基于分解的多值模型的逼近关系

陈娟娟 魏 欧
(南京航空航天大学计算机科学与技术学院 南京 210016)

摘 要 多值模型可用于对包含不确定与不一致信息的软件系统进行建模与验证。提出了采用基于分解的方式来刻画多值模型之间的逼近关系,这为采用抽象方法解决模型检测时所产生的状态爆炸问题奠定了理论基础。为此,首先给出了多值模型分解为多个三值模型的方法,并且证明了任意 μ 演算公式在多值模型上的检测结果等于在分解后所有三值模型上的检测结果的合并。进一步,由三值模型上的混合模拟关系给出了多值模型间逼近关系的结构定义,并证明对于任意给定的两个满足逼近关系的多值模型,μ 演算公式在其上的检测结果在信息序关系上得以保持。

关键词 模型检测,多值模型,逼近关系,抽象
中图法分类号 TP301 **文献标识码** A

Approximation of Multi-valued Models via Reduction

CHEN Juan-juan WEI Ou
(College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)

Abstract Multi-valued model can be used for modeling and verification of software systems with uncertain and inconsistent information. In this paper, the approximation of multi-valued models was described by reducing, which provides the theoretical basis for solving the state-explosion problem. A new approach of decomposing the multi-valued model into several three-valued ones was proposed. The equality of the model-checking result of any μ-calculus formula on the multi-valued model and the union of that on the associated three-valued ones was strictly proves. Furthermore, the approximation of multi-valued models was defined based on the mixed simulation of the corresponding three-valued models, which preserves μ-calculus model-checking results with respect to information order.

Keywords Model checking, Multi-valued model, Approximation, Abstraction

1 引言

模型检测[1]是一种广泛应用的自动验证技术。一般来说,用户给定一个采用状态迁移系统定义的模型 K,并且给定一个时序逻辑属性 p;如果模型 K 满足属性 p,则模型检测器返回 true,反之返回 false。传统的模型检测定义在布尔模型上,即明确表示了系统中允许(true)与禁止(false)的动作。然而,在大型软件系统开发的过程中不可避免地涉及到不确定与不一致信息的处理。多值模型[2]是传统布尔模型的推广,与布尔模型相比,多值模型更适合对包含不确定和不一致信息的软件系统进行建模。

本文采用基于世界双格(world-based bilattice)[3]的多值逻辑作为对多值模型定义和分析的基础。例如,在软件开发过程中对某个功能的需求与否可以用命题 p 表示,假如用集合 W 表示所有用户群体,那么可以用有序对 $\langle U,V\rangle$ 来表示 p 的逻辑值,其中 U 与 V 都是 W 的子集,U 表示要求 p 为真的用户集,V 表示要求 p 为假的用户集。以此为基础构造出基于世界双格的多值逻辑,该逻辑包含两种序关系:真值序关系 $\leqslant_t$ 和信息序关系 $\leqslant_i$。例如:$\langle U_1,V_1\rangle\leqslant_t\langle U_2,V_2\rangle$ 表示 $\langle U_2,V_2\rangle$ 比 $\langle U_1,V_1\rangle$ 更真;$\langle U_1,V_1\rangle\leqslant_i\langle U_2,V_2\rangle$ 则表示 $\langle U_2,V_2\rangle$ 比 $\langle U_1,V_1\rangle$ 包含的信息量更多。三值逻辑,如 Kleene 逻辑[4],是特殊的多值逻辑。在这种情况下,可认为 W 中只包含一个用户 w,若某个功能的需求值为 $\langle\{w\},\varnothing\rangle$,则表示用户 w 认为需要这个功能,即为真;而若值为 $\langle\varnothing,\varnothing\rangle$ 则表示用户 w 没有表态,即为可能;类似地,若值为 $\langle\varnothing,\{w\}\rangle$,则表示用户 w 认为不需要这个功能,即为假。所以 $\langle\{w\},\varnothing\rangle$,$\langle\varnothing,\varnothing\rangle$,$\langle\varnothing,\{w\}\rangle$ 分别对应于三值逻辑中的 t(真),m(可能)和 f(假)。

为此,可以定义出基于世界分配双格上的三值模型。对三值模型的研究已日趋成熟,因此,可以将多值模型问题转换为三值模型问题进行研究。本文给出了多值模型分解为多个三值模型的方法,并且证明了任意的 μ 演算公式 φ 在多值模型 M 上的检测结果等于 φ 在 M 分解后的所有三值模型上的检测结果在信息序关系上的并($\oplus$)。

多值模型检测是对传统模型检测的扩展[2,5],与传统模型检测受制于状态爆炸问题相同,多值模型检测也面临着这个问题。抽象[6]是解决状态爆炸问题的一个重要方法,它的基本思想是首先构造一个比原系统的具体模型 M_C 小的有限抽象模型 M_A,然后通过属性在 M_A 上的检测结果推测出其在

到稿日期:2013-07-30 返修日期:2013-11-11 本文受国家自然科学基金项目(61170043,61100034)资助。
陈娟娟(1989—),女,硕士生,主要研究领域为模型检测、软件形式化验证,E-mail:juanjchen@nuaa.edu.cn;魏 欧(1974—),男,博士,副教授,主要研究领域为形式化方法、软件自动验证。

M_C 上是否可满足。M_C 与 M_A 之间的关系可以用逼近关系(approximation relation)来描述。在多值模型中,这种逼近关系可以通过要求模型检测结果保持信息序关系来定义,即要求公式 φ 在 M_C 上的检测结果比在 M_A 上的检测结果精确($\|\varphi\|^{M_A}\leqslant_i\|\varphi\|^{M_C}$)。

逼近关系作为抽象分析的基础对解决模型检测的状态爆炸问题有重要的意义。两个模型之间的逼近关系通常从模型的结构上对其进行刻画。对于三值模型,文献[6-8]提出了采用混合模拟关系(mixed simulation)来刻画逼近关系,并且被用于对软件代码的抽象模型检测中[9]。对于一般的多值模型,主要的已有工作是文献[11]所定义的以双格为多值逻辑基础的混合模拟关系,但是该定义存在着两个局限性:(1)它仅仅是确保两个多值模型间满足逼近关系的充分条件,而非必要条件;(2)此定义与三值模型上的结构刻画存在不一致;也就是说,当把此定义作用于三值模型上时,所得到混合模拟关系与文献[8]中的定义不相符合。

鉴于此,本文提出了一种采用基于分解的方式来刻画多值模型间的逼近关系,其主要思想是将多值模型问题转换为三值模型问题进行研究;首先将一个多值模型分别分解为多个三值模型,再由对应的三值模型间的逼近关系来刻画多值模型之间的逼近关系。为此,本文的主要工作包括:

