基于模糊逻辑的几类Kripke结构之间的关系

潘海玉[1] 张 敏[2] 陈仪香[2]
(安徽工程大学计算机与信息学院 芜湖 241000)[1]
(华东师范大学上海市高可信计算重点实验室 上海 200062)[2]

摘 要 根据初始状态、状态之间的转换关系和命题赋值函数是否为分明的,模糊Kripke结构可分为8类。提出将模糊计算树逻辑作为判断模糊Kripke结构之间是否是等价的依据;详细讨论了8种模糊Kripke结构之间的关系。这些结论为设计应用中模型的合理选取提供了理论依据,也为解决模糊计算树逻辑的模型检测问题提供了一种新的方法。

关键词 Kripke结构,形式化验证,模糊逻辑,计算树逻辑
中图法分类号 TP301 **文献标识码** A

Relationships among Several Types of Kripke Structures Based on Fuzzy Logic

PAN Hai-yu[1] ZHANG Min[2] CHEN Yi-xiang[2]
(College of Computer and Information, Anhui Polytechnical University, Wuhu 241000, China)[1]
(Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, Shanghai 200062, China)[2]

Abstract With respect to the initial state, transition relation and propositional valuation function being crisp or not, fuzzy Kripke structure is classified into eight forms. This paper provided a kind of fuzzy computation tree logic to show that two different fuzzy Kripke structures are equivalent if they give the same truth values for every formula of fuzzy computation tree logic, and discussed the relationship among different fuzzy Kripke structures. The results provide the theoretical foundations for the appropriate choice of models in practice and present a new method for model checking of fuzzy computation tree logic.

Keywords Kripke structure, Formal verification, Fuzzy logic, Computation tree logic

1 引言

在计算机科学中,形式化方法[1,2]是指采用数学和逻辑的方法对软硬件系统的建构进行支持的技术,其目的在于保证系统相对规范的正确性,其最基本的内容包括形式规范和形式验证。人们常用转换系统(如Kripke结构(Kripke Structure,KS)、自动机)作为系统的模型,用时态逻辑描述系统的行为规范。

Kripke结构一般包括状态集合S、状态转换关系$R\subseteq S\times S$、初始状态s_0、原子命题集合AP以及用以确定在一个状态上哪些原子命题为真的函数。随着形式化验证方法研究的深入,研究者认识到传统的转换系统不能描述系统建模设计和实现中的一些有用的量化信息,通过将传统的Kripke结构等转化系统的真值从二值逻辑扩展到多值逻辑上,得到了多种不同形式的量化的Kripke结构[3-6],取得了一系列的研究成果。比较有代表意义的量化模型是基于有限DeMorgan代数的Kripke结构[5],该结构的主要特点是:原子命题公式在一个状态上不再是是否为真,而是成立的真值是有限DeMorgan代数中的一个元素,状态之间的转换关系变成了格值转换关系,另外初始状态集合变成了格值子集。

到目前为之,量化Kripke结构的定义按照真值集的代数结构以及状态初始集合、状态转换关系、命题赋值函数的不同选取已有许多种不同的定义,但是这些形式上不同的量化Kripke结构之间到底有什么关系是一个并未得到深入研究的课题。本文将在模糊集所定义的Kripke结构下讨论这个问题。

根据初始状态、状态之间的转换关系和命题赋值函数是否为分明的,模糊Kripke结构可分为8类。尽管在模糊自动机理论中,从接受语言角度出发,对不同类型的模糊自动机的等价性问题的研究已有很多的进展[7-9],但是,根据某种判断标准来分析这些不同的模糊Kripke结构是否是等价的,还没有文献涉及。本文试图解决这一问题,提出一种模糊计算树逻辑,给出其语法和语义解释。对于任意的模糊计算树逻辑公式,若两种模糊Kripke结构给出的逻辑公式成立的真值是

到稿日期:2012-07-20 返修日期:2012-10-21 本文受国家自然科学基金(61021004,61202105,1127123761228305),973项目(2011CB302802),上海市重点学科建设项目(B412)资助。

潘海玉(1976—),男,博士,讲师,主要研究方向为形式化分析与验证,E-mail:phyu76@sohu.com;张 敏(1977—),女,博士,副教授,主要研究方向为形式化方法,E-mail:mzhang@sei.ecnu.edu.cn(通信作者);陈仪香(1961—),男,博士,教授,博士生导师,主要研究方向为物联网、云计算、实时软件系统、程序语义模型与可信软件、知识科学与知识工程。

