迁移关系得到商结构(quotient structure).根据对称性,商结构与原始的系统之间呈互模拟关系.因此,在商结构上对时序逻辑所表达的系统属性进行验证时,可以得到与在原系统上相同的结果.由于根据置换群所划分的等价类的数目远小于系统原有的状态,因此采用对称化简可以有效地减少系统的状态空间,提高模型检测的效率.

然而,实际中的许多系统并不是真正的对称.这类系统往往包含多个近似的而非完全相同的进程.例如,对于读者-写者协议,由于读者与写者有相似的状态迁移关系,即空闲→请求→使用资源→空闲,因此系统的整体行为具有高度的相似性;但是,由于写者比读者有更高的访问关键资源的优先级,因此系统行为并非完全对称.在这种情况下,无法对系统使用传统的对称化简方法来减少被验证模型的规模.为了解决这一问题,本文定义一种新的对称性,称为循环对称,使得对称化简可以扩展到非对称的系统上.循环对称放宽了传统用于刻画对称性的条件,不要求置换为自同构.我们证明,根据循环对称置换所得到的商结构仍然与原系统保持互模拟的关系,因此同样可以用于对时序逻辑属性的验证.

在目前的文献中,对称化简还只应用于传统的二值模型.在这种模型中,每个原子命题在状态上的值以及状态之间的迁移关系为真或者假.而随着多值模型[10,11]在软件建模和分析中的应用,多值模型上的对称化简研究也是一个很有意义的问题.多值模型将传统的二值模型扩展到多值逻辑上,用来表示信息的不同真实程度.例如,对于一组软件产品系列(software product family)可以用一个多值模型加以描述[12].另外,在软件开发过程中往往通过迭代精化的方法获取最终的软件系统,在这个过程中的模型往往是不完备的.这时候,采用多值模型可以对信息的不确定性进行描述[13].对于多值模型,已经存在着用以进行模型检测的工具.但是,正如传统的二值模型检测中存在状态爆炸问题一样,多值模型检测也同样受这个问题的制约.在本文中,我们以一种常用的多值模型——三值模型为研究对象,定义对它的对称化简.

三值模型中原子命题的取值以及状态迁移关系除了可以用“真”或“假”进行描述外,还可以赋予“可能”值.三值模型最早由 Larsen 提出,用以对并发系统进行描述,其具体的模型形式为模态迁移系统(modal transition system);Huth,Godfroid 和 Chechik 等人又相继提出了 Kripke 模态迁移系统(Kripke modal transition system)、不完备 Kripke 系统(partial Kripke structure)、三值 Kripke 结构(3-valued Kripke structure)[10,13].Godefroid 证明,这些三值模型虽然有不同的结构特征,但是都具有相同的表达能力.本文以三值 Kripke 结构为具体的研究对象,定义传统的对称化简以及我们所提出的循环对称化简在这种模型上的扩展.另外,对三值模型的分析可以通过将其约简为二值模型检测进行[14].因此,我们也进一步分析了三值模型与通过约简所得到二值模型上的对称化简之间的关系,证明了两者的等价性.

本文第 1 节介绍对称化简及三值模型的理论基础.第 2 节讨论如何将对称化简扩展到非对称模型上,定义循环对称以及基于此对称性的化简.第 3 节讨论如何在三值模型上扩展传统的对称化简以及循环对称化简,并分析三值模型与约简所得到的二值模型上的对称化简之间的关系.第 4 节讨论相关工作.第 5 节对本文作总结.

1 理论基础

1.1 计算模型与互模拟

我们采用 Kripke 结构作为系统的计算模型.定义在一组原子命题集合 AP 上的一个 Kripke 结构是一个三元组 $M=(S,R,L)$,其中,S 是有限状态集,$R\subseteq S\times S$ 是全状态迁移关系,$L:S\to 2^{AP}$ 是状态标注函数.我们分析计算树逻辑(computation tree logic,简称 CTL)描述的系统属性.用符号 $M,s\vDash\varphi$ 表示一个 CTL 公式 φ 在模型 M 中的状态 s 上被满足.

Kripke 结构之间相对于 CTL 公式的等价关系可以用互模拟进行刻画[1].

定义 1. 设 $M=(S,R,L)$ 与 $M'=(S',R',L')$ 为定义在原子命题集合 AP 上的两个 Kripke 结构.关系 $B\subseteq S\times S'$ 是 M 与 M' 之间的互模拟关系,当且仅当对所有的 $s\subseteq S$ 和 $s'\subseteq S'$,如果 $(s,s')\in B$,那么下列条件成立:

(a) $L(s)=L'(s')$;

(b) $\forall t\in S\cdot(s,t)\in R\Rightarrow\exists t'\in S'\cdot(s',t')\in R'\wedge(t,t')\in B$;

(c) $\forall t'\in S'\cdot(s',t')\in R'\Rightarrow\exists t\in S\cdot(s,t)\in R\wedge(t,t')\in B$.

定理 1. 设 $M=(S,R,L)$ 与 $M'=(S',R',L')$ 为两个 Kripke 结构.关系 $B\subseteq S\times S'$ 是 M 与 M' 之间的一个互模拟关系,φ 为任意的 CTL 公式.那么对所有的 $(s,s')\in B$,$M,s\vDash\varphi\Leftrightarrow M',s'\vDash\varphi$.

1.2 对称化简

集合 A 上的置换 σ 是双射函数 $\sigma:A\to A$.对于置换群 G,置换 σ 的阶是使得 $a^k=e$ 成立的最小正整数 k,记作 $|\sigma|$.如果置换群 G 是由一组置换 $\{\sigma_1,\sigma_2,\ldots,\sigma_k\}$ 通过复合运算所得到的闭包(closure),称这组置换为 G 的生成置换,记作 $G=(\sigma_1,\sigma_2,\ldots,\sigma_k)$.对置换 σ,若 $\sigma(t_1)=t_2,\sigma(t_2)=t_3,\ldots,\sigma(t_{k-1})=t_k,\sigma(t_k)=t_1$,且保持其他元素不变,则称 σ 为轮换,记作 $\sigma=(t_1,t_2,\ldots,t_{k-1},t_k)$.每个置换都可以被表示成不相交的轮换的复合.

对称化简基于 Kripke 结构中状态空间上的置换[7].

定义 2. 设 $M=(S,R,L)$ 为一个 Kripke 结构.状态空间 S 上的置换 σ 是 M 的自同构,当且仅当它保持状态迁移关系 R,即

$$\forall s_1,s_2\in S\cdot(s_1,s_2)\in R\Leftrightarrow(\sigma(s_1),\sigma(s_2))\in R.$$

置换群 G 是 Kripke 结构 M 的自同构群,当且仅当 G 中的每一个置换都是 M 的自同构.

定义 3. 设 $M=(S,R,L)$ 为一个 Kripke 结构.置换 σ 是原子命题 p 的不变置换,当且仅当下列条件成立

$$\forall s\in S\cdot p\in L(s)\Leftrightarrow p\in L(\sigma(s)).$$

Kripke 结构 M 上的置换群 G 是公式 φ 的不变置换群,当且仅当 G 中的每一个置换都是 φ 所有原子命题的不变置换.

给定一个 Kripke 结构 $M=(S,R,L)$ 及其置换群 G,S 可被划分为一组等价类:对于 S 中的任意状态 s,定义 s 的等价类为 $\theta(s)=\{s'\in S|\exists\sigma\in G\cdot\sigma(s)=s'\}$.该等价类也被称为 s 的轨道(orbit).对每一个轨道,任意选取一个状态作代表状态,记作 $rep(\theta(s))$.以 S 中所有状态的轨道为状态空间定义商结构 $M_G=(S_G,R_G,L_G)$,其中:

- $S_G=\{\theta(s)|s\in S\}$;
- $R_G=\{(\theta(s),\theta(t))|(s,t)\in R\}$;
- $L_G(\theta(s))=L(rep(\theta(s)))$.

如果 G 是 M 的自同构群,且是公式 φ 的不变置换群,那么相对于 φ 中的原子命题,关系 $B=\{(s,\theta(s))|s\in S\}$ 是商结构 M_G 与原结构 M 之间的互模拟关系.因此,对 φ 在 M_G 与 M 上可以得到相同的模型检测结果.

定理 2. 设 $M=(S,R,L)$ 为 Kripke 结构,G 是 M 上的自同构置换群.如果 G 是公式 φ 的不变置换群,那么有

$$\forall s\in S\cdot M,s\vDash\varphi\Leftrightarrow M_G,\theta(s)\vDash\varphi.$$

1.3 三值模型与精化

多值模型检测是传统的二值模型检测的扩展,可用于对不确定信息的推理.其输入通常为一个多值状态迁

移系统 M,一个用于描述系统属性的时序逻辑公式φ.模型检测的结果采用相应的多值逻辑值表示时序逻辑公式在系统上被满足的程度,在状态 s 的值记作$\|\varphi\|^M(s)$.在本文中,我们重点研究 CTL 公式在三值模型上的验证.