1. 给出了多值模型分解为多个三值模型的方法,并且证明了 μ 演算公式在多值模型上的检测结果等于在分解后所有三值模型上检测结果的并($\oplus$);

2. 根据三值模型上的逼近关系对多值模型的逼近关系进行刻画,给出相应的定义,并证明此定义是多值模型间满足逼近关系的充分且必要条件。

本文第 2 节主要介绍了基于世界分配双格的多值模型以及 μ 演算在其上的语义;第 3 节提出了多值模型分解为三值模型的方法;第 4 节给出了多值模型上逼近关系的结构刻画;第 5 节讨论了相关工作;最后对本文作总结。

2 基本概念

这节主要介绍基于世界双格的多值模型以及 μ 演算公式在其上面的语义。

2.1 基于世界双格(world-based bilattice)

本文采用基于世界双格(world-based bilattice)[3]所定义的多值逻辑。在此逻辑中,逻辑值之间不仅存在真值序关系还存在信息序关系,因此,其既可以用来作为模型检测的结果,也可以用来表示信息的精确程度。

定义 1[3] 基于世界双格结构为 $\mathscr{B}_W=\langle B_W,\leqslant_t,\leqslant_i,\rightarrow\rangle$,其中 $B_W=P(W)\times P(W)$,对于任意的$\langle U,V\rangle,\langle S,T\rangle\in B_W$,以下条件成立:

1)$\langle U,V\rangle\leqslant_t\langle S,T\rangle\triangleq U\subseteq S\wedge T\subseteq V$

2)$\langle U,V\rangle\leqslant_i\langle S,T\rangle\triangleq U\subseteq S\wedge V\subseteq T$

3)$\neg\langle U,V\rangle\triangleq\langle V,U\rangle$

其中,W 为世界的集合,$P(W)$为 W 的幂集,有序对$\langle U,V\rangle$表示逻辑值,如果某个命题 p 的逻辑值为$\langle U,V\rangle$,则表示 p 在 U 这个集合的世界里都为真,在 V 这个集合的世界里都为假。为了与实际应用相一致,我们要求 $U\cap V=\varnothing$,即一个命题不可以同时在一个世界里既为真又为假,所以 $\mathscr{B}_W$ 中不包含形如$\langle\{\cdots a\cdots\},\{\cdots a\cdots\}\rangle$的逻辑值。其中$\leqslant_t$和$\leqslant_i$分别表示真值序关系与信息序关系。

下面分别给出基于真值序关系和信息序关系上的交(meet)和并(join)操作,其中$\wedge$、$\vee$对应于$\leqslant_t$序关系,$\otimes$、$\oplus$对应于$\leqslant_i$序关系。

定理 1[11] 设 $\mathscr{B}_W=\langle B_W,\leqslant_t,\leqslant_i,\rightarrow\rangle$,对于所有$\langle U,V\rangle$,$\langle S,T\rangle\in B_W$ 满足以下条件:

1)$\langle U,V\rangle\wedge\langle S,T\rangle=\langle U\cap S,V\cup T\rangle$

2)$\langle U,V\rangle\vee\langle S,T\rangle=\langle U\cup S,V\cap T\rangle$

3)$\langle U,V\rangle\otimes\langle S,T\rangle=\langle U\cap S,V\cap T\rangle$

4)$\langle U,V\rangle\oplus\langle S,T\rangle=\langle U\cup S,V\cup T\rangle$

定理 2[11] 设 $\mathscr{B}_W=\langle B_W,\leqslant_t,\leqslant_i,\rightarrow\rangle$,$\mathscr{B}_i=\langle B_W,\leqslant_i\rangle$,$\mathscr{B}_t=\langle B_W,\leqslant_t,\rightarrow\rangle$,则有下面 3 个条件成立:

1)$\mathscr{B}_i$ 中的$\otimes$和$\oplus$,以及 $\mathscr{B}_t$ 中的$\wedge$和$\vee$都相对于$\leqslant_i$和$\leqslant_t$单调;

2)$\otimes$和$\oplus$,$\wedge$和$\vee$相互满足分配律;

3)$\rightarrow$相对于$\leqslant_t$单调。

传统的三值(Kleene)逻辑是多值逻辑的一种特殊情况,也可以用基于世界双格的多值逻辑来表示。三值逻辑包含了 3 个逻辑值,即 t、f 和 m,分别表示为真(true)、假(false)和可能(maybe)。其中的真值序关系($\leqslant_t$)定义为 $f\leqslant_t m\leqslant_t t$,并且对所有值有 $x\leqslant_t x$;信息序关系($\leqslant_i$)定义为 $m\leqslant_i t$,$m\leqslant_i f$,并且对所有值有 $x\leqslant_i x$。对三值逻辑可以考虑只包含一个元素 w 的集合 W,则$\langle\{w\},\varnothing\rangle$、$\langle\varnothing,\{w\}\rangle$和$\langle\varnothing,\varnothing\rangle$分别与 t、f 和 m 相对应。

2.2 多值模型的定义与 μ 演算

下面给出基于世界双格的多值 Kripke 模型的定义,以及 μ 演算公式在多值模型上的语义。

定义 2[12] 一个多值 Kripke 模型是一个六元组 $M=\langle\mathscr{B}_W,AP,S,s_0,R,\Theta\rangle$,其中:

1)$\mathscr{B}_W=\langle B_W,\leqslant_t,\leqslant_i,\rightarrow\rangle$;

2)AP 为原子命题集合;

3)S 为有限状态集合;

4)s_0 为初始状态;

5)$R:S\times S\rightarrow B_W$ 为迁移到多值 B_W 上的映射;

6)$\Theta:AP\rightarrow(S\rightarrow B_W)$为标签函数。

定义 3[11] 设 AP 为原子命题集合,Var 为命题变量集合。μ 演算公式的定义如下:

$\varphi::=p|\neg\varphi|Z|\varphi_1\vee\varphi_2|\varphi_1\wedge\varphi_2|\Box\varphi|\Diamond\varphi|\mu Z.\varphi|\nu Z.\varphi$

其中,$p\in AP$,$Z\in Var$。

对于形如 $\mu Z.\varphi$ 和 $\nu Z.\varphi$ 的公式,Z 必须出现在偶数次非操作范围内。对于一个公式 φ,若变量 Z 出现在 μ 或 ν 范围内,则称 Z 为约束变量,否则称其为自由变量。若公式 φ 中不包含任何自由变量,则称其为封闭的,我们记满足上述约束的 μ 演算公式为 L_μ。