相同的，就认为这两种模糊 Kripke 结构是等价的。我们详细地分析不同模糊 Kripke 结构之间的关系。选择模糊计算树逻辑作为判断模糊 Kripke 结构是否等价的标准，是有合理依据的，因为模糊化的时态逻辑，如模糊计算树逻辑，是量化的反应式系统的规范语言，而模糊 Kripke 结构是描述量化的反应式系统的行为模型。

2 模糊 Kripke 结构和模糊计算树逻辑

本节首先给出模糊 Kripke 结构的定义，然后介绍计算树逻辑在模糊情形下的一种扩张形式。设 AP 为有限原子命题集合。

定义 1 一个基于 AP 的模糊 Kripke 结构(Fuzzy Kripke Structure，FKS)是一个四元组 $K=(S,S^0,\delta,V)$，其中

(1)S 是非空有限状态集合；

(2)$S^0:S\to[0,1]$是模糊初始状态集合；

(3)$\delta:S\times S\to[0,1]$是模糊转换关系；

(4)$V:S\times AP\to[0,1]$是一个赋值函数，对于给定的状态 s 和命题 p，$V(s,p)$给出 p 在 s 上成立的真值。

进一步，根据 S^0,δ,V 是否为分明的，FKS 可分为 8 类：

1. FKS1：S^0 是模糊子集，δ,V 是分明子集。
2. FKS2：S^0,δ 是模糊子集，V 是分明子集。
3. FKS3：S^0,V 是模糊子集，δ 是分明子集。
4. FKS4：S^0,δ 是分明子集，V 是模糊子集。
5. FKS5：S^0 是分明子集，δ,V 是模糊子集。
6. FKS6：S^0,V 是分明子集，δ 是模糊子集。
7. FKS7：S^0,δ,V 都是分明子集。
8. FKS8：S^0,δ,V 都是模糊子集。

$|S|$是集合 S 中状态的个数。若模糊 Kripke 结构的 S^0,δ,V 都是分明的，此结构就是通常的 Kripke 结构。一个(可能无限的)状态序列 $\pi=s_0,s_1,\cdots$成为 s 的一条路径若 $s_0=s$。后文用 $\pi(i)$表示 π 的第 i 个状态 。

以下给出模糊计算树逻辑的语法与语义。

定义 2 模糊计算树逻辑(Fuzzy Computation Tree Logic，FCTL)的公式的构成如下：

$$\varphi::=\mathrm{tt}\mid p\mid\varphi\vee\varphi\mid\varphi\wedge\varphi\mid\exists X\varphi\mid\exists\varphi U\varphi\mid\exists G\varphi$$

其中 $p\in AP$。全体模糊计算树逻辑公式之集记为 F。

从语法上说，FCTL 公式是经典的 CTL 公式集的真子集，在 CTL 公式集中，有非运算符$\neg$和路径分支符号 $\forall$。FCTL 公式解释在 FKS 上。

定义 3 给定一个模糊 Kripke 结构 K。设 $s\in S,\varphi\in F$。φ在 s 上的真值记为 $\|\varphi\|_K(s)$，归纳定义如下：

$$\|p\|_K(s)=V(s,p)$$

$$\|\varphi_1\vee\varphi_2\|_K(s)=\|\varphi_1\|_K(s)\vee\|\varphi_2\|_K(s)$$

$$\|\varphi_1\wedge\varphi_2\|_K(s)=\|\varphi_1\|_K(s)\wedge\|\varphi_2\|_K(s)$$

$$\|\exists\varphi\|_K(s)=\bigvee_{s'\in S}(\delta(s,s')\wedge\|\varphi\|_K(s'))$$

$$\|\exists\varphi_1U\varphi_2\|_K(s)=\bigvee_{\pi\in\Pi(s)}\bigvee_{i\in\mathbf{N}}\Big(\bigwedge_{0\leqslant j<i}(\|\varphi_1\|_K(\pi(j))\wedge\delta(\pi(j),\pi(j+1)))\wedge\|\varphi_2\|_K(\pi(i))\Big)$$

$$\|\exists G\varphi\|_K(s)=\bigvee_{\pi\in\Pi(s)}\bigwedge_{i\in\mathbf{N}}(\|\varphi\|_K(\pi(i))\wedge\delta(\pi(i),\pi(i+1)))$$