三值逻辑也称作 Kleene 逻辑,比二值逻辑增加了一个逻辑值,包含 3 个逻辑值,即 t,f 和 m,分别表示真(true)、假(false)和可能(maybe).在这些逻辑值上定义有两种序关系:一种是真实序关系($\leqslant$),用于表示逻辑值的真实程度,定义为 $f\leqslant m\leqslant t$,并且对所有值 $x\leqslant x$;另一种是信息序关系($\preceq$),用于表示逻辑值的信息完整程度,定义为 $m\preceq t$,$m\preceq f$,并且对所有值 $x\preceq x$.

相应的模型采用三值 Kripke 结构定义.定义在一组原子命题 AP 上的一个三值 Kripke 结构是一个三元组 $M=(S,R,L)$.与第 2.1 节中定义的传统二值 Kripke 结构不同的是,R 与 L 定义在三值逻辑上,即 $R:S\times S\to\{t,m,f\}$,$L:S\times AP\to\{t,m,f\}$.

三值 Kripke 结构之间的精化关系通过对二值 Kripke 结构之间的模拟关系扩展而得到[10].

定义 4. 设 $M_1=(S_1,R_1,L_1)$与 $M_2=(S_2,R_2,L_2)$为定义在原子命题集 AP 上的两个三值 Kripke 结构.关系$\rho\subseteq S_1\times S_2$是 M_1 与 M_2 之间的精化关系,当且仅当对任意的 $s_1\in S_1,s_2\in S_2$,如果$(s_1,s_2)\in\rho$,则下列条件成立:

(a) $\forall p\in AP\cdot L_2(s_2,p)\preceq L_1(s_1,p)$;

(b) $\forall t_2\in S_2\cdot R_2(s_2,t_2)=t\Rightarrow\exists t_1\in S_1\cdot R_1(s_1,t_1)=t\wedge(t_1,t_2)\in\rho$;

(c) $\forall t_1\in S_1\cdot R_1(s_1,t_1)\geqslant m\Rightarrow\exists t_2\in S_2\cdot R_2(s_2,t_2)\geqslant m\wedge(t_1,t_2)\in\rho$.

如果 M_1 与 M_2 存在如上定义的精化关系,则称 M_1 是 M_2 的精化,记作 $M_2\preceq_\rho M_1$.在这种情况下,时序逻辑公式在 M_1 上模型检测结果相对于信息序关系比在 M_2 上的结果更加精确,即可以得到更多确定性的(真或假)结果.

定理 3. 设 $M_1=(S_1,R_1,L_1)$与 $M_2=(S_2,R_2,L_2)$为定义在原子命题集合 AP 上的两个三值 Kripke 结构,关系$\rho\subseteq S_1\times S_2$是 M_1 与 M_2 之间的精化关系,那么对于任意的 CTL 公式φ,如果$(s_1,s_2)\in\rho$,则

$$\|\varphi\|^{M_2}(s_2)\preceq\|\varphi\|^{M_1}(s_1).$$

也就是说,如果φ在 s_2 上为 t(真)或 f(假),那么它在 s_1 上相应地分别为 t 或 f;如果φ在 s_2 上为 m(可能),那么它在 s_1 可以为 t,f 或者 m.

2 循环对称化简

在本节中,我们扩展传统的对称化简到非对称模型上,定义循环对称,研究在此基础上的对称化简.

2.1 基于循环对称置换群的化简

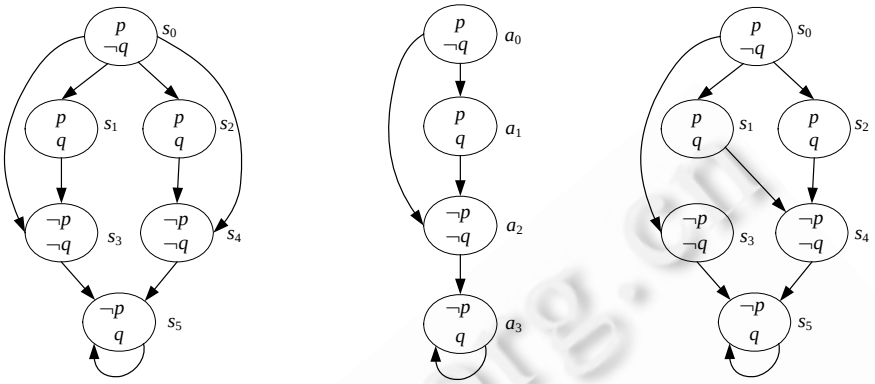
第 1.2 节介绍的传统的对称化简基于状态空间上的自同构置换.例如,对于图 1(a)中所示的 Kripke 结构 M_1,s_1 与 s_2,以及 s_3 与 s_4 分别为相应的对称状态.因此,$\sigma=(s_1,s_2)(s_3,s_4)$是 M_1 的自同构置换.考虑由σ生成的群 $G=\langle\sigma\rangle$.G 中只包含两个置换:σ以及单位元.根据 G 可以定义 4 个轨道(状态对称等价类),即$\{s_0\}$,$\{s_1,s_2\}$,$\{s_3,s_4\}$和$\{s_5\}$,分别用 a_0,a_1,a_2 和 a_3 表示.根据定义,可以得到如图 1(b)所示的商结构 M_{1G}.由于 G 是原子命题 p 和 q 的不变置换群,因此 M_1 和 M_{1G} 基于对称关系互模拟,在这两个模型上,对 CTL 公式的检测结果相同.

然而,对于图 1(c)所示的 Kripke 结构 M_2,虽然它与 M_1 相似,但是由于缺少了状态迁移关系 $s_0\to s_4$ 和 $s_1\to s_3$,并且增加了 $s_1\to s_4$,M_2 相对于置换群 G 是非对称的,即 G 不是 M_2 的自同构群.例如,对于 M_2 中的迁移关系 $s_0\to s_3$,应用 G 中的置换σ,有$\sigma(s_0)=s_0$,$\sigma(s_3)=s_4$,但是 M_2 中不存在状态迁移关系 $s_0\to s_4$;同样,对于 M_2 中的迁移关系 $s_1\to s_4$,M_2 中不存在相应的迁移关系$\sigma(s_1)\to\sigma(s_4)$,即 $s_2\to s_4$.在这种情况下,无法根据传统的对称性采用 G 对 M_2 进行化简.

但是,进一步分析可以发现,虽然 M_2 相对于 G 不是完全对称,但是这些非对称的部分事实上并不影响采用 G 对 M_2 进行化简.例如前面提到,对于迁移关系 $s_0\to s_3$,M_2 不存在与它对称的迁移关系 $s_0\to s_4$.但是,由于 s_3 与 s_4 仍然对称,即 s_3 与 s_4 上的原子命题相同并且可以到达相同的状态.因此,缺少迁移关系 $s_0\to s_4$ 不影响表达如下信息,即从 s_0 可以到达一个命题 p 和 q 都为假的状态,并进一步可以到达一个 p 为假且 q 为真的状态.类似地,虽然 M_2

中不存在与迁移关系 $s_1\to s_4$ 对称的迁移关系 $s_2\to s_3$,但是在 M_2 中,从 s_2 可以到达与 s_3 对称的状态 s_4,这可以用来表示与迁移关系 $s_2\to s_3$ 相同的信息.

基于上述考虑,接下来定义循环对称,并且证明在这种情况下,根据 G 所得到 M_2 的商结构 M_{2G},仍然与 M_2 存在互模拟关系,从而实现将对称化简扩展到非对称模型上.



(a) A Kripke structure M_1
(a) Kripke 结构 M_1

(b) M_{1G}: The quotient structure of M_1
(b) M_{1G}: M_1 的商结构

(c) A Kripke structure M_2
(c) Kripke 结构 M_2

Fig.1
图 1

定义 5. 设 $M=(S,R,L)$为一个 Kripke 结构,S 上的置换σ是 M 的循环对称置换,当且仅当下列条件成立:

$$\forall s_1,s_2\in S\cdot(s_1,s_2)\in R\Rightarrow\exists i\geqslant 1\cdot(\sigma(s_1),\sigma^i(s_2))\in R.$$

根据定义,如果σ是 M 的循环对称置换,那么对于 M 中的任意迁移关系 $s_1\to s_2$,即使 M 中不存在相应的对称迁移关系$\sigma(s_1)\to\sigma(s_2)$,经过对$\sigma$的 i 次复合,在 M 中仍然存在从$\sigma(s_1)$到$\sigma^i(s_2)$的迁移关系.

根据理论基础,置换σ可以被表示成不相交的轮换的复合,设其分解式为

$$\sigma=\sigma_1\sigma_2\ldots\sigma_l,$$

其中,任何两个置换都作用于不同的元素.如果定义 5 中的 i 存在并且$\sigma_k(1\leqslant k\leqslant l)$作用在 s_2 上,则有 $1\leqslant i\leqslant|\sigma_k|$.如果$\sigma$是 M 的自同构置换,则 i 的取值为 1.因此,基于自同构的对称可以看作是循环对称的一种特殊情况.