在 L_μ 中,环境 $V:Var\rightarrow(S\rightarrow B_W)$给出了自由变量的语义。对于变量 $Z\in Var$ 和映射 $l:S\rightarrow B_W$,我们用 $V[Z=l]$表示把 V 中 Z 的映射替换为 l 后得到的新环境。给定模型 M 和环境 V,公式 φ 的语义 $\|\varphi\|_V^M$ 是一个映射 $S\rightarrow B_W$,对 M 的每个状态 s 赋予 B_W 中的一个逻辑值,表示 φ 在 s 上的逻辑值。

μ 演算公式 φ 在多值 Kripke 模型 M 和环境 V 上的语义

如下[8]：

$\| p \|_V^M \triangleq \lambda s.\ \Theta(p)(s)$

$\| \neg p \|_V^M \triangleq \lambda s.\ \neg\Theta(p)(s)$

$\| \varphi_1 \vee \varphi_2 \|_V^M \triangleq \lambda s.\ \| \varphi_1 \|_V^M(s) \vee \| \varphi_2 \|_V^M(s)$

$\| \varphi_1 \wedge \varphi_2 \|_V^M \triangleq \lambda s.\ \| \varphi_1 \|_V^M(s) \wedge \| \varphi_2 \|_V^M(s)$

$\| \Diamond\varphi \|_V^M \triangleq \lambda s.\ \bigvee_{s' \in S}(R(s,s') \wedge \| \varphi \|_V^M(s'))$

$\| \Box\varphi \|_V^M \triangleq \lambda s.\ \bigwedge_{s' \in S}(\neg R(s,s') \vee \| \varphi \|_V^M(s'))$

$\| Z \|_V^M \triangleq V(Z)$

$\| \mu Z.\ \varphi \|_V^M \triangleq \mu(\lambda g.\ \| \varphi \|_{V[Z=g]}^M)$

$\| \nu Z.\ \varphi \|_V^M \triangleq \nu(\lambda g.\ \| \varphi \|_{V[Z=g]}^M)$

下面是处理 μ 演算公式中环境变量公式的定理[11]，为我们在第 4 节中的证明提供了基础。

定理 3[11]　对一个有限状态的多值模型 M，任意 μ 演算公式 φ 存在自然数 α 对任意的 $s \in S$，有 $\| \eta Z.\ \varphi \|_V^M(s) = Z^\alpha(s)$，其中 $\eta \in \mu, \nu$。

2.3　三值模型上的逼近关系的刻画

如前所述，三值模型也可以定义在 $\mathscr{B}_W$ 上，其中 $W=\{w\}$。相应地，R 与 Θ 定义在 $\mathscr{B}_W$ 上，即：$R: S\times S \to \{\langle\{w\},\emptyset\rangle, \langle\emptyset,\emptyset\rangle, \langle\emptyset,\{w\}\rangle\}$，$\Theta: S\times AP \to \{\langle\{w\},\emptyset\rangle, \langle\emptyset,\emptyset\rangle, \langle\emptyset,\{w\}\rangle\}$；同时，三值模型上的混合模拟关系亦可定义在 $\mathscr{B}_W$ 上。

定义 4[8]　设 $M_1=(\mathscr{B}_W, AP, S_1, s_{10}, R_1, \Theta_1)$ 与 $M_2=(\mathscr{B}_W, AP, S_2, s_{20}, R_2, \Theta_2)$ 为定义在原子命题集合 AP 上的两个基于 $\mathscr{B}_W$ 上的三值模型，其中 $W=\{w\}$。关系 $\rho \subseteq S_1 \times S_2$ 是 M_1 与 M_2 之间的混合模拟关系，当且仅当对任意 $s_1 \in S_1$，$s_2 \in S_2$，如果 $(s_1, s_2) \in \rho$，则下列条件成立：

1) $\forall p \in AP \cdot \Theta_2(p)(s_2) \leqslant_i \Theta_1(p)(s_1)$；

2) $\forall t_2 \in S_2 \cdot R_2(s_2, t_2) = \langle\{w\},\emptyset\rangle \Rightarrow \exists t_1 \in s_1 \cdot R_1(s_1, t_1) = \langle\{w\},\emptyset\rangle \wedge (t_1, t_2) \in \rho$；

3) $\forall t_1 \in S_1 \cdot \langle\emptyset,\emptyset\rangle \leqslant_t R_1(s_1, t_1) \Rightarrow \exists t_2 \in S_2 \cdot \langle\emptyset,\emptyset\rangle \leqslant_t R_2(s_2, t_2) \wedge (t_1, t_2) \in \rho$。

如果 M_1 中的初始状态 s_{10} 与 M_2 中的初始状态 s_{20} 满足 $(s_{10}, s_{20}) \in \rho$，则称 M_2 是 M_1 的模拟，记作 $M_2 \leqslant_\rho M_1$。

下面的定理说明满足混合模拟关系是三值模型间存在逼近关系的充分必要条件。

定理 4[8]　设 $M_1=(\mathscr{B}_W, AP, S_1, s_{10}, R_1, \Theta_1)$ 与 $M_2=(\mathscr{B}_W, AP, S_2, s_{20}, R_2, \Theta_2)$ 为定义在原子命题集 AP 上的两个基于 $\mathscr{B}_W$ 上的三值模型，其中 $W=\{w\}$。$\rho \subseteq s_1 \times s_2$ 是 M_1 与 M_2 之间的混合模拟关系，那么对于任意的 $\varphi \in L_\mu$，$(s_1, s_2) \in \rho$ 当且仅当 $\| \varphi \|^{M_2}(s_2) \leqslant_i \| \varphi \|^{M_1}(s_1)$。

也就是说，对于两个三值模型上的状态 s_2 和 s_1，它们满足混合模拟关系，当且仅当 φ 在它们上面对应的模型检测结果保持信息序关系，即如果 φ 在 s_2 上为 t 或者 f，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，那么它在 s_1 上可以为 t, f 或者 m。也即，三值模型上的混合模拟关系是模型间存在逼近关系的充分必要条件。因此三值模型上的混合模拟关系刻画了对应的逼近关系，这为我们下面研究一般多值模型间逼近关系的刻画奠定了基础。

3　多值模型的分解

因为多值模型与三值模型都可以定义在基于世界双格上，并且三值模型中的三值逻辑只包含一个世界，因此可以将三值逻辑作为多值逻辑的基本单位，进而将多值模型等价分解为多个三值模型。具体的分解方法定义如下：

定义 5　对于多值模型 $M=\langle\mathscr{B}_W, AP, S, s_0, R, \Theta\rangle$，$|W|=m$，可将 M 分解为 m 个三值模型 $\{M_{w_1}, \cdots, M_{w_i}, \cdots, M_{w_m}\}$，其中，对 $\forall w_i \in W$，三值模型 $M_{w_i}=\langle\mathscr{B}_{w_i}, AP, S_{w_i}, s_{0w_i}, R_{w_i}, \Theta_{w_i}\rangle$ 的定义如下：