式中，$\mathbf{N}$是自然数，$\Pi(s)$是所有以 s 为起点的路径的集合。

φ在 K 上的真值定义为：

$$\|K,\varphi\|=\bigvee_{s\in S}(S^0(s)\wedge\|\varphi\|_K(s))$$

设 $f:F\to[0,1]$。若存在一个 FKS K，对于任意的 $\varphi\in F$，有 $\|K,\varphi\|=f(\varphi)$，则称 f 可以被一个 FKS 所接受。对于一个 Kripke 结构 K 的一个状态 s 和公式 $\varphi\in F$，若 $\|\varphi\|_K(s)=1$，记为 $K,s|=\varphi$。

定义 4 两个 FKS K_1 和 K_2 称为等价的，如果对于任意的 $\varphi\in F$，$\|K_1,\varphi\|=\|K_2,\varphi\|$。

我们给出一个有用的结论，证明可参见文献[6]。

定理 1 设 $s\in S$ 和 $\exists\varphi_1U\varphi_2,\exists G\varphi\in F$。

(1)存在一个 $k\leqslant|S|$和路径 $\pi\in\Pi(s)$，使得

$$\|\exists\varphi_1U\varphi_2\|_K(s)=\bigwedge_{0\leqslant j<k}(\|\varphi_1\|_K(\pi(j))\wedge\delta(\pi(j),\pi(j+1)))\wedge\|\varphi_2\|_K(\pi(k))$$

(2)存在一个 $k\leqslant|S|$和路径 $\pi\in\Pi(s)$，使得

$$\|\exists G\varphi\|_K(s)=\bigwedge_{0\leqslant j<k}(\|\varphi\|_K(\pi(j))\wedge\delta(\pi(j),\pi(j+1)))$$

3 模糊 Kripke 结构之间的关系

在具体讨论模糊 Kripke 结构之间的关系之前，需要引入一些记号和定义。

设 X 为非空集合。对于模糊子集 $f:X\to[0,1]$，令 $R(f)=\{f(x):x\in X,f(x)>0\}$。对于任意的 $a\in[0,1]$，定义 X 的子集 f_a 为 $f_a=\{x:x\in X,f(x)\geqslant a\}$。$a\wedge f_a$ 定义为：当 $x\in f_a$ 时，$(a\wedge f_a)(x)=a$，在其他情形下，$(a\wedge f_a)(x)=0$。

定义 5 给定一个 FKS $K=(S,S^0,\delta,V)$。对于所有的 $a\in[0,1]$，Kripke 结构 $K_a=(S,S^0_a,\delta_a,V_a)$定义如下：

- $S^0_a=\{s:S^0(s)\geqslant a,s\in S\}$。
- $\delta_a=\{(s_1,s_2):\delta(s_1,s_2)\geqslant a,s_1,s_2\in S\}$。
- 对于所有的 $s\in S,V_a(s)=\{p:V(s,p)\geqslant a,p\in AP\}$。

根据以上的构造方法，可以得到下面一个引理：

引理 1 对于所有的 $\varphi\in F,s\in S,K_{a_1\vee a_2},s|=\varphi$ 当且仅当 $K_{a_i},s|=\varphi,i\in\{1,2\},a_i\in[0,1]$。

以下的结论将用于定理 2 的证明。

引理 2 设 $f_1,f_2:F\to[0,1]$。若 f_1 和 f_2 分别为一个 FKS 所接受，则它们的并也可以为一个 FKS 所接受。

定理 2 设 $f:F\to[0,1]$，则以下条件等价：

(1)f 可以被一个 FKS1 接受。

(2)f 可以被一个 FKS2 接受。

(3)f 可以被一个 FKS3 接受。

(4)f 可以被一个 FKS4 接受。

(5)f 可以被一个 FKS5 接受。

(6)f 可以被一个 FKS7 接受。

(7)$R(f)$有限，且对于任意的 $a\in R(f)$，f_a 可以被一个 FKS8 接受。

证明：(1)⇒(2)⇒(6)，(1)⇒(3)⇒(6)，(4)⇒(5)⇒(6)明显成立，因为前者是后者的一个特例。

(6)⇒(7)：假设 f 可以被一个 FKS7 接受。设该 FKS7 为 $K=(S,S^0,\delta,V)$。现用结构归纳法证明

$$R(f)\subseteq R(S^0)\cup R(\delta)\cup R(V)\cup\{1\}$$

即 $R(f)$是有限的。

·当 $\varphi=\mathrm{tt}$ 时，结论明显成立。当 $\varphi=p, p\in AP$ 时，

$$\|K,p\| = \vee\{S^0(s)\wedge V(s,p): s\in S\}$$
$$=\max\{\min(S^0(s),V(s,p)): s\in S\}$$