置换群 G 是 Kripke 结构 M 的循环对称置换,当且仅当 G 中的每一个置换都是 M 的循环对称置换.对于循环对称置换群,我们可以采用与传统对称化简相同的方法(第 1.2 节)定义 M 在 G 下的商结构.

下面证明,当 G 同时也是原子命题的不变置换群时,与传统的对称化简中的情况一样,该商结构与原模型存在互模拟关系.

引理 1. 设 $M=(S,R,L)$为一个定义在原子命题集合 AP 上的 Kripke 结构,G 是 M 的循环对称置换群,$M_G=(S_G,R_G,L_G)$是 M 在 G 下的商结构.定义关系 $B\subseteq S\times S_G$ 为$\forall s\in S\cdot(s,\theta(s))\in B$.那么,如果 G 是 AP 的不变置换群,B 是 M 与 M_G 的互模拟关系.

证明:根据互模拟的定义,对于任意$(s,\theta(s))\in B$,我们证明以下结果成立:

(a) $L(s)=L_G(\theta(s))$;

(b) $\forall t\in S\cdot(s,t)\in R\Rightarrow\exists t'\in S\cdot(\theta(s),\theta(t'))\in R_G\wedge(t,\theta(t'))\in B$;

(c) $\forall t'\in S\cdot(\theta(s),\theta(t'))\in R_G\Rightarrow\exists t\in S\cdot(s,t)\in R\wedge(t,\theta(t'))\in B$.

- 我们首先证明结果(a)成立.

  根据商结构 M_G 的定义

  $$L_G(\theta(s))=L(rep(\theta(s))).$$

  根据$\theta(s)$的定义

$$\exists \sigma \in G \cdot rep(\theta(s)) = \sigma(s).$$

因为 G 是 AP 的不变置换群,则

$$\forall p \in AP \cdot p \in L(s) \Leftrightarrow p \in L(rep(\theta(s))).$$

因此有

$$L_G(\theta(s)) = L(rep(\theta(s))) = L(s).$$

所以,结果(a)成立.

- 再证明结果(b)成立.

  考虑任意的 $t \in S$,使得$(s,t) \in R$.根据 R_G 的定义,有$(\theta(s),\theta(t)) \in R_G$.

  根据 B 的定义,有$(t,\theta(t)) \in B$.令 $t'=t$,则结果(b)成立.

- 最后证明结果(c)成立.

  考虑任意的 $t' \in S$,使得$(\theta(s),\theta(t')) \in R_G$.根据 R_G 的定义,有

  $$\exists s_1 \in S \cdot \exists t_1 \in S \cdot (s_1,t_1) \in R \wedge s_1 \in \theta(s) \wedge t_1 \in \theta(t').$$

  根据轨道的定义以及置换群的属性,有

  $$\exists \sigma_1 \in G \cdot s = \sigma_1(s_1),$$

  以及

  $$\exists \sigma_2 \in G \cdot t_1 = \sigma_2(t').$$

  因为 G 是 M 的循环对称置换群,并且$(s_1,t_1) \in R$,根据定义,有

  $$\exists i \geqslant 1 \cdot (\sigma_1(s_1), \sigma_1^i(t_1)) \in R.$$

  令 $t = \sigma_1^i(t_1)$,则$(s,t) \in R$.

  令 $\sigma_3 = \sigma_1^i(t_1)\sigma_2$,因为 G 是置换群,$\sigma_3 \in G$.因此有,

  $$t \in \sigma_3(t'), t \in \theta(t'), \theta(t) = \theta(t').$$

  根据 B 的定义,有$(t,\theta(t)) \in B$.因此,$(t,\theta(t')) \in B$.结果(c)成立. □

根据引理 1,有以下推论.

推论 1. 设 M 为一个定义在原子命题集合 AP 上的 Kripke 结构,G 是 M 的循环对称置换群,M_G 是由 G 导出的 M 的商结构.如果 G 是 AP 的不变置换群,那么对任意的 CTL 公式φ,有

$$\forall s \in S \cdot M, s \models \varphi \Leftrightarrow M_G, \theta(s) \models \varphi.$$

根据推论 1,容易得到下面的定理.它表明,如果 G 对一个 CTL 公式φ中出现的原子命题保持不变,那么对φ的模型检测结果在 M 与商结构 M_G 上相对于对称关系相同.

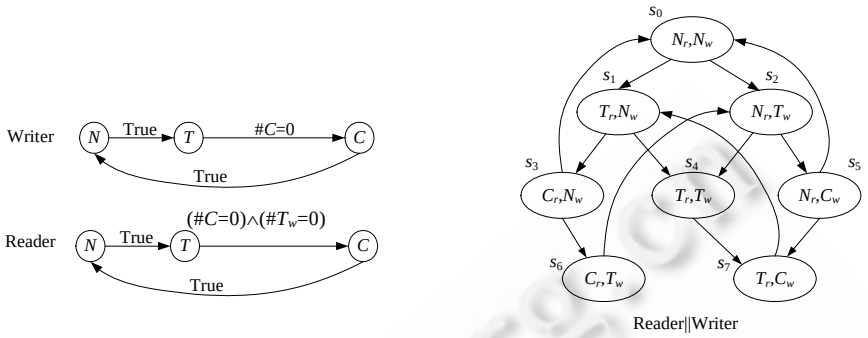
定理 4. 设 M 为一个定义在原子命题集合 AP 上的 Kripke 结构,G 是 M 的循环对称置换群,M_G 是由 G 导出的 M 的商结构.对于任意的 CTL 公式φ,如果 G 是φ中原子命题的不变置换群,那么有

$$\forall s \in S \cdot M, s \models \varphi \Leftrightarrow M_G, \theta(s) \models \varphi.$$

现在再次考虑图 1(c)所示的 Kripke 结构 M_2,以及置换群 $G=\langle (s_1,s_2)(s_3,s_4) \rangle$.$G$ 是 M_2 的循环对称置换群,同时也是原子命题 p 与 q 的不变置换群.例如,对于 M_2 中的迁移关系$(s_0,s_3) \in R$ 以及$\sigma=(s_1,s_2)(s_3,s_4)$,$M_2$ 存在着迁移关系$\sigma(s_0) \to \sigma^2(s_3)$,即 $s_0 \to s_3$;同样,对于迁移关系 $s_2 \to s_4$,M_2 中存在着迁移关系$\sigma(s_2) \to \sigma^2(s_4)$,即 $s_1 \to s_4$.由 G 所导出的 M_2 的商结构 M_{2G} 与 M_1 的商结构 M_{1G} 相同(如图 1(b)所示).M_{2G} 与 M_2 相对于对称关系互模拟,根据定理 4,对定义在命题 p 和 q 上的 CTL 公式的模型检测结果在 M_2 和 M_{2G} 上相同.

对于如图 2(a)所描述的读者-写者协议,由于读者与写者有相似的状态迁移关系,即空闲(N)→请求(T)→使用资源(C)→空闲(N),因此,系统的整体行为具有高度的相似性;但是,由于写者比读者有更高的访问关键资源的优先级,即当一个读者被允许访问关键资源的时候,除了要求当前没有进程访问关键资源(#C=0)之外,还要求当前没有写者请求访问关键资源(#T_w=0),因此,系统的整体行为并非完全对称.例如,考虑如图 2(b)所示的由一个读者和一个写者组成的并发系统,在状态 s_4,当读者和写者都请求访问关键资源的时候,由于写者有更高的优先级,因此系统中只允许从 s_4~s_7 的状态迁移,即只有写者可以被允许访问关键资源.

对于这种非对称的系统,如果要验证互斥属性,即关键资源在任何时刻最多只能被一个进程访问,虽然无法应用传统的对称化简方法,但可以采用循环对称化简.定义置换群 $G=\langle(s_1,s_2)(s_3,s_5)(s_6,s_7)\rangle$,容易证明,$G$ 是图 2(b)所示模型的循环对称置换群.令 $p=\neg(C_r\wedge C_w)$,则 G 是原子命题 p 的不变置换群.因此,对于 CTL 表示的互斥属性 AGp,在原模型上与在由 G 所导出的商结构上的模型检测结果相同.



(a) Reade-Writer protocol (a) 读者-写者协议

(b) An example composed of one reader and one writer (b) 由一个读者和一个写者组成的系统示例

Fig.2

图 2

由行为相似的进程组成的非对称系统往往是从相关的对称系统演变而得到的.例如,非对称的读者-写者协议从对称的互斥协议变化得到.造成进程间行为相似但并不完全相同的原因,通常是由于访问共享关键资源的进程具有不同的优先级和权限.在实际中,这种行为相似性可以由领域专家首先根据对进程的描述做出判断,然后考虑采用循环对称化简提高模型检测效率.