1) $\mathscr{B}_{w_i}=\langle B_{w_i}, \leqslant_i, \leqslant_t, \neg\rangle$ 为 $\mathscr{B}_W$ 的一个子双格

2) $S_{w_i}=S$

3) $s_{0w_i}=s_0$

4) $R_{w_i}(s,t) \triangleq R(s,t) \otimes \langle\{w_i\},\{w_i\}\rangle$

5) $\Theta_{w_i}(p)(s) \triangleq \Theta(p)(s) \otimes \langle\{w_i\},\{w_i\}\rangle$

在上述定义中，条件 1) 保证了 $B_{w_i}=\{\langle\{w_i\},\emptyset\rangle, \langle\emptyset,\{w_i\}\rangle, \langle\emptyset,\emptyset\rangle\} \subseteq B_W$，并且 $\leqslant_i, \leqslant_t, \neg$ 分别与定义在 $\mathscr{B}_W$ 上的序关系与补操作一致，因此 $\mathscr{B}_{w_i}$ 上的 $\vee, \wedge, \oplus, \otimes$ 操作亦与 $\mathscr{B}_W$ 上对应的操作一致。由条件 4) 与 5) 易得：

$$R(s,t) = \bigoplus_{\forall w_i \in W} R_{w_i}(s,t) \qquad (*)$$

$$\Theta(p)(s) = \bigoplus_{\forall w_i \in W} \Theta_{w_i}(p)(s) \qquad (**)$$

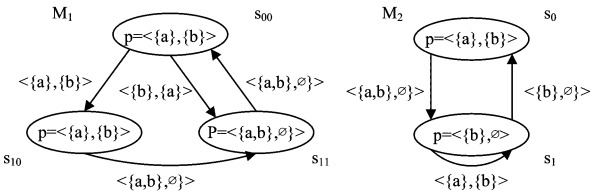
也即，多值模型上的迁移关系值（标签函数值）等于分解后所有三值模型上对应迁移关系值（标签函数值）在信息序关系下的并（$\oplus$）。

例如：对于图 1(a) 所示的基于 $W=\{a,b\}$ 的多值模型 M_1，根据定义 5，得到 M_1 分解后的三值模型为 M_{1a} 与 M_{1b}（分别如图 1(c) 与 (e) 所示），其中：

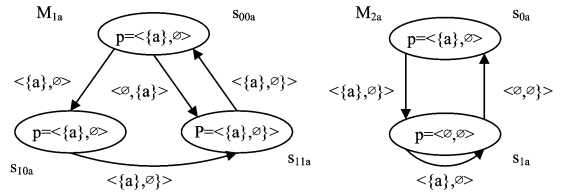
$\Theta_{1a}(p)(s_{00a}) = \Theta(p)(s_{00}) \otimes \langle\{a\},\{a\}\rangle = \langle\{a\},\emptyset\rangle$

$R_{1b}(s_{00b}, s_{11b}) = R(s_{00}, s_{11}) \otimes \langle\{b\},\{b\}\rangle = \langle\{b\},\emptyset\rangle$

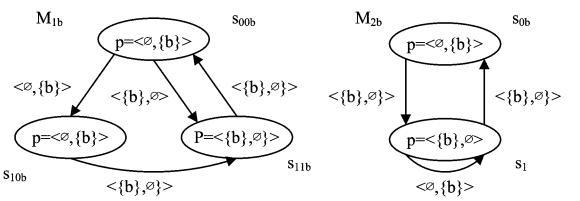
$R_1(s_{11}, s_{00}) = R_{1a}(s_{11a}, s_{00a}) \oplus R_{1b}(s_{11b}, s_{00b}) = \langle\{a,b\},\emptyset\rangle$



(a)基于世界W={a,b}双格多值模型M_1　(b)基于世界W={a,b}双格多值模型M_2



(c)M_1相对于a分解后的三值模型M_{1a}　(d) M_2相对于a分解后的三值模型M_{2a}



(e) M_1相对于b分解后的三值模型M_{1b}　(f) M_2相对于b分解后的三值模型M_{1b}

图 1　多值模型及分解示例

接下来证明，对于多值模型 M，任意 L_μ 公式 φ 在 M 上的检测结果等于 φ 在对 M 分解所得到的三值模型上的检测结果相对于信息序关系上的并（$\oplus$）。

定理 5　设 M 为定义在 $\mathscr{B}_W$ 上的多值模型，$|W|=m$，

$\{M_{w_1},\cdots,M_{w_i},\cdots,M_{w_m}\}$为将$M$分解后所得到的三值模型的集合，则对$M$中的任意状态$s$有：$\forall\varphi\in L_\mu\cdot\|\varphi\|^M(s)=\bigoplus_{\forall w_i\in W}\|\varphi\|^{M_{w_i}}(s)$。

证明：为了处理L_μ公式中子公式里的环境，我们将用下面的公式进行转化。设φ'为L_μ公式φ的子公式，记$\varphi'=\eta Z.\varphi(Z)$，其中$\eta\in\mu,\nu$。根据定理3，存在自然数$\alpha$使得$\|\varphi'\|^M(s)=Z^\alpha(s)$，这里的$Z^\alpha$是不包含变量$Z$的新公式。

对于任意给定的$\varphi\in L_\mu$，可以用上面的转换方法转换所有形如$\eta Z.\varphi(Z)$的子公式。这就得出了一个新的公式ϕ满足条件$\|\varphi\|^M(s)=\|\phi\|^M(s)$。进而，因为$\varphi$为一封闭的$\mu$演算公式，则$\phi$不含任何变量。

下面将对转换后的公式ϕ结构进行归纳来证明上面的定理。

归纳基础：

a)$\phi=p\in AP$

根据式$(**)$得$\|p\|^M(s)=\bigoplus_{\forall w_i\in W}\|p\|^{M_{w_i}}(s)$。

归纳步骤

b)$\phi=\neg\phi_1$

由定义可知：$\|\neg\phi_1\|^M(s)=\neg\|\phi_1\|^M(s)$，又由归纳假设可知：

$$\|\phi_1\|^M(s)=\bigoplus_{\forall w_i\in W}\|\phi_1\|^{M_{w_i}}(s)$$

所以有：

$$\neg\|\phi_1\|^M(s)=\neg\left(\bigoplus_{\forall w_i\in W}\|\phi_1\|^{M_{w_i}}(s)\right)$$

