计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.200500036

模糊安全性和活性

石铁柱　钱俊彦　潘海玉
桂林电子科技大学广西可信软件重点实验室　广西 桂林 541004
(tiezhus86@163.com)

摘　要　形式规约使用形式语言构建所开发的软硬件系统的规约,刻画系统的模型和性质。其中,性质规约中的分支时间规约对于系统验证有着非常重要的作用。在经典情形下,系统性质规约是基于二值逻辑的,不能描述不一致或不确定的信息。因此,将其推广到模糊逻辑背景下,有助于对模糊系统进行形式验证。文中首先给出了性质规约中分支时间属性在模糊背景下的形式化定义,重点研究了其中的安全性和活性;然后,定义了两种闭包操作,从而产生了4种类型的属性,即泛安全性、泛活性、存在安全性和存在活性;最后,证明了每个分支时间属性,或是存在安全性和存在活性的交,或是泛安全性和泛活性的交,或是存在安全性和泛活性的交。

关键词:形式规约;模糊逻辑;分支时间属性;安全性;活性
中图法分类号　TP301

Fuzzy Safety and Liveness Properties

SHI Tie-zhu,QIAN Jun-yan and PAN Hai-yu
Guangxi Key Laboratory of Trusted Software,Guilin University of Electronic Technology,Guilin,Guangxi 541004,China

Abstract　Formal specification is to construct specification of the developed software and hardware systems by using formal language and describes their models and properties. Among which,the specification of properties which includes the specification of branching-time properties,plays an important role in verification of systems. In the classical setting,the specification of properties is based on two-valued logic,and hence cannot describe the inconsistent or uncertain information. Consequently,extending the specification languages of properties to the fuzzy setting helps to verify the fuzzy systems. In this paper,first,a formal definition of branching-time properties,especially the safety and liveness properties in the fuzzy setting,is given. Then,two types of closure operations are defined,resulting in 4 types of properties which are universal safety,universal liveness,existential safety,and existential liveness. Finally,it is shown that any branching-time property is the intersection between an existential safety property and an existential liveness property,or a universal safety property and a universal liveness property,or an existential safety property and a universal liveness property.

Keywords　Formal specification,Fuzzy logic,Branching-time properties,Safety properties,Liveness properties

1　引言

形式化方法[1]是指采用数学证明的手段对计算机软硬件系统进行形式规约、分析和验证的技术,其中,形式规约分为模型规约和性质规约。形式规约为形式开发与验证奠定了基础。模型检测[2]作为一种形式验证技术,通过自动遍历系统模型的有穷状态空间,来检验系统模型与其性质规约之间的满足关系。在经典的模型检测理论中,系统模型与其性质规约都是二值的,然而在某些大型系统中不可避免地会涉及到一些不确定或不一致信息的处理。因此,人们提出了基于概率理论的概率模型检测[2-8]、基于模糊逻辑的模型检测[9-15]等。

针对系统的行为和特点,其性质规约通常可以被分为线性时间规约和分支时间规约,它们也被称为线性时间(Linear-time)和分支时间(Branching-time)属性。线性时间属性常被定义为无限字符串的集合,而分支时间属性则为完全树的集合。安全性和活性[16-18]作为研究线性时间和分支时间属性的基础属性,受到了人们的广泛关注。安全性可以保证系统在运行过程中不会发生"坏"的事情,活性要求"好"的事情最终会发生。安全性和活性的定义将成为系统验证的关键。

对于线性时间属性,人们已经对其中的安全性和活性做了大量的研究。Lamport[19]于1977年引入了安全性和活性的概念。Alpern等[20-21]从拓扑学中闭包的角度,给出了安全

到稿日期:2020-05-11　返修日期:2020-08-16　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:国家自然科学基金(61672023);广西自然科学基金(2018GXNSFAA281326);广西可信软件重点实验室基金(kx201911)
This work was supported by the National Natural Science Foundation of China (61672023), Natural Science Foundation of Guangxi (2018GXNSFAA281326) and Foundation of Guangxi Key Laboratory of Trusted Software(kx201911).
通信作者:潘海玉(phyu76@126.com)

性和活性的刻画，同时他们证明了每个线性时间属性是安全性和活性的交。随后，Sistla[22]从线性时态逻辑的角度给出了安全性和活性的刻画。特别地，Li 等[23]研究了线性时间属性在模糊系统中的模型检测问题，定义出安全性、活性在多值逻辑中的推广形式，并讨论了多值线性时间属性的验证算法。