2.2 基于循环对称置换生成群的化简

本节进一步分析基于循环对称置换生成群的化简.我们证明在这种情况下,原模型与其商结构之间仍然保持互模拟关系.

定义 6. 一个置换群 $G=\langle g_1,g_2,\ldots,g_k\rangle$ 是 Kripke 结构 M 的循环对称生成群,当且仅当 G 中的每一个生成置换 $g_i(1\leqslant i\leqslant k)$ 都是 M 的循环对称置换.

循环对称置换生成群并不一定是循环对称群.这是因为即使两个置换 σ_1 和 σ_2 都是循环对称置换,他们的复合 $\sigma_1\sigma_2$ 也可能不满足循环对称性.所以,第 2.1 节的定理不适用于循环对称置换生成群.为此,我们证明下面的结果,说明由循环对称置换生成群所导出的商结构仍与原结构互模拟,可以用于对模型进行化简.

引理 2. 设 $M=(S,R,L)$ 为一个定义在原子命题集合 AP 上的 Kripke 结构,$G=\langle g_1,g_2,\ldots,g_k\rangle$ 是 S 上的置换群,其中每个生成置换 $g_i(1\leqslant i\leqslant k)$ 都是 M 的循环对称置换.令 $M_G=(S_G,R_G,L_G)$ 为由 G 导出的 M 的商结构.如果每个 g_i 同时也是 AP 的不变置换,那么定义关系 $B\subseteq S\times S_G$ 为 $\forall s\in S\cdot(s,\theta(s))\in B$,$B$ 是 M 与 M_G 之间的互模拟关系.

证明:我们根据互模拟的定义证明下列 3 个条件成立:

(a) $L(s)=L_G(\theta(s))$;

(b) $\forall t\in S\cdot(s,t)\in R\Rightarrow\exists t'\in S\cdot(\theta(s),\theta(t'))\in R_G\wedge(t,\theta(t'))\in B$;

(c) $\forall t'\in S\cdot(\theta(s),\theta(t'))\in R_G\Rightarrow\exists t\in S\cdot(s,t)\in R\wedge(t,\theta(t'))\in B$.

因为每一个生成置换 g_i 都是 AP 的不变置换,由它们复合而得到的置换也是 AP 的不变置换,因此条件(a)成立.条件(b)与引理 1 中的证明相似.

接下来证明条件(c)成立.考虑任意的 $t'\in S$ 使得 $(\theta(s),\theta(t'))\in R_G$.根据 R_G 的定义,有

$$\exists s_1\in S\cdot\exists t_1\in S\cdot(s_1,t_1)\in R\wedge s_1\in\theta(s)\wedge t_1\in\theta(t').$$

根据轨道的定义以及置换群的属性,有

$$\exists\sigma_1\in G\cdot s=\sigma_1(s_1),$$

以及

$$\exists\sigma_2\in G\cdot t_1=\sigma_2(t').$$

因为 G 是循环对称置换生成群,存在着 $n\geqslant 1$ 使得 $\sigma_1=g_{i_1}g_{i_2}...g_{i_n}$,其中,每个 $g_{i_m}(1\leqslant m\leqslant n)\in\{g_1,g_2,...,g_k\}$.因为每个生成置换 $g_i(1\leqslant i\leqslant k)$都是 M 的循环对称置换,对 $\sigma_1=g_{i_1}g_{i_2}...g_{i_n}$ 以及$(s_1,t_1)\in R$,有

$$\exists j_1\geqslant 1\cdot\exists j_2\geqslant 1\cdot\exists j_n\geqslant 1\cdot((g_{i_1}g_{i_2}...g_{i_n})(s_1),(g_{i_1}^{j_1}g_{i_2}^{j_2}...g_{i_n}^{j_n})(t_1))\in R.$$

令 $t=g_{i_1}^{j_1}g_{i_2}^{j_2}...g_{i_n}^{j_n}(t_1)$,有$(s,t)\in R$.

令 $\sigma_3=g_{i_1}^{j_1}g_{i_2}^{j_2}...g_{i_n}^{j_n}\sigma_2$.因为 G 是置换群,$\sigma_3\in G$.因此有

$$t\in\sigma_3(t'),t\in\theta(t'),\theta(t)=\theta(t').$$

根据 B 的定义,有$(t,\theta(t))\in B$.因此,$(t,\theta(t'))\in B$.所以,条件(c)成立. □

与第 2.1 节类似,由引理 2,我们可以得到下列结果.

推论 2. 设 $M=(S,R,L)$为一个定义在原子命题集合 AP 上的 Kripke 结构,$G=\langle g_1,g_2,\ldots,g_k\rangle$是 S 上的置换群,其中每个生成置换 $g_i(1\leqslant i\leqslant k)$都是 M 的循环对称置换.令 $M_G=(S_G,R_G,L_G)$为由 G 导出的 M 的商结构.如果每个 g_i 同时也是 AP 的不变置换,那么对任意的 CTL 公式φ,有

$$\forall s\in S\cdot M,s\vDash\varphi\Leftrightarrow M_G,\theta(s)\vDash\varphi.$$

定理 5. 设 $M=(S,R,L)$为一个定义在原子命题集合 AP 上的 Kripke 结构,$G=\langle g_1,g_2,\ldots,g_k\rangle$是 S 上的置换群,其中每个 $g_i(1\leqslant i\leqslant k)$都是 M 的循环对称置换.令 $M_G=(S_G,R_G,L_G)$为由 G 导出的 M 的商结构.对于任意的 CTL 公式,如果每个 g_i 都是φ中出现的原子命题的不变置换,那么有

$$\forall s\in S\cdot M,s\vDash\varphi\Leftrightarrow M_G,\theta(s)\vDash\varphi.$$

3 对称化简与三值模型

本节研究三值 Kripke 结构上的对称化简.我们首先将传统的对称化简以及本文定义的循环对称化简扩展到三值模型上.通过分析三值模型以及商结构之间的精化关系,我们证明三值模型检测可以在商结构上获得与原模型相同的结果.另外,从每一个三值模型可以约简导出两个二值模型,分别表示原模型中确定和可能的行为.通过分析三值模型上的对称化简与这两个二值模型上的对称化简之间的关系,证明了这两种途径的等价性.

3.1 三值模型的对称化简

首先定义三值模型上的不变置换和自同构置换.

定义 7. 设 $M=(S,R,L)$为一个定义在原子命题集合 AP 上的三值 Kripke 结构.S 上的置换σ是原子命题 $p\in AP$ 的不变置换,当且仅当下列条件成立:

$$\forall s\in S\cdot L(s,p)=L(\sigma(s),p).$$

M 的置换群 G 是 CTL 公式φ的不变置换群,当且仅当 G 中的每一个置换σ都是φ中出现的原子命题的不变置换.

定义 8. 三值 Kripke 结构 $M=(S,R,L)$上的置换σ是 M 的自同构置换,当且仅当σ保持迁移关系 R 的值,即下列条件成立:

$$\forall s_1\in S\cdot\forall s_2\in S\cdot R(s_1,s_2)=R(\sigma(s_1),\sigma(s_2)).$$

G 是三值结构 M 的自同构置换群,当且仅当 G 中的每一个置换σ都是 M 的自同构置换.注意,对于三值逻辑,由于 $m\Leftrightarrow m$ 并不为真,所以在上述定义中,我们采用相等关系(=)而不是逻辑等价关系(⇔)来表示σ对原子命题和迁移关系保持不变.

下面定义三值模型的商结构.设 $M=(S,R,L)$是一个定义在原子命题集合 AP 上的三值 Kripke 结构,G 是 M 上的置换群.由 G 所导出的 M 的商结构 $M_G=(S_G,R_G,L_G)$定义如下:

- $S_G=\{\theta(s)|s\in S\}$;

- $R_G:S_G\times S_G\to\{t,m,f\}$,其中,对于任意的 $s,t\in S$:
  (1) $R_G(\theta(s),\theta(t))\triangleq t$,当且仅当
  $$\exists s'\in\theta(s)\cdot\exists t'\in\theta(t)\cdot R(s',t')=t.$$
  (2) $R_G(\theta(s),\theta(t))\triangleq m$,当且仅当条件(1)不成立,并且
  $$\exists s'\in\theta(s)\cdot\exists t'\in\theta(t)\cdot R(s',t')=m.$$
  (3) $R_G(\theta(s),\theta(t))\triangleq f$,当且仅当条件(1)与条件(2)都不成立;
- $L_G:S_G\times AP\to\{t,m,f\}$定义为
  $$\forall s\in S\cdot\forall p\in AP\cdot L_G(\theta(s),p)\triangleq L(rep(\theta(s),p)).$$

接下来证明,当 G 是 M 的自同构置换群并且是 CTL 公式φ中出现的原子命题的不变置换群时,M 与 M_G 互为对方的精化,因此对φ的模型检测结果在 M 与 M_G 上相同.