设$\|\phi_1\|^{M_{w_i}}(s)=\langle X_{w_i},Y_{w_i}\rangle$，则有：

$$\bigoplus_{\forall w_i\in W}\|\phi_1\|^{M_{w_i}}(s)=\bigoplus_{\forall w_i\in W}\langle X_{w_i},Y_{w_i}\rangle=\left\langle\bigcup_{\forall w_i\in W}X_{w_i},\bigcup_{\forall w_i\in W}Y_{w_i}\right\rangle$$

$$\neg\bigoplus_{\forall w_i\in W}\|\phi_1\|^{M_{w_i}}(s)=\left\langle\bigcup_{\forall w_i\in W}Y_{w_i},\bigcup_{\forall w_i\in W}X_{w_i}\right\rangle=\bigoplus_{\forall w_i\in W}\langle Y_{w_i},X_{w_i}\rangle=\bigoplus_{\forall w_i\in W}(\neg\langle X_{w_i},Y_{w_i}\rangle)=\bigoplus_{\forall w_i\in W}\neg\|\phi_1\|^{M_{w_i}}(s)=\bigoplus_{\forall w_i\in W}\|\neg\phi_1\|^{M_{w_i}}(s)$$

所以证得：

$$\neg\bigoplus_{\forall w_i\in W}\|\phi_1\|^{M_{w_i}}(s)=\bigoplus_{\forall w_i\in W}\|\neg\phi_1\|^{M_{w_i}}(s)$$

c)$\phi=\phi_1\wedge\phi_2$

由定义可知：$\|\phi_1\wedge\phi_2\|^M(s)=\|\phi_1\|^M(s)\wedge\|\phi_2\|^M(s)$，又因为$\phi_1,\phi_2$为公式$\phi_1\wedge\phi_2$的子公式，所以由归纳假设得：

$$\|\phi_1\wedge\phi_2\|^M(s)=\bigoplus_{\forall w_i\in W}\|\phi_1\|^{M_{w_i}}(s_{w_i})\wedge\bigoplus_{\forall w_i\in W}\|\phi_2\|^{M_{w_i}}(s_{w_i})$$

令$\|\phi_1\|^{M_{w_i}}(s)=\langle A_{w_i},B_{w_i}\rangle$，$\|\phi_2\|^{M_{w_i}}(s)=\langle C_{w_i},D_{w_i}\rangle$，则

$$\bigoplus_{\forall w_i\in W}\|\phi_1\|^{M_{w_i}}(s_{w_i})\wedge\bigoplus_{\forall w_i\in W}\|\phi_2\|^{M_{w_i}}(s_{w_i})=\bigoplus_{\forall w_i\in W}\langle A_{w_i},B_{w_i}\rangle\wedge\bigoplus_{\forall w_i\in W}\langle C_{w_i},D_{w_i}\rangle=\left\langle\bigcup_{\forall w_i\in W}A_{w_i},\bigcup_{\forall w_i\in W}B_{w_i}\right\rangle\wedge\left\langle\bigcup_{\forall w_i\in W}C_{w_i},\bigcup_{\forall w_i\in W}D_{w_i}\right\rangle$$

$$=\left\langle\left(\bigcup_{\forall w_i\in W}A_{w_i}\right)\cap\left(\bigcup_{\forall w_i\in W}C_{w_i}\right),\left(\bigcup_{\forall w_i\in W}B_{w_i}\right)\cup\left(\bigcup_{\forall w_i\in W}D_{w_i}\right)\right\rangle$$

$$=\left\langle\left[A_{w_1}\cap\left(\bigcup_{\forall w_i\in W}C_{w_i}\right)\right]\cup\cdots\left[A_{w_m}\cap\left(\bigcup_{\forall w_i\in W}C_{w_i}\right)\right],(B_{w_1}\cup D_{w_1})\cup\cdots(B_{w_m}\cup D_{w_m})\right\rangle\quad(1)$$

又因为$A_{w_i}\in P(\{w_i\})$，$C_{w_j}\in P(\{w_j\})$，其中$P(U)$表示集合U的幂集；若$i\neq j$，则$P(\{w_i\})\cap P(\{w_j\})=\emptyset$，也即$A_{w_i}\cap C_{w_j}=\emptyset$。所以

$$\text{式}(1)=\langle(A_{w_1}\cap C_{w_1})\cup\cdots(A_{w_m}\cap C_{w_m}),(B_{w_1}\cup D_{w_1})\cup\cdots(B_{w_1}\cup D_{w_1})\rangle=\bigoplus_{\forall w_i\in W}\langle A_{w_i}\cap C_{w_i},B_{w_i}\cup D_{w_i}\rangle=\bigoplus_{\forall w_i\in W}(\langle A_{w_i},B_{w_i}\rangle\wedge\langle C_{w_i},D_{w_i}\rangle)=\bigoplus_{\forall w_i\in W}(\|\phi_1\wedge\phi_2\|)^{M_{w_i}}(s_{w_i})$$

所以

$$\bigoplus_{\forall w_i\in W}\|\phi_1\|^{M_{w_i}}(s_{w_i})\wedge\bigoplus_{\forall w_i\in W}\|\phi_2\|^{M_{w_i}}(s_{w_i})=\bigoplus_{\forall w_i\in W}(\|\phi_1\wedge\phi_2\|)^{M_{w_i}}(s_{w_i})\quad(2)$$

所以$\|\phi_1\wedge\phi_2\|^M(s)==\bigoplus_{\forall w_i\in W}(\|\phi_1\wedge\phi_2\|)^{M_{w_i}}(s_{w_i})$。

d)$\phi=\phi_1\vee\phi_2$：证明与$\phi=\phi_1\wedge\phi_2$类似。

e)$\phi=\Diamond\phi_1$

由定义可知：$\|\Diamond\phi_1\|^M(s)=\bigvee_{t_k\in S}(R(s,t_k)\wedge\|\phi_1\|^M(t_k))$，根据式$(*)$且由归纳假设可知：$\|\phi_1\|^M(t_k)=\bigoplus_{\forall w_i\in W}\|\phi_1\|^{M_{w_i}}(t_k)$，所以有：

$$R(s,t_k)\wedge\|\phi_1\|^M(t_k)=\bigoplus_{\forall w_i\in W}R_{w_i}(s,t_k)\wedge\bigoplus_{\forall w_i\in W}\|\phi_1\|^{M_{w_i}}(t_k)\quad(3)$$

由式(2)可知：式(3)$=\bigoplus_{\forall w_i\in W}(R_{w_i}(s,t_k)\wedge\|\phi_1\|^{M_{w_i}}(t_k))$。令$R_{w_i}(s,t_k)\wedge\|\phi_1\|^{M_{w_i}}(t_k)=\langle E_{kw_i},F_{kw_i}\rangle$，所以

$$\bigvee_{t_k\in S}(R_{w_i}(s,t_k)\wedge\|\phi_1\|^{M_{w_i}}(t_k))=\bigvee_{k\in[1,n]}\left(\bigoplus_{\forall w_i\in W}\langle E_{kw_i},F_{kw_i}\rangle\right),i\in[1,m]\quad(4)$$