所以

$$R(f)\subseteq R(S^0)\cup R(V)\subseteq R(S^0)\cup R(\delta)\cup R(V)\cup\{1\}$$

·当 $\varphi=\varphi_1\vee\varphi_2$ 时，可以得到

$$R(f(\varphi_1\vee\varphi_2))=R(\|K,\varphi_1\vee\varphi_2\|)$$
$$\subseteq R(f(\varphi_1))\cup R(f(\varphi_2))$$
$$\subseteq R(S^0)\cup R(\delta)\cup R(V)\cup\{1\}$$

·当 $\varphi=\varphi_1\wedge\varphi_2$ 时，可以得到

$$R(f(\varphi_1\wedge\varphi_2))\subseteq R(S^0)\cup R(\delta)\cup R(V)\cup\{1\}$$

·当 $\varphi=\exists X\varphi_1$ 时，

$$\|K,\exists X\varphi_1\| = \vee\{S^0(s)\wedge\bigvee_{s'\in S}(\delta(s,s')\wedge\|\varphi_1\|_K(s')): s\in S\}$$

所以

$$R(f(\exists X\varphi_1))\subseteq R(S^0)\cup R(\delta)\cup R(f(\varphi_1))$$
$$\subseteq R(S^0)\cup R(\delta)\cup R(V)\cup\{1\}$$

·当 $\varphi=\exists\varphi_1 U\varphi_2$ 时，用定理 1 可以得到

$$R(f(\exists\varphi_1 U\varphi_2))=R(\|K,\exists\varphi_1 U\varphi_2\|)$$
$$\subseteq R(f(\varphi_1))\cup R(f(\varphi_2))\cup R(\delta)$$
$$\subseteq R(S^0)\cup R(\delta)\cup R(V)\cup\{1\}$$

·当 $\varphi=\exists G\varphi_1$ 时证明类似于 $\varphi=\exists\varphi_1 U\varphi_2$ 情形，略。

设 $a\in R(f)$。$K_a=(S,S_a^0,\delta_a,V_a)$ 是一个如定义 5 所生成的 Kripke 结构。注意到对于任意的 $\varphi\in F$，$\|K,\varphi\|\geqslant a$，则存在一个 $s\in S$，使得 $S^0(s)\geqslant a$，$\|\varphi\|_K(s)\geqslant a$。所以只需要证明若 $\|\varphi\|_K(s)\geqslant a$，则 $K_a,s|=\varphi$。用归纳法证明

$$\|\varphi\|_K(s)\geqslant a\Leftrightarrow K_a,s|=\varphi$$

成立。

·若 $\varphi=\mathrm{tt}$，结论明显成立。若 $\varphi=p(p\in AP)$，易证

$$\|p\|_K(s)\geqslant a\Leftrightarrow K_a,s|=p$$

·若 $\varphi=\varphi_1\vee\varphi_2$，可以得到

$$\|\varphi_1\vee\varphi_2\|_K(s)\geqslant a\Leftrightarrow\|\varphi_1\|_K(s)\geqslant a\vee\|\varphi_2\|_K(s)\geqslant a$$
$$\Leftrightarrow K_a,s|=\varphi_1\vee K_a,s|=\varphi_2$$
$$\Leftrightarrow K_a,s|=\varphi_1\vee\varphi_2$$

·若 $\varphi=\varphi_1\wedge\varphi_2$ 时，也可证结论成立。

·若 $\varphi=\exists X\varphi_1$ 时，根据归纳假设，有

$$\|\exists X\varphi_1\|_K(s)\geqslant a\Leftrightarrow\text{存在一个 } s'\in S \text{ 使得 } \delta(s,s')\geqslant a$$
$$\text{和}\|\varphi_1\|_K(s')\geqslant a$$
$$\Leftrightarrow(s,s')\in\delta_a, K_a,s'|=\varphi_1$$
$$\Leftrightarrow K_a,s|=\exists X\varphi_1$$