引理 3. 设 $M=(S,R,L)$为定义在原子命题集合 AP 上的三值 Kripke 结构,G 是 M 的自同构置换群,并且是 AP 的不变置换群.令 $M_G=(S_G,R_G,L_G)$为由 G 导出的 M 的商结构.定义关系$\rho\subseteq S_G\times S$ 为$\forall s\in S\cdot(\theta(s),s)\in\rho$.那么 $M\preceq_\rho M_G$ 并且 $M_G\preceq_{\rho^{-1}}M$.

证明:我们给出 $M\preceq_\rho M_G$ 的证明.根据精化关系的定义,对于任意的$(\theta(s),s)\in\rho$,证明下列条件成立:

(a) $\forall p\in AP\cdot L(s,p)\preceq L_G(\theta(s),p)$;

(b) $\forall s'\in S\cdot R(s,s')=t\Rightarrow\exists t'\in S\cdot R_G(\theta(s),\theta(t'))=t\wedge(\theta(t'),s')\in\rho$;

(c) $\forall t'\in S\cdot R_G(\theta(s),\theta(t'))\geqslant m\Rightarrow\exists s'\in S\cdot R(s,s')\geqslant m\wedge(\theta(t'),s')\in\rho$.

因为 G 是 AP 的不变置换群,容易证明条件(a)成立.

再证明条件(b)成立.考虑任意的 $s'\in S$ 使得 $R(s,s')=t$.根据 R_G 的定义,有 $R_G(\theta(s),\theta(s'))=t$.

又根据ρ的定义,$(\theta(s'),s')\in\rho$.令 $t'=s'$,则条件(b)成立.

最后证明条件(c)成立.考虑任意的 $t'\in S$,使得 $R_G(\theta(s),\theta(t'))\geqslant m$.

如果 $R_G(\theta(s),\theta(t'))=t$,那么根据 R_G 的定义,有
$$\exists s_1\in S\cdot\exists t_1\in S\cdot R(s_1,t_1)=t\wedge s_1\in\theta(s)\wedge t_1\in\theta(t').$$
根据轨道的定义,有$\exists\sigma\in G\cdot s=\sigma_2(s_1)$.

因为 G 是 M 的自同构群,有 $R(\sigma(s_1),\sigma(t_1))$=t.令 $s'=\sigma(t_1)$,有 $R(s,s')$=t.

因为 $t_1\in\theta(t')$,根据轨道的定义,$s'\in\theta(t')$,并且$\theta(s')\in\theta(t')$.又根据ρ的定义,$(\theta(s'),s')\in\rho$.因此,$(\theta(t'),s')\in\rho$.

所以,当 $R_G(\theta(s),\theta(t'))=t$ 时,条件(c)成立.同理可证,当 $R_G(\theta(s),\theta(t'))=m$ 时,条件(c)也成立.

因此,$M\preceq_\rho M_G$ 成立. $M_G\preceq_{\rho^{-1}}M$ 的证明与此相似. □

根据引理 3,容易得到下面的结果.

推论 3. 设 $M=(S,R,L)$为定义在原子命题集合 AP 上的三值 Kripke 结构,G 是 M 的自同构置换群,并且是 AP 的不变置换群,$M_G=(S_G,R_G,L_G)$是由 G 导出的 M 的商结构.对于任意的 CTL 公式φ,有
$$\forall s\in S\cdot\|\varphi\|^M(s)=\|\varphi\|^{M_G}(\theta(s)).$$

定理 6. 设 $M=(S,R,L)$为定义在原子命题集合 AP 上的三值 Kripke 结构,G 是 M 的自同构置换群,$M_G=(S_G,R_G,L_G)$是由 G 导出的 M 的商结构.对于任意的 CTL 公式φ,如果 G 是φ中出现的原子命题的不变置换群,那么有
$$\forall s\in S\cdot\|\varphi\|^M(s)=\|\varphi\|^{M_G}(\theta(s)).$$

与传统对称化简在二值 Kripke 结构上存在的问题相同,自同构由于要求置换必须保持原有的迁移关系不变这种过强的条件,而无法应用于更多的非完全对称的三值模型上.例如,对于如图 3(a)所示的三值模型 M_3 以及置换群 $G=\langle(s_1,s_2)(s_3,s_4)\rangle$,由于 G 不是 M_3 的自同构置换,因此不能根据上述结果使用 G 对 M_3 化简.第 2.1 节定义了循环对称化简,它放宽了传统的对称化简要求自同构的条件,因此可以用于非对称模型的化简.接下来,我们将循环对称化简扩展到三值模型上.

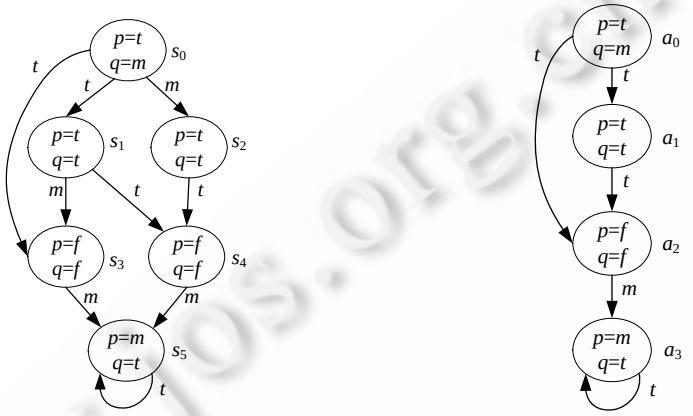
首先将循环对称置换的定义扩展到三值 Kripke 结构上.

定义 9. 三值 Kripke 结构 $M=(S,R,L)$上的置换σ是 M 的循环对称置换,当且仅当对任意的 $s_1,s_2\in S$,下列条件成立:

$$(R(s_1,s_2)=t\Rightarrow\exists i\geqslant 1\cdot R(\sigma(s_1),\sigma^i(s_2))=t)\wedge(R(s_1,s_2)=m\Rightarrow\exists i\geqslant 1\cdot R(\sigma(s_1),\sigma^i(s_2))\geqslant m).$$

根据定义,如果σ是 M 的循环对称置换,那么对于 M 中的两个状态 s_1 与 s_2,如果从 s_1 有一个为真的迁移关系到 s_2,那么经过对σ的 i 次复合,在 M 中也存在着从$\sigma(s_1)$到$\sigma^i(s_2)$的为真的迁移关系;如果从 s_1 到 s_2 的迁移关系为可能,那么在 M 中存在着可能或者为真的从$\sigma(s_1)$到$\sigma^i(s_2)$的迁移关系.

与二值模型上的定义类似,三值 Kripke 结构 M 上的置换群 G 是 M 的循环对称置换群,当且仅当每个$\sigma\in G$都是 M 的循环对称置换;$G=\langle g_1,g_2,\ldots,g_k\rangle$是 M 的循环对称生成群,当且仅当每个生成置换 $g_i(1\leqslant i\leqslant k)$都是 M 的循环对称置换.



(a) A three-valued Kripke structure M_3 (b) M_{3G}: The quotient structure of M_3

(a) 三值 Kripke 结构 M_3 (b) M_{3G}: M_3 的商结构

Fig.3

图 3

与上一节的方法相似,我们可以证明下列定理,将循环对称化简扩展到三值 Kripke 结构上.

定理 7. 设 $M=(S,R,L)$为一个定义在原子命题集合 AP 上的三值 Kripke 结构,G 是 M 的循环对称置换群,$M_G=(S_G,R_G,L_G)$是由 G 导出的 M 的置换群.对于 CTL 公式φ,如果 G 是φ中出现的命题的不变置换群,那么对于 $s\in S$,φ在 M 中的 s 上和 M_G 中的$\theta(s)$上的模型检测结果相同,即

$$\forall s\in S\cdot\|\varphi\|^M(s)=\|\varphi\|^{M_G}(\theta(s)).$$

定理 8. 设 $M=(S,R,L)$为一个定义在原子命题集合 AP 上的三值 Kripke 结构,$G=\langle g_1,g_2,\ldots,g_k\rangle$是 M 的循环对称置换生成群,$M_G=(S_G,R_G,L_G)$是由 G 导出的 M 的商结构.对于 CTL 公式φ,如果 G 中每个生成置换 $g_i(1\leqslant i\leqslant k)$都是$\varphi$中出现的命题的不变置换群,那么对任意的 $s\in S$,φ在 M 中 s 上与 M_G 中$\theta(s)$上的模型检测结果相同,即

$$\forall s\in S\cdot\|\varphi\|^M(s)=\|\varphi\|^{M_G}(\theta(s)).$$

例如,对于如图 3(a)所示的模型 M_3 以及置换群 $G=\langle(s_1,s_2)(s_3,s_4)\rangle$,容易证明 G 是 M_3 的循环对称置换群,并且是命题 p 和 q 的不变置换群.由 G 导出 M_3 的商结构如图 3(b)所示,其中,状态 a_0,a_1,a_2 和 a_3 分别对应轨道$\{s_0\}$,$\{s_1,s_2\}$,$\{s_3,s_4\}$和$\{s_5\}$.根据上述结果,对 CTL 公式在 M 和 M_G 上的模型检测结果相同.