又因为$W=\{w_1,w_2,\cdots,w_m\}$，$|s|=n$，所以

$$\text{式}(4)=\bigvee_{k\in[1,n]}(\langle E_{kw_1},F_{kw_1}\rangle\oplus\cdots\oplus\langle E_{kw_m},F_{kw_m}\rangle)=\bigvee_{k\in[1,n]}\left\langle\bigcup_{\forall w_i\in W}E_{kw_i},\bigcup_{\forall w_i\in W}F_{kw_i}\right\rangle=\left\langle\left(\bigcup_{\forall w_i\in W}E_{1w_i}\right)\cup\cdots\cup\left(\bigcup_{\forall w_i\in W}E_{nw_i}\right),\left(\bigcup_{\forall w_i\in W}F_{1w_i}\right)\cap\cdots\cap\left(\bigcup_{\forall w_i\in W}F_{nw_i}\right)\right\rangle$$

$$=\left\langle\bigcup_{k\in[1,n]}(E_{kw_1})\cup\cdots\bigcup_{k\in[1,n]}(E_{kw_m}),\left(\bigcup_{k\in[1,n]}F_{kw_1}\right)\cap\cdots\cap\left(\bigcup_{k\in[1,n]}F_{kw_1}\right)\right\rangle\quad(5)$$

又因为当$i\neq j$时，$F_{w_i}\cap F_{w_j}=\emptyset$，所以

$$\text{式}(5)=\left\langle\left(\bigcup_{k\in[1,n]}E_{kw_1}\right)\cup\cdots\cup\left(\bigcup_{k\in[1,n]}E_{kw_m}\right),\left(\bigcap_{k\in[1,n]}F_{kw_1}\right)\cup\cdots\cup\left(\bigcap_{k\in[1,n]}F_{kw_m}\right)\right\rangle=\bigoplus_{\forall w_i\in W}\left\langle\bigcup_{k\in[1,n]}E_{kw_i},\bigcap_{k\in[1,n]}F_{kw_i}\right\rangle=\bigoplus_{\forall w_i\in W}\bigvee_{t_k\in S}\langle E_{kw_i},F_{kw_i}\rangle$$

所以

$$\bigvee_{t_k\in S}\left(\bigoplus_{\forall w_i\in W}R_{w_i}(s,t_k)\wedge\bigoplus_{\forall w_i\in W}\|\phi_1\|^{M_{w_i}}(t_k)\right)=\bigoplus_{\forall w_i\in W}\bigvee_{t_k\in S}(R_{w_i}(s,t_k)\wedge\|\phi_1\|^{M_{w_i}}(t_k))$$

所以 $\| \Diamond\phi_1 \|^{M}(s)=\bigoplus_{\forall w_i\in W} \| \Diamond\phi_1 \|^{M_{w_i}}(s)$。

f) $\phi=\Box\phi_1$：证明与 $\phi=\Diamond\phi_1$ 相似。

综上所述：

$\forall \phi\in L_\mu \cdot \| \phi \|^{M}(s)=\bigoplus_{\forall w_i\in W} \| \phi \|^{M_{w_i}}(s)$

定理 5 给出了一种求解公式 φ 在多值模型上检测结果的方法，例如，对于图 1(a)所示的多值模型 M_1，可分解为三值模型 M_{1a} 与 M_{1b}。属性 $\Diamond p$ 在 M_1，M_{1a} 与 M_{1b} 上的检测结果分别为：

$\| \Diamond p \|^{M_1}(s_{00})=(\langle\{a\},\{b\}\rangle \wedge \langle\{a\},\{b\}\rangle) \vee (\langle\{b\},\{a\}\rangle \wedge \langle\{a,b\},\emptyset\rangle)=\langle\{a,b\},\emptyset\rangle$

$\| \Diamond p \|^{M_{1a}}(s_{00a})=(\langle\{a\},\emptyset\rangle \wedge \langle\{a\},\emptyset\rangle) \vee (\langle\emptyset,\{a\}\rangle \wedge \langle\{a\},\emptyset\rangle)=\langle\{a\},\emptyset\rangle$

$\| \Diamond p \|^{M_{1b}}(s_{00b})=(\langle\emptyset,\{b\}\rangle \wedge \langle\emptyset,\{b\}\rangle) \vee (\langle\{b\},\emptyset\rangle \wedge \langle\{b\},\emptyset\rangle)=\langle\{b\},\emptyset\rangle$

所以有 $\| \Diamond p \|^{M_1}(s_{00})=\| \Diamond p \|^{M_{1a}}(s_{00a}) \oplus \| \Diamond p \|^{M_{1b}}(s_{00b})$。

根据定理 5，可以得到下面的推论。

推论 1 设 M 为定义在 $\mathscr{P}_W$ 上的多值模型，$|W|=m$，M 分解为 m 个三值模型 $\{M_{w_1}, M_{w_2}, \cdots, M_{w_i}, \cdots, M_{w_m}\}$，则对 M_{w_i} 中的任意状态 s 有：$\forall \varphi\in L_\mu \cdot \| \varphi \|^{M_{w_i}}(s)=\| \varphi \|^{M}(s) \otimes \langle\{w_i\},\{w_i\}\rangle$。

证明：由定理 5 可知 $\forall \varphi\in L_\mu \cdot \| \varphi \|^{M}(s)=\bigoplus_{\forall w_i\in W} \| \varphi \|^{M_{w_i}}(s)$，所以：

$$\begin{aligned}
&\| \varphi \|^{M}(s)\otimes\langle\{w_i\},\{w_i\}\rangle\\
&=(\bigoplus_{\forall w_i\in W} \| \varphi \|^{M_{w_i}}(s))\otimes\langle\{w_i\},\{w_i\}\rangle\\
&=(\| \varphi \|^{M_{w_1}}(s)\oplus\cdots \| \varphi \|^{M_{w_i}}(s)\oplus\cdots \| \varphi \|^{M_{w_m}}(s))\\
&\quad\otimes\langle\{w_i\},\{w_i\}\rangle\\
&=(\| \varphi \|^{M_{w_1}}(s)\otimes\langle\{w_i\},\{w_i\}\rangle)\oplus\cdots(\| \varphi \|^{M_{w_i}}(s)\otimes\\
&\quad\langle\{w_i\},\{w_i\}\rangle)\oplus\cdots(\| \varphi \|^{M_{w_m}}(s)\otimes\langle\{w_i\},\{w_i\}\rangle)
\end{aligned} \tag{6}$$

又因为 $\| \varphi \|^{M_{w_j}}(s)$ 中只包含元素 w_j，所以 $\| \varphi \|^{M_{w_j}}(s)\otimes\langle\{w_i\},\{w_i\}\rangle=\langle\emptyset,\emptyset\rangle(j\neq i)$，所以式(6)$=\| \varphi \|^{M_{w_i}}(s)\otimes\langle\{w_i\},\{w_i\}\rangle=\| \varphi \|^{M_{w_i}}(s)$，所以：