·若 $\varphi=\exists\varphi_1 U\varphi_2$ 时，根据定理 1，有

$$\|\exists\varphi_1 U\varphi_2\|_K(s)\geqslant a\Leftrightarrow\text{存在一个 }\pi\in\prod(s)\text{和 }i\in\mathbf{N}\text{ 使得}$$
$$\bigwedge_{0\leqslant j<i}(\|\varphi_1\|_K(\pi(j))\wedge\delta(\pi(j),\pi(j+1)))\wedge\|\varphi_2\|_K(\pi(i))\geqslant a$$
$$\Leftrightarrow K_a,s|=\exists\varphi_1 U\varphi_2$$

·若 $\varphi=\exists G\varphi_1$，根据定理 1，也可证明结论成立。

(7)⇒(1)：对于任意的 $a\in R(f)$，f_a 可以被一个 Kripke 结构 $K=(S,S^0,\delta,V)$ 接受，注意到 $a\wedge f_a$ 可以被一个 FKS1 $K'=(S,a\wedge S^0,\delta,V)$ 接受。根据 $f=\bigvee_{a\in R(f)}(a\wedge f_a)$ 和引理 2，则其可以被一个 FKS1 接受。

最后，我们证明(7)⇒(4)。对于任意的 $a\in R(f)$，f_a 可以被一个 Kripke 结构 $K=(S,S^0,\delta,V)$ 接受。注意到 $a\wedge f_a$ 可以被一个 FKS4 $K'=(S,S^0,\delta,a\wedge V)$ 接受，所以 f 可以被一个 FKS4 接受。至此，我们完成定理的证明。

定理 2 分析了从接受模糊计算树逻辑公式的角度，6 种模糊 Kripke 结构之间的关系，它还有其它重要的意义：

定理 3 对于所有的 $\varphi\in F, s\in S$。

$$\|\varphi\|_K(s)=\vee\{a|K_a,s|=\varphi, a\in[0,1]\}$$

定理 4 设 $f:F\to[0,1]$。若 f 可以被一个 FKS6 接受，则 f 可以被某个 FKS5 接受。但反之不真。

证明：定理 4 的前一部分明显成立。设 $K=(\{s\},\{s\},\delta,V)$ 是一个 FKS5，其中

$$AP=\{p\},\delta(s,s)=0.8,V(s,p)=0.8$$

我们算出 $\|K,p\|=0.8$。因为 FKS6 的初始状态集合和命题赋值函数是分明的，所以对于任意的 FKS6，p 在此模型的真值都不可能是 0.8。至此我们完成定理 4 的证明。

结束语 本文利用时态逻辑的方法研究了模糊 Kripke 结构之间的关系，证明了除了具有模糊转换关系的 Kripke 结构和经典的 Kripke 结构外，从接受模糊计算树逻辑公式的角度来说，其它的模糊 Kripke 结构是等价的。这些结论为设计应用中模型的合理选取提供了理论依据，也为解决模糊 Kripke 结构上的模糊 CTL 模型检测问题提出了全新的方法。

参 考 文 献

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

[2] Baier C, Katoen J P. Principles of Model Checking [M]. The MIT Press, 2007

[3] de Alfaro L, Faella M, Henzinger T A, et al. Model checking discounted temporal properties[J]. Theoretical Computer Science, 2005, 345(1): 139-170

[4] Chechik M, Gurfnkel A, Devereux B, et al. Data structures for symbolic multi-valued model-checking[J]. Formal Methods in Software Design, 2006, 29(3): 295-344

[5] Kupferman O, Lusting Y. Latticed simulation relations and games [J]. International Journal on the Foundations of Computer Science, 2010, 21(2): 167-189

[6] 潘海玉. 状态转化系统的格值量化验证方法研究[D]. 上海：华东师范大学，2012

[7] Li Y M, Pedrycz W. Fuzzy nite automata and fuzzy regular expressions with membership values in lattice ordered monoids [J]. Fuzzy Sets and Systems, 2005, 156: 68-92

[8] Li Z H, Li P, Li Y M. The relationships among several types of fuzzy automata[J]. Information Sciences, 2006, 176: 2208-2226

[9] Li Y M. Approximation and robustness of fuzzy finite automata [J]. International Journal of Approximate Reasoning, 2008, 47(2): 247-257