在分支时间属性中，Manolios 等[24]在线性时间属性研究的基础上，开展了分支时间下安全性和活性的研究。Bouajjani 等[25]使用树自动机和分支时态逻辑对一种特殊的安全性进行刻画。Zhang 等[26]以 Manolios 的分支时间安全性和活性为基础，基于离散时间马尔可夫链研究了概率背景下分支时间中安全性和活性的扩展问题，他们将分支时间属性定义为概率树的集合，并且提供了一种分解结果，证明了每个分支时间属性可以被分解为安全性和活性的交。此外他们还提出了一种将概率计算树逻辑公式分解为安全性公式和活性公式的算法。

遗憾的是，在模糊背景下，将分支时间属性扩展到模糊系统中还没有相应的形式化定义，本文将开展相关工作，为模糊模型检测的进一步发展提供理论支持。首先，我们将模糊 Kripke 结构展开，给出模糊树的概念，同时给出模糊树的前缀和后缀关系；然后定义分支时间属性的两种前缀和两种闭包操作；接着定义存在安全性、泛安全性、存在活性、泛活性；最后，我们考虑了每个属性是否都能表示为安全性和活性的交。

2 预备知识

本节首先给出一些定义和记号。$\mathbb{N}$ 表示自然数集合。设 Σ 是一个集合，则 $\mathscr{P}(\Sigma)$ 表示它的幂集。Σ 上的模糊集[27]合 A 是 Σ 到 $[0,1]$ 的一个映射，即 $\mu:\Sigma\to[0,1]$。μ 的支撑集的定义为：

$$\mathrm{supp}(\mu)=\{x\in\Sigma:\mu(x)>0\}$$

设函数 $f:A\to B$ 且 $A'\subseteq A$，则 f 在 A' 上的限制定义为 $f\upharpoonright_{A'}:A'\to B$。同时后文用 $dom(f)$ 表示函数 f 的定义域。

设 Σ 是集合，Σ^* 和 Σ^ω 分别表示 Σ 上的有限和无限序列的集合，记 Σ^∞ 为 $\Sigma^*\cup\Sigma^\omega$。$\varepsilon$ 是一个空序列。设 $u,v\in\Sigma^\infty$，用 $|v|$ 表示 v 的长度。$v(i)$ 表示序列 v 的第 $i+1$ 个元素，其中 $i<|v|$。v_l 表示有限序列 v 的最后一个元素。$u\cdot v$ 表示 u 和 v 的连接。称 u 是 v 的前缀，记作 $u\leq v$，若 $dom(u)\subseteq dom(v)$ 且对所有 $i\in dom(u)$，则 $u(i)=v(i)$。若 $u\leq v$ 且 $u\neq v$，则称 u 是 v 的真前缀，记作 $u<v$。设 $U\subseteq\Sigma^\infty$，若 $v\in U$ 且 $u\leq v$，有 $u\in U$，则称 U 是前缀封闭的。

3 前缀和闭包

本节首先介绍模糊 Kripke 结构和模糊树的概念，然后定义模糊树之间的前缀关系，并给出模糊树的前缀操作和闭包操作，最后证明了属性和属性闭包之间的一些性质。

模糊 Kripke 结构是经典 Kripke 结构在模糊集上的一种扩展形式，定义如下。

定义 1[14] 模糊 Kripke 结构(Fuzzy Kripke Strcture, FKS)是一个五元组 $K=(S,s_0,R,AP,L)$，其中：

(1) S 是非空状态集合；

(2) $s_0\in S$ 是初始状态；

(3) $R:S\times S\to[0,1]$ 是模糊转换函数；

(4) AP 是原子命题的集合；

(5) $L:S\to\mathscr{P}(AP)$ 是标记函数。

模糊 Kripke 结构可以看作一种有向标签图，如图 1 所示，图中的结点表示状态，结点里面和结点旁边的标签分别表示状态名和该状态上的原子命题集。例如，状态 s_1 上的标签为 $\{q\}$，这表示原子命题 q 在该状态上的值为真。有向边表示状态之间的迁移，边上的数值表示迁移程度。例如，结点 s_0 到 s_1 的有向边上的数值为 0.2，这表示状态 s_0 到 s_1 的迁移程度为 0.2。为了方便起见，当状态之间的迁移程度为 0 时，省略有向边。初始状态有一个箭弧进入且该箭弧没有任何出发结点。例如，状态 s_0 表示初始状态。