$\forall \varphi\in L_\mu \cdot \| \varphi \|^{M_{w_i}}(s)=\| \varphi \|^{M}(s)\otimes\langle\{w_i\},\{w_i\}\rangle$

例如，图 1 中 M_{1a} 为 M_1 分解后的一个三值模型，$\Diamond p$ 在 M_{1a} 与 M_1 上的检测结果分别为 $\| \Diamond p \|^{M_{1a}}(s_{00a})=\langle\{a\},\emptyset\rangle$，$\| \Diamond p \|^{M_1}(s_{00})=\langle\{a,b\},\emptyset\rangle$，则有 $\| \Diamond p \|^{M_{1a}}(s_{00a})=\| \Diamond p \|^{M_1}(s_{00})\otimes\langle\{a\},\{a\}\rangle$。

4 多值模型间的逼近关系

根据第 3 节的结果，一个多值模型可以相对于世界集合中的每一个元素分解成多个三值模型。基于此，可以考虑通过相应的三值模型之间的逼近关系来刻画多值模型间的逼近关系。简单而言，将两个多值模型分别分解为多个三值模型后，如果相应的三值模型之间存在逼近关系，则对任意的 L_μ 公式 φ，在三值模型上检测结果保持信息序关系；由于 φ 在多值模型上的模型检测结果可以由 φ 在三值模型上的检测结果的⊕运算得到，而⊕运算相对于信息序关系单调，因此可以推出 φ 在多值模型上的检测结果同样保持信息序关系，即多值模型之间存在逼近关系。对上述分析的严格描述和证明如下。

定理 6 设 M_1 与 M_2 都为定义在 $\mathscr{P}_W$ 上的多值模型，$|W|=m$，则 M_1，M_2 分别划分为 m 个三值模型。若 $\forall w_i\in W$，M_1 与 M_2 的划分分别为 M_{1w_i} 与 M_{2w_i}，则 $\forall w_i\in W$，M_{1w_i} 与 M_{2w_i} 满足三值上的精化关系当且仅当 $\forall \varphi\in L_\mu \cdot \| \varphi \|^{M_2}(s_{20})\leqslant_i \| \varphi \|^{M_1}(s_{10})$，其中 s_{10} 与 s_{20} 分别为 M_1 与 M_2 的初始状态。

证明：

(⇒)由定理 5 可知：$\forall \phi\in L_\mu$

$\| \phi \|^{M_1}(s_{10})=\bigoplus_{\forall w_i\in W} \| \phi \|^{M_{1w_i}}(s_{10})$

$\| \phi \|^{M_2}(s_{20})=\bigoplus_{\forall w_i\in W} \| \phi \|^{M_{2w_i}}(s_{20})$

由已知条件可知 $\forall w_i\in W$，M_{1w_i} 与 M_{2w_i} 满足三值上的精化关系。此条件等价于

$\forall w_i\in W \cdot \forall \varphi\in L_\mu \cdot \| \varphi \|^{M_{2w_i}}(s_{20})\leqslant_i \| \varphi \|^{M_{1w_i}}(s_{10})$

又因为 $\leqslant_i$ 相对于⊕单调，则 $\bigoplus_{\forall w_i\in W} \| \phi \|^{M_{2w_i}}(s_2)\leqslant_i \bigoplus_{\forall w_i\in W} \| \phi \|^{M_{1w_i}}(s_1)$，所以 $\| \phi \|^{M_2}(s_{20})\leqslant_i \| \phi \|^{M_1}(s_{10})$。

所以证得 $\forall \varphi\in L_\mu \cdot \| \varphi \|^{M_2}(s_{20})\leqslant_i \| \varphi \|^{M_1}(s_{10})$。

(⇐)由推论 1 知：

$\forall \varphi\in L_\mu \cdot \| \varphi \|^{M}(s)\otimes\langle\{w_i\},\{w_i\}\rangle=\| \varphi \|^{M_{w_i}}(s)$，又因为 $\forall \varphi\in L_\mu \cdot \| \varphi \|^{M_2}(s_{20})\leqslant_i \| \varphi \|^{M_1}(s_{10})$，并且 $\leqslant_i$ 相对于⊕单调，所以：

$\| \varphi \|^{M_2}(s)\otimes\langle\{w_i\},\{w_i\}\rangle\leqslant_i \| \varphi \|^{M_1}(s)\otimes\langle\{w_i\},\{w_i\}\rangle$

所以 $\| \varphi \|^{M_{2w_i}}(s_{20})\leqslant_i \| \varphi \|^{M_{1w_i}}(s_{10})$。

根据定理 4 及定理 6，有以下推论成立。

推论 2 两个多值模型 M_1 与 M_2 分解后对应的三值模型之间存在混合模拟关系当且仅当 $\forall \varphi\in L_\mu \cdot \| \varphi \|^{M_2}(s_{20})\leqslant_i \| \varphi \|^{M_1}(s_{10})$，其中 s_{10} 与 s_{20} 分别为 M_1 与 M_2 的初始状态。

这样我们把多值模型的逼近关系和分解得到的三值模型的混合模拟关系联系起来，就从结构上完成了多值模型逼近关系的刻画。

如图 1 中(a)与(b)分别为多值模型 M_1 与 M_2 的迁移图，M_1 分解后的三值模型为 M_{1a} 与 M_{1b}，M_2 分解后的三值模型为 M_{2a} 与 M_{2b}(如图 1(d)与(f)所示)。对于关系 $\rho_a=\{\langle s_{00a}, s_{0a}\rangle, \langle s_{10a}, s_{1a}\rangle, \langle s_{11a}, s_{1a}\rangle\}$ 与关系 $\rho_b=\{\langle s_{00b}, s_{0b}\rangle, \langle s_{11b}, s_{1b}\rangle\}$，从图中可以看出 ρ_a，ρ_b 分别为 M_{1a} 与 M_{2a}，M_{1b} 与 M_{2b} 间的混合模拟关系，由 μ 演算公式在多值模型上的语义易得属性 $\Box p$ 在 M_1 与 M_2 上的检测结果分别为：$\| \Box p \|^{M_1}(s_{00})=\langle\{a,b\},\emptyset\rangle$，$\| \Box p \|^{M_2}(s_0)=\langle\{b\},\emptyset\rangle$，则有 $\| \Box p \|^{M_2}(s_0)\leqslant_i \| \Box p \|^{M_1}(s_{00})$。