3.2 对称化简与三值模型的约简

本节研究根据置换群 G 导出的三值模型 M 的商结构与由 M 约简得到的二值模型的商结构之间的关系.我们已经证明,无论 G 是自同构群、循环对称群还是循环对称生成群,模型与其商结构之间都存在着相同的精化关系.因此在本节中,我们对置换群的类型不作具体区分.

对一个定义在原子命题集合 AP 上的三值 Kripke 结构 $M=(S,R,L)$,可以对其直接采用多值模型检测器进行验证[13],也可以从 M 中约简导出的两个二值 Kripke 结构 $M^{\geqslant t}$ 和 $M^{\geqslant m}$,用传统的二值模型检测器进行验证[14]. $M^{\geqslant t}$ 和 $M^{\geqslant m}$ 分别表示了 M 中的确定和可能的行为,对其定义为

$$M^{\geqslant t}=(S,L^{\geqslant t},R^{\geqslant t}),M^{\geqslant m}=(S,L^{\geqslant m},R^{\geqslant m}),$$

其中,对于任意的 $s_1,s_2\in S,p\in AP$ 以及 $v\in\{t,m\}$,定义

$$L^{\geqslant v}(s_1,p)\triangleq L(s_1,p)\geqslant v,R^{\geqslant v}(s_1,s_2)\triangleq R(s_1,s_2)\geqslant v.$$

例如,对于图 3(a)所示的三值模型 M_3,由它约简可以得到两个二值模型 $M_3^{\geqslant t}$ 和 $M_3^{\geqslant m}$,分别如图 4(a)和图 4(b)所示.

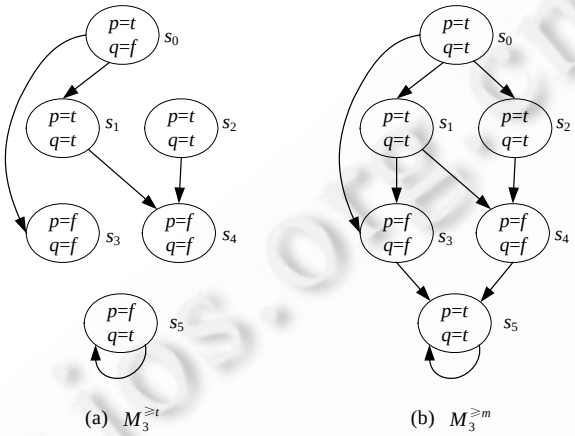


Fig.4 Two Boolean models reduced from M_3

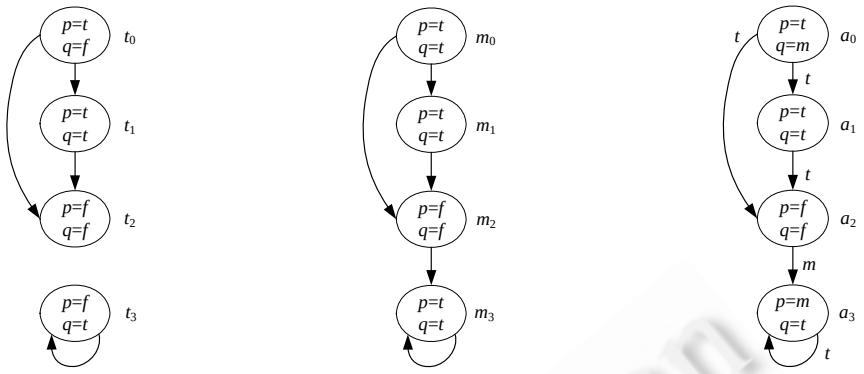
图 4 由 M_3 约简得到的两个二值模型

给定 M 上的置换群,二值模型 $M^{\geqslant t}$ 和 $M^{\geqslant m}$ 具有相同的状态空间.根据第 1.2 节的定义,我们可以分别构造由该置换群导出的 $M^{\geqslant t}$ 和 $M^{\geqslant m}$ 的商结构 $M_G^{\geqslant t}$ 和 $M_G^{\geqslant m}$.例如,对于对于置换群 $G=\langle(s_1,s_2)(s_3,s_4)\rangle$,根据商结构的定义,我们可以得到由 G 导出的 $M_3^{\geqslant t}$ 和 $M_3^{\geqslant m}$ 的商结构 $M_{3G}^{\geqslant t}$ 和 $M_{3G}^{\geqslant m}$ (分别如图 5(a)和图 5(b)所示).

$M_G^{\geqslant t}$ 和 $M_G^{\geqslant m}$ 定义在相同的轨道集合,所以具有相同的状态空间.我们可以将它们合并为一个三值结构,合并结构的状态空间与 $M_G^{\geqslant t}$ 和 $M_G^{\geqslant m}$ 的状态空间相同.其中的迁移关系定义如下:对任意的轨道状态 θ_1 和 θ_2,从 θ_1 到 θ_2 的迁移关系的值为:

- 真(t):当且仅当 $M_G^{\geqslant t}$ 和 $M_G^{\geqslant m}$ 中都存在从 θ_1 到 θ_2 的迁移关系;
- 可能(m):当且仅当 $M_G^{\geqslant t}$ 和 $M_G^{\geqslant m}$ 中只有一个模型存在从 θ_1 到 θ_2 的迁移关系;
- 假(f):当且仅当 $M_G^{\geqslant t}$ 和 $M_G^{\geqslant m}$ 中都不存在从 θ_1 到 θ_2 的迁移关系.

对于合并结构的标注函数,可以用类似的方法定义.例如,$M_{3G}^{\geqslant t}$ 和 $M_{3G}^{\geqslant m}$ 合并后的三值结构如图 5(c)所示.容易看出,该三值结构与图 3(b)中所示的由 G 导出的 M_3 的商结构相同.事实上,上述的先对一个三值模型进行约简,然后构造相应的两个二值模型的商结构,最后再合并的过程,与第 3.1 节中直接对三值模型构造商结构的过程是等价的(如图 6 所示).



(a) $M_{3G}^{\geqslant t}$: The quotient structure of $M_3^{\geqslant t}$ (b) $M_{3G}^{\geqslant m}$: The quotient structure of $M_3^{\geqslant m}$ (c) The combination of $M_{3G}^{\geqslant t}$ and $M_{3G}^{\geqslant m}$

(a) $M_3^{\geqslant t}$ 的商结构 $M_{3G}^{\geqslant t}$ (b) $M_3^{\geqslant m}$ 的商结构 $M_{3G}^{\geqslant m}$ (c) $M_{3G}^{\geqslant t}$ 与 $M_{3G}^{\geqslant m}$ 的合并

Fig.5

图 5

Fig.6 Direct construction of M_G vs. combination of $M_G^{\geqslant t}$ and $M_G^{\geqslant m}$

图 6 直接构造 M_G 与合并 $M_G^{\geqslant t}$ 和 $M_G^{\geqslant m}$ 之间的关系

下面的结果总结了上述分析过程.

定理 9. 设 $M=(S,R,L)$为一个定义在原子命题集合 AP 上的三值 Kripke 结构,G 是 M 的置换群,$M_G=(S_G,R_G,L_G)$ 是由 G 导出的 M 的商结构, $M_G^{\geqslant t}$ 和 $M_G^{\geqslant m}$ 分别是由 G 导出的 $M_G^{\geqslant t}$ 和 $M_G^{\geqslant m}$ 的商结构.如果 G 是 AP 的不变置换群,那么 M_G 是 $M_G^{\geqslant t}$ 与 $M_G^{\geqslant m}$ 的合并.

证明:设 $M_G^{\geqslant t}=(S_G^{\geqslant t},R_G^{\geqslant t},L_G^{\geqslant t}),M_G^{\geqslant M}=(S_G^{\geqslant m},R_G^{\geqslant m},L_G^{\geqslant m}),M_G^{\geqslant t}$ 与 $M_G^{\geqslant m}$ 的合并结构为 $M'_G=(S'_G,R'_G,L'_G)$.

我们来证明 $M_G=M'_G$.

首先,根据商结构定义, $M_G,M_G^{\geqslant t},M_G^{\geqslant M}$ 与 $M_G^{\geqslant m}$ 的轨道状态空间相同.因此, $S_G=S_G^{\geqslant t}=S_G^{\geqslant m}$.根据合并结构的定义, $S_G=S'_G$.

再证明 $L_G=L'_G$.对任意的 $\theta_G\in S_G$,令 $\theta'_G,\theta_G^{\geqslant t}$ 和 $\theta_G^{\geqslant m}$ 分别为 $S'_G,S_G^{\geqslant t}$ 和 $S_G^{\geqslant t}$ 中与之相对应的轨道状态.

对于任意的 $p\in AP$,如果 $L_G(\theta_G,p)=t$,因为 G 是 AP 的不变置换群,所以对 $s\in\theta_G$,有 $L(s,p)=t$.