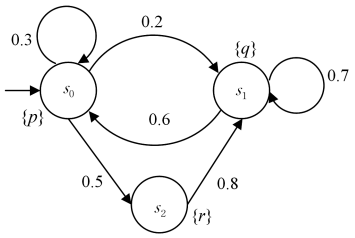

图 1 模糊 Kripke 结构

Fig. 1 Fuzzy Kripke structure

一棵树[28] W 是 $\mathbb{N}^*$ 上一个前缀封闭的集合且 $W\subseteq\mathbb{N}^*$，W 中的元素被称为树的结点。对于任意的 $x\in W$，称 $x\cdot c$ 为 x 的后继，其中 $c\in\mathbb{N}$。设 $A,B,\cdots\in\mathscr{P}(AP)$，其中 $\{p\}$ 简记为 p。若一个结点没有后继结点，则该结点是叶子结点，用 $leaf(W)$ 表示 W 中所有叶子结点的集合。若 W 没有叶子结点，则称 W 是完全的。称 W 是有限深度的，若存在 $n\in\mathbb{N}$，使得任意 $x\in W$，则有 $|x|\leqslant n$。$\mathbb{T}^{tot}$，$\mathbb{T}^{nt}$ 和 $\mathbb{T}^{f}$ 分别表示完全、非完全和有限深度树。注意到 $\mathbb{T}^{all}=\mathbb{T}^{tot}\cup\mathbb{T}^{nt}$ 且 $\mathbb{T}^{f}\subset\mathbb{T}^{nt}$。

定义 2 称 T 为模糊树，记 $T=(W,V,F)$，若：

(1) $(W\cup\{\varepsilon\})\subseteq\mathbb{N}^*$ 是一棵树；

(2) $V:W\to\mathscr{P}(\Sigma)$ 是结点标记函数；

(3) $F:W\times W\to[0,1]$ 是边标记函数，且满足 $F(x,x')>0$ 当且仅当存在 $c\in\mathbb{N}$，则使得 $x'=x\cdot c$。

图 2 给出了一棵有限深度模糊树，其中，结点旁边和结点里面分别为结点标签和结点序号，如结点 00 上的标签为 $\{q\}$；有向边上的数值表示结点间的迁移程度，如结点 00 到结点 000 的迁移程度为 0.7。该树的结点集合表示为：$W=\{0,00,01,02,000,001,010,020,021,022\}$。

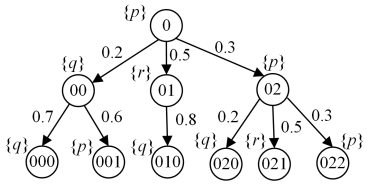

图 2 模糊树

Fig. 2 Fuzzy tree

该树也可以表示为如下形式：{(1, p), (1, p)(0.2, q), (1, p)(0.5, r), (1, p)(0.3, p), (1, p)(0.2, q)(0.7, q), (1, p)(0.2, q)(0.6, p), (1, p)(0.5, r)(0.8, q), (1, p)(0.2, q)(0.6, p), (1, p)(0.3, p)(0.2, q), (1, p)(0.3, p)(0.5, r), (1, p)

$(0.3,p)(0.3,p)\}$。

下面定义模糊树之间的前缀关系。

定义 3 设 $T_i=(W_i,V_i,F_i)$，其中，$i=1,2$ 且 $T_1\in\mathbb{T}^{nt}$，$T_2\in\mathbb{T}^{tot}$。称 T_1 是 T_2 的前缀，记作 $T_1\leq T_2$，如果：1）$W_1\subseteq W_2$；2）$V_2\upharpoonright_{W_1}=L_1$；3）$F_2\upharpoonright_{W_1\times W_1}=F_1$。

基于模糊树之间的前缀关系，我们定义两种前缀操作 np 和 fp，它们都是 $\mathbb{T}^{tot}$ 到 $\mathbb{T}^{all}$ 的函数。对于任意 $T\in\mathbb{T}^{tot}$，用 $np(T)$ 和 $fp(T)$ 分别表示对模糊树 T 进行非完全前缀操作和完全前缀操作所得到的集合，即：

$$fp(T)=\{T_1\in\mathbb{T}^{f}:T_1\leq T\}$$

$$np(T)=\{T_1\in\mathbb{T}^{nt}:T_1\leq T\}$$

引理 1 设函数 f,g 和 h 为函数，$dom(f)\subseteq dom(g)\subseteq dom(h)$。若 $g\upharpoonright_{dom(f)}=f$ 且 $h\upharpoonright_{dom(g)}=g$，则 $h\upharpoonright_{dom(f)}=f$。

证明：根据函数限制定义可知，对于任意 $x\in dom(f)$ 且 $y\in dom(g)$，有 $g\upharpoonright_{dom(f)}(x)=f(x)$ 和 $h\upharpoonright_{dom(g)}(y)=g(y)$。又因为 $dom(f)\subseteq dom(g)\subseteq dom(h)$，所以对于任意 $z\in dom(f)$，有：

$$\begin{aligned}h\upharpoonright_{dom(f)}(z)&=h\upharpoonright_{dom(g)}(z)\\&=g(z)\\&=g\upharpoonright_{dom(f)}(z)\\&=f(z)\end{aligned}$$