5 相关工作

多值模型是传统布尔模型的扩展，可以有效地表示系统中的不确定与不一致信息，因此对多值模型的研究也越来越广泛。例如，三值模型可以对包含部分信息的系统进行建模[13]。四值逻辑可以表示不一致信息，因此对于包含不一致信息的系统，可以用四值模型对其进行建模[14]。文献[15]以符号模型检测算法为基础，设计出了多值模型检测器 χChek，它可以准确返回属性在系统上的满足程度。文献[16]研究了如何将多值模型检测问题分解为多个传统二值模型检测问

题，再利用二值模型上的检测算法与检测工具来解决多值模型检测问题。与我们不同的是，其不仅分解了模型，而且定义了新的逻辑公式，将 μ 演算公式分解为新的逻辑公式；而我们只需分解多值模型，保持 μ 演算公式不变。相比而言，我们的方法更为简单。

研究多值模型时，同样面临着状态爆炸问题，目前解决此问题的主要方法有抽象方法[6]、组合方法[11]以及对称化简方法[17]等等。对于抽象方法，文献[18]提出了给定具体模型系统的构建抽象模型的方法；文献[19]介绍了一种可选的模拟关系来表示逼近关系，然而这种关系返回的是一个值，表示两个模型间的逼近程度；而本文中定义的逼近刻画返回的只能是真或者假，即表示两个模型是否满足逼近关系。文献[8]与文献[10]分别介绍了三值与六值模型上的混合模拟关系刻画的逼近关系，与本文中的逼近关系定义类似，对逻辑属性的模型检测结果在信息序关系上得以保持；然而，三值模型与六值模型都是特殊的多值模型，而文中讨论的是更一般的多值模型。文献[11]给出了多值模型混合模拟关系的定义，从结构上刻画了两模型间的确定逼近关系。但是，其定义过于狭窄，与三值模型上的混合模拟关系[8]存在不一致性。文献[12]首次提出了基于世界双格的多值模型，给出了多值模型间逼近关系结构刻画(精化关系)，最后以此精化关系为基础，给出了多值模型上商结构的定义，并给出了多值模型对称化简方法。但是，文献[11]与文献[12]中的结构刻画都只是多值模型间满足逼近关系的充分条件，而非必要条件。为此，本文将多值模型分解为多个三值模型，并借助于三值模型上混合模拟关系的定义从逻辑上刻画多值模型间的确定逼近关系，进一步，证得此逻辑刻画是多值模型间满足逼近关系的充分必要条件，解决已有工作的局限性。

结束语 多值模型广泛用于对包含不确定和不一致信息的软件系统进行建模。与传统的布尔模型一样，多值模型同样存在着状态爆炸问题，抽象是解决状态爆炸问题的一种重要方法。为了刻画多值模型中抽象模型与具体模型间的逼近关系，本文首先提出了将基于双格的多值模型分解为多个三值模型的方法，并且证明对任意 μ 演算公式 φ，其在多值模型上的检测结果为 φ 在分解后各三值模型上检测结果的合并。再进一步由三值模型上的精化关系来得到多值模型之间逼近关系的逻辑刻画。因此，对于一般的多值模型，可以通过对应的分解后得到的三值模型之间的混合模拟关系来判断多值模型的逼近关系，并且证明了该条件的充分必要性，完成了对一般多值模型的逼近关系的刻画。

在后续的工作中，我们将研究多值模型是否满足逼近关系的算法的设计与实现，并且进一步将我们给出的多值模型间的逼近关系的刻画运用到多值模型的抽象方法中，解决相应的模型检测中的状态爆炸问题。

参 考 文 献

[1] Clarke E, Grumberg O, Peled D. Model Checking[M]. MIT press, 1999

[2] Shoham S, Grumberg O. Multi-valued model checking games [J]. Journal of Computer and System Sciences, 2012, 78(2): 414-429

[3] Ginsberg M L. Multi valued logics : a uniform approach to reasoning in artificial intelligence[J]. Computational intelligence, 1988, 4(3): 265-316

[4] Kleene S C. Introduction to Metamathematics[M]. North Holland, 1987

[5] Chechik M, Devereux B, Easterbrook S, et al. Multi-valued symbolic model-checking[J]. ACM Transactions on Software Engineering and Methodology (TOSEM), 2003, 12(4): 371-408

[6] Dams D, Gerth R, Grumberg O. Abstract interpretation of reactive systems[J]. ACM Transactions on Programming Languages and Systems (TOPLAS), 1997, 19(2): 253-291

[7] Godefroid P, Jagadeesan R. Automatic abstraction using generalized model checking [M] // Computer Aided Verification. Springer Berlin Heidelberg, 2002: 137-151

[8] Godefroid P, Jagadeesan R. On the expressiveness of 3-valued models[M] // Verification, Model Checking, and Abstract Interpretation. Springer Berlin Heidelberg, 2003: 206-222

[9] Gurfinkel A, Wei O, Chechik M. Model checking recursive programs with exact predicate abstraction[M] // Automated Technology for Verification and Analysis. Springer Berlin Heidelberg, 2008: 95-110

[10] Ball T, Kupferman O, Yorsh G. Abstraction for falsification [M] // Computer Aided Verification. Springer Berlin Heidelberg, 2005: 67-81

[11] Meller Y, Grumberg O, Shoham S. A framework for compositional verification of multi-valued systems via abstraction-refinement[M] // Automated Technology for Verification and Analysis. Springer Berlin Heidelberg, 2009: 271-288

[12] 陈娟娟，魏欧，黄志球，等. 基于双格的多值模型的精化关系与对称化简[J]. 计算机工程与应用，2013，49(22)：40-45

[13] Bruns G, Godefroid P. Model checking partial state spaces with 3-valued temporal logics[M] // Computer Aided Verification. Springer Berlin Heidelberg, 1999: 274-287

[14] Huth M, Pradhan S. Lifting assertion and consistency checkers from single to multiple viewpoints[M]. Imperial College of Science, Technology and Medicine, Department of Computing, 2002

[15] Chechik M, Gurfinkel A, Devereux B. χChek : A multi-valued model-checker[M] // Computer Aided Verification. Springer Berlin Heidelberg, 2002: 505-509

[16] Gurfinkel A, Chechik M. Multi-valued model checking via classical model checking[M] // CONCUR 2003-Concurrency Theory. Springer Berlin Heidelberg, 2003: 266-280

[17] 魏欧，袁泳，蔡昕烨，等. 循环对称化简及在三值模型上的扩展[J]. 软件学报，2011，22(6)

[18] Gurfinkel A, Wei O, Chechik M. Systematic construction of abstractions for model-checking[M] // Verification, Model Checking, and Abstract Interpretation. Springer Berlin Heidelberg, 2006: 381-397

[19] Kupferman O, Lustig Y. Latticed simulation relations and games [M] // Automated Technology for Verification and Analysis. Springer Berlin Heidelberg, 2007: 316-330