然后,根据 $L^{\geqslant t}$ 和 $L^{\geqslant M}$ 的定义,有

$$L_G^{\geqslant t}(\theta_G^{\geqslant t},p)=t,L_G^{\geqslant m}(\theta_G^{\geqslant m},p)=t.$$

因此,

$$L'_G(\theta'_G,p)=t=L_G(\theta_G,p).$$

同样,如果 $L_G(\theta_G,p)=m$,则有

$$L_G^{\geqslant t}(\theta_G^{\geqslant t},p)=f,L_G^{\geqslant m}(\theta_G^{\geqslant m},p)=t.$$

所以,

$$L'_G(\theta'_G,p)=m=L_G(\theta_G,p).$$

$L_G(\theta_G,p)=f$ 的情况同理可证.因此, $L_G=L'_G$.

最后证明 $R_G = R'_G$.考虑 S_G 中任意的状态对 (θ_G^1,θ_G^2),令 $(\theta_G'^1,\theta_G'^2),(\theta_G^{1,\geqslant t},\theta_G^{2,\geqslant t}),(\theta_G^{1,\geqslant m},\theta_G^{2,\geqslant m})$ 分别为 $S'_G,S_G^{\geqslant t}$ 和 $S_G^{\geqslant m}$ 中与之相对应的状态对.

如果 $R_G(\theta_G^1,\theta_G^2)=t$,根据三值模型的商结构的定义,有

$$\exists s' \in \theta_G^1 \cdot \exists t' \in \theta_G^2 \cdot R(s',t') = t.$$

根据 $R^{\geqslant t}$ 和 $R^{\geqslant m}$ 的定义,有

$$R_G^{\geqslant t}(\theta_G^{1,\geqslant t},\theta_G^{2,\geqslant t}) = t,\ R_G^{\geqslant m}(\theta_G^{1,\geqslant m},\theta_G^{2,\geqslant m}) = t.$$

因此,

$$R'_G(\theta'^1_G,\theta'^2_G) = t = R_G(\theta_G^1,\theta_G^2).$$

同样,如果 $R_G(\theta_G^1,\theta_G^2)=m$,则有

$$R_G^{\geqslant t}(\theta_G^{1,\geqslant t},\theta_G^{2,\geqslant t}) = f, R_G^{\geqslant m}(\theta_G^{1,\geqslant m},\theta_G^{2,\geqslant m}) = t.$$

所以,

$$R'_G(\theta'^1_G,\theta'^2_G) = m = R_G(\theta_G^1,\theta_G^2).$$

$R_G(\theta_G^1,\theta_G^2)=f$ 的情况同理可证.因此,$R_G = R'_G$. □

4 相关工作

对称化简是一种解决对称系统中模型检测状态爆炸问题的有效方法.为了将对称化简扩展到非对称系统上,Emerson 等人首先定义了近似对称(near symmetry)以及粗糙对称(rough symmetry)[15],最后将其扩展为虚拟对称(virtual symmetry)[16].虚拟对称的基本思想是基于对给定的模型 M 和置换群 G 所导出的对称结构 M'的分析.对称结构 M'通过对 M 添加缺失的对称迁移关系而得到,使得 G 是 M 的自同构置换群.如果 M'中的迁移关系可以通过对 M 的迁移关系进行置换而得到,那么称 M'是 M 的虚拟对称.Emerson 等人证明,虚拟对称是保证一个模型与其商结构之间互模拟的最通用的条件.文献[17]进一步从抽象的角度对虚拟对称进行了刻画,并提出了自动判断并发系统中是否存在虚拟对称的方法.

虚拟对称基于一个置换群中的所有置换,也就是说,虚拟对称描述了一个置换群的整体属性.而在实际中,对称化简的过程常常首先由用户根据对系统的观察提供一组置换,然后根据这组置换所生成的置换群进行对称化简[18].与虚拟对称不同,本文所提出的循环对称性基于单个置换所表现出的属性.由于放宽了传统对称化简中的自同构条件,循环对称可以用来帮助用户发现更多非对称系统中可用于对称化简的置换.

循环对称化简方法可以与其他验证步骤相结合提高模型检测效率.例如,对于带参系统的验证(PMCP),文献[19]提出对采用特定描述方式定义的带参系统的验证可以归约为对由一定上界内的进程组成的有限系统的验证,如对带参的读者-写者协议系统的验证可以转化为对一定数量的读者和写者进程组成的系统的验证.由于这种有限系统是由具有相似的行为状态变化的进程所组成,因此可以通过进一步采用对称化简降低模型的复杂度,提高模型检测的效率.

本文研究的对称化简基于单一的置换群,这个置换群作用于模型中所有的迁移关系.文献[20,21]放宽了这一条件,考虑与迁移关系相关的对称化简.在这种情况下,用于对称化简的置换群可以根据不同的迁移关系而动态地改变,从而允许采用不同的置换群以获得更好的对原系统的状态空间的简化.另一方面,为保证能够在商结构上对所有的 CTL 公式都能获得与原模型相同的模型检测结果,我们要求商结构与原模型之间存在着互模拟的关系.文献[22]放宽了置换对所有的迁移关系本身保持不变的条件,仅要求置换对所有迁移关系的闭包(closure)保持不变,称这种对称性为体系结构对称(architectural symmetry).这种情况下所得到的商结构与原模型之间并不一定存在互模拟关系,但是对可达性的分析在商结构上仍可以获得与原模型相同的结果.由于许多实际中的问题可以归结为对可达性的分析,因此,采用体系结构对称可以在无法适用传统的对称化简时获得对系统的简化.

由于多值模型可以有效地表示系统的不完备或者不确定信息[12,13,23],与传统的二值模型相比,更适用于在

逐步求精的软件开发过程的应用,以及对软件系统从不同角度的建模分析,因此,对多值模型的研究引起越来越多的关注.对于多值模型的验证,同样需要克服状态爆炸问题.文献[13]研究了多值模型的符号模型检测.文献[24]以抽象解释的理论为基础,研究了对给定模型定义最优抽象模型的方法,其结果适用于对多值模型的化简.文献[25]结合多值模型在软件产品线中的应用,定义了通过合并系统状态以及多值逻辑中的逻辑值来构建多值模型的抽象模型的方法.文献[26]以双格(bilattice)为基础,提出了综合采用组合方式和抽象方法对多值模型进行验证的框架.本文研究了对称化简方法,通过对其进行扩展,将传统的以及新定义的循环对称化简应用于具体的多值模型——三值模型.据我们所知,这是首次将对称化简方式应用到对多值模型的验证分析上.

5 总 结

状态爆炸问题是模型检测研究中的一个最根本的问题.对于并发系统,由于常常存在着行为相似的组成部分,因此可以根据状态之间的对称性来减少模型检测所需要搜索的状态空间,提高模型检测的效率和扩大其应用范围.为了将对称化简应用于更多的非对称系统,我们定义了一种新的对称性,称为循环对称.我们证明,采用循环对称置换群得到的商结构与原模型之间仍然存在互模拟关系.同时,我们也研究了由一组循环对称置换所生成的置换群,证明在这种情况下,同样可以对系统进行对称化简.这些结果拓展了传统的对称化简,有助于促进模型检测对并发系统的验证和分析.

已有的对称化简研究工作仅应用于传统的二值模型上.结合近年来对多值模型检测的研究,本文进一步将对称化简扩展到三值模型上.我们首先扩展了传统的对称化简,定义了构造三值模型的商结构的方法,证明原模型与商结构之间存在着互相精化的关系,因此可以获得相同的对 CTL 公式的模型检测结果.然后,将本文新定义的循环对称性扩展到三值模型上,同样证明了原模型与商结构之间的互相精化关系.最后研究了三值模型的商结构与约简得到的二值模型的商结构之间的关系,证明了两种途径的等价性.在未来的工作中,我们将考虑如何将对称化简与其他解决多值模型状态爆炸问题的方法相结合.例如对于符号模型检测,Clarke 等人已证明,直接采用符号方法进行对称化简往往需要构造随着系统规模呈指数增长的判定图[7],因此是不可行的.最近提出的符号计数抽象方法已被有效地用于对采用布尔程序描述的对称并发系统的验证[27],我们今后将结合本文的结果,研究如何将这种方法应用于多值模型所描述的系统上.另外,本文只考虑了三值模型上的对称化简.在下一步工作中,我们希望将这些结果扩展到通用的多值模型上.

References:

[1] Clarke EM, Grumberg O, Peled D. Model Checking. 4th ed., Cambridge: MIT Press, 1999.

[2] Lin HM, Zhang WH. Model checking: Theories, techniques and applications. Acta Electronica Sinica, 2002,30(z1):1907−1912 (in Chinese with English abstract).

[3] Cimatti A, Clarke E, Giunchiglia E, Giunchiglia F, Pistore M, Roveri M, Sebastiani R, Tacchella A. NuSMV 2: An OpenSource tool for symbolic model checking. In: Brinksma Ed, Larsen KG, eds. Proc. of the 14th Int'l Conf. on Computer Aided Verification (CAV 2002). LNCS 2404, Copenhagen: Springer-Verlag, 2002. 359−364. [doi: 10.1007/3-540-45657-0_29]

[4] Cousot P. The role of abstract interpretation in formal methods. In: Proc. of the 5th IEEE Int'l Conf. on Software Engineering and Formal Methods (SEFM 2007). London: IEEE Computer Society, 2007. 135−140. [doi: 10.1109/SEFM.2007.42]

[5] Pu F, Zhang W. Combining search space partition and abstraction for LTL model checking. Science in China (Series E): Information Sciences, 2007,37(12):1504−1520 (in Chinese with English abstract).

[6] Kahlon V, Wang C, Gupta A. Monotonic partial order reduction: An optimal symbolic partial order reduction technique. In: Bouajjani A, Maler O, eds. Proc. of the 21st Int'l Conf. on Computer Aided Verification (CAV 2009). LNCS 5643, Grenoble: Springer-Verlag, 2009. 398−413. [doi: 10.1007/978-3-642-02658-4_31]

[7] Clarke EM, Filkorn T, Jha S. Exploiting symmetry in temporal logic model checking. In: Courcoubetis C, ed. Proc. of the 5th Int'l Conf. on Computer-Aided Verification (CAV'93). LNCS 697, Elounda: Springer-Verlag, 1993. 450−461.

[8] Emerson EA, Sistla AP. Symmetry and model checking. In: Courcoubetis C, ed. Proc. of the 5th Int'l Conf. on Computer-Aided Verification (CAV'93). LNCS 697, Elounda: Springer-Verlag, 1993. 105−131. [doi: 10.1007/BF00625970]

[9] Miller A, Donaldson AF, Calder M. Symmetry in temporal logic model checking. ACM Computing Surveys, 2006,38(3):1−36. [doi: 10.1145/1132960.1132962]

[10] Godefroid P, Jagadeesan R. On the expressiveness of 3-valued models. In: Zuck LD, Attie PC, Cortesi A, Mukhopadhyay S, eds. Proc. of the 4th Int'l Conf. on Verification, Model Checking, and Abstract Interpretation (VMCAI 2003). LNCS 2575, New York: Springer-Verlag, 2003. 206−222. [doi: 10.1007/3-540-36384-X_18]

[11] Wei O, Gurfinkel A, Chechik M. Mixed transition systems revisited. In: Jones ND, Müller-Olm M, eds. Proc. of the 10th Int'l Conf. on Verification, Model Checking, and Abstract Interpretation (VMCAI 2009). LNCS 5403, Savannah: Springer-Verlag, 2009. 349−365. [doi: 10.1007/978-3-540-93900-9_28]

[12] Gruler A, Leucker M, Scheidemann KD. Modeling and model checking software product lines. In: Barthe G, de Boer FS, eds. Proc. of the 10th IFIP WG 6.1 Int'l Conf. on Formal Methods for Open Object-Based Distributed Systems (FMOODS 2008). LNCS 5051, Oslo: Springer-Verlag, 2008. 113−131. [doi: 10.1007/978-3-540-68863-1_8]

[13] Chechik M, Devereux B, Esterbrook S, Gurfinkel A. Multi-Valued symbolic model-checking. ACM Trans. on Software Engineering and Methodology, 2003,12(4):1−38. [doi: 10.1145/990010.990011]

[14] Gurfinkel A, Chechik M. Multi-Valued model checking via classical model checking. In: Amadio RM, Lugiez D, eds. Proc. of the 14th Int'l Conf. on Concurrency Theory (CONCUR 2003). LNCS 2761, Marseille: Springer-Verlag, 2003. 266−280. [doi: 10.1007/978- 3-540-45187-7_18]

[15] Emerson EA, Trefler RJ. From asymmetry to full symmetry: new techniques for symmetry reduction in model checking. In: Pierre L, Kropf T, eds. Proc. of the 10th Advanced Research Working Conf. on Correct Hardware Design and Verification Methods (CHARME'99). Bad Herrenalb: Springer-Verlag, 1999. 142−157. [doi: 10.1007/3-540-48153-2_12]

[16] Emerson EA, Havlicek JW, Trefler RJ. Virtual symmetry reduction. In: Proc. of the 15th Annual IEEE Symp. on Logic in Computer Science (LICS 2000). Santa Barbara: IEEE Computer Society, 2000. 121−131.

[17] Wei O, Gurfinkel A, Chechik M. Identification and counter abstraction for full virtual symmetry. In: Borrione D, Paul WJ, eds. Proc. of the 13th Advanced Research Working Conf. on Correct Hardware Design and Verification Methods (CHARME 2005). LNCS 3725, Saarbrücken: Springer-Verlag, 2005. 285−300.

[18] Barner S, Grumberg O. Combining symmetry reduction and under-approximation for symbolic model checking. Formal Methods in System Design, 2005,27(1-2):29−66. [doi: 10.1007/s10703-005-2246-x]

[19] Emerson EA, Kahlon V. Reducing model checking of the many to the few. In: McAllester D, ed. Proc. of the 17th Int'l Conf. on Automated Deduction (CADE 2000). LNAI 1831, Pittsburgh: Springer-Verlag, 2000. 236−254.

[20] Sistla AP, Wang XD, Zhou M. Checking extended CTL properties using guarded quotient structures. Formal Methods in System Design, 2007,31(3):197−219. [doi: 10.1007/s10703-007-0037-2]

[21] Wahl T. Adaptive symmetry reduction. In: Damm W, Hermanns H, eds. Proc. of the 19th Int'l Conf. on Computer Aided Verification (CAV 2007). LNCS 4590, Berlin: Springer-Verlag, 2007. 393−405. [doi: 10.1007/978-3-540-73368-3_43]

[22] Trefler RJ, Wahl T. Extending symmetry reduction by exploiting system architecture. In: Jones ND, Müller-Olm M, eds. Proc. of the 10th Int'l Conf. on Verification, Model Checking, and Abstract Interpretation (VMCAI 2009). LNCS 5403, Savannah: Springer-Verlag, 2009. 320−334. [doi: 10.1007/978-3-540-93900-9_26]

[23] Uchitel, S, Brunet, G, Chechik, M. Synthesis of partial behavior models from properties and scenarios. IEEE Trans. on Software Engineering, 2009,35(3):384−406. [doi: 10.1109/TSE.2008.107]

[24] Gurfinkel A, Wei O, Chechik M. Systematic construction of abstractions for model-checking. In: Emerson EA, Namjoshi KS, eds. Proc. of the 7th Int'l Conf. on Verification, Model-Checking, and Abstract Interpretation (VMCAI 2006). LNCS 3855, Charleston: Springer-Verlag, 2006. 381−397. [doi: 10.1007/11609773_25]

[25] Campetelli A, Gruler A, Leucker M, Thoma D. Don't know for multi-valued systems. In: Liu Z, Ravn AP, eds. Proc. of the 7th Int'l Symp. on Automated Technology for Verification and Analysis (ATVA 2009). LNCS 5799, Macao: Springer-Verlag, 2009. 289−305. [doi: 10.1007/978-3-642-04761-9_22]

[26] Meller Y, Grumberg O, Shoham S. A framework for compositional verification of multi-valued systems via abstraction-refinement. In: Liu Z, Ravn AP, eds. Proc. of the 7th Int'l Symp. on Automated Technology for Verification and Analysis (ATVA 2009). LNCS 5799, Macao: Springer-Verlag, 2009. 271−288. [doi: 10.1007/978-3-642-04761-9_21]

[27] Basler G, Mazzucchi M, Wahl T, Kroening D. Symbolic counter abstraction for concurrent software. In: Bouajjani A, Maler O, eds. Proc. of the 21st Int'l Conf. on Computer Aided Verification (CAV 2009). LNCS 5643, Grenoble: Springer-Verlag, 2009. 64–78. [doi: 10.1007/978-3-642-02658-4_9]

附中文参考文献:

[2] 林惠民,张文辉.模型检测:理论方法与应用.电子学报,2002,30(z1):1907–1912.

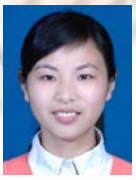
[5] 蒲飞,张文辉.结合搜索空间划分和抽象进行 LTL 模型检测.中国科学(E 辑),2007,37(12):1504–1520.

魏欧(1974－),男,山东曹县人,博士,副教授,主要研究领域为形式化方法,软件自动验证.

袁泳(1980－),男,博士生,主要研究领域为模型检测,软件验证.

蔡昕烨(1982－),男,博士,讲师,主要研究领域为软件工程,优化算法.

黄志球(1965－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为软件工程,可信软件.



徐丙凤(1986－),女,博士生,CCF 学生会员,主要研究领域为软件验证,形式化方法.