因此 $h\upharpoonright_{dom(f)}=f$。

根据模糊树之间的前缀关系，我们给出下面一个引理。

引理 2 前缀关系 $\leq$ 是 $\mathbb{T}^{f}$ 上的偏序关系。

证明：设任意 $T_1,T_2,T_3\in\mathbb{T}^{f}$。因为 $W_1\subseteq W_1$，$V_1\upharpoonright_{W_1}=V_1$ 和 $F_1\upharpoonright_{W_1\times W_1}=F_1$，所以 $T_1\leq T_1$。如果 $T_1\leq T_2$，$T_2\leq T_1$，则以下条件就成立：若 $W_1\subseteq W_2$，$W_2\subseteq W_1$，则 $W_1=W_2$；若 $V_2\upharpoonright_{W_1}=V_1$，$V_1\upharpoonright_{W_2}=V_2$，则 $V_2\upharpoonright_{W_1}=V_2\upharpoonright_{W_2}$，故 $V_1=V_2$；若 $F_2\upharpoonright_{W_1\times W_1}=F_1$，$F_1\upharpoonright_{W_2\times W_2}=F_2$，则 $P_1=P_2\upharpoonright_{W_1\times W_1}=P_2\upharpoonright_{W_2\times W_2}=P_2$。如果 $T_1\leq T_2$ 且 $T_2\leq T_3$，以下条件就成立：若 $W_1\subseteq W_2$ 且 $W_2\subseteq W_3$，则 $W_1\subseteq W_3$；若 $V_2\upharpoonright_{W_1}=V_1$ 且 $V_3\upharpoonright_{W_2}=V_2$，则由引理 1 可得 $V_3\upharpoonright_{W_1}=V_1$；若 $F_2\upharpoonright_{W_1\times W_1}=F_1$，$F_3\upharpoonright_{W_2\times W_2}=F_2$，则由引理 1 可得 $F_3\upharpoonright_{W_2\times W_2}=F_2$。

因此，$\leq$ 是 $\mathbb{T}^{f}$ 上的偏序关系。

一个系统从初始状态开始运行，由于其行为的不确定性，可能有多个后续状态，每个这样的状态又可能有多个后续状态，以此类推，可以产生一棵树。

下面将模糊 Kripke 结构展开为一棵模糊树。设模糊 Kripke 结构 $K=(S,s_0,R,AP,L)$ 和模糊树 $T(K)=(W_K,V_K,F_K)$，则以下 3 个条件成立：

（1）W_K 满足：$s_0\in W_K$ 且 $x\in W_K$ 使得对于任意 $t\in supp(\mu)$ 有 $x\cdot t\in W_K$，其中 $\mu(x_l)>0$。

（2）对于任意 $x\in W_K$，有 $V_K(x)=L(x_l)$。

（3）$P_K(x,x')=\mu(\pi_l')$，其中 $\mu(x_l)>0$。

注意到，初始状态 s_0 是模糊树 $T(K)$ 的根结点。

设 T_1 是图 2 给出的模糊树，T_2 可以表示为：$T_2=\{(1,p),(1,p)(0.2,q),(1,p)(0.5,r),(1,p)(0.3,p)\}$，则 T_2 是 T_1 的一个前缀。T_1 和 T_2 都可以看作图 1 给出的 FKS K 的部分来执行。注意到 T_1 和 T_2 都是 $T(K)$ 的前缀。

经典的分支时间属性是完全树的集合。因此，模糊背景下的分支时间属性是完全模糊树的集合，即 $P\subseteq\mathbb{T}^{tot}$。

一般来说，如果一个系统的行为被包含在给定的规范中，就称系统满足规范。称模糊 Kripke 结构 K 满足属性 P，记作 $K\models P$，如果 $T(K)\in P$。

为了研究安全性和活性，我们引入闭包的概念，同时将前缀操作提升到属性上。

定义 4 设 $P\subseteq\mathbb{T}^{tot}$，则有以下两种情况。

（1）分支时间属性 P 的两种前缀 $np(P)$ 和 $fp(P)$ 分别定义为：

$$np(P)=\{T_1\in\mathbb{T}^{nt}:\exists\,T\in P,T_1\leq T\}$$

$$fp(P)=\{T_1\in\mathbb{T}^{f}:\exists\,T\in P,T_1\leq T\}$$

（2）分支时间属性 P 的两种闭包 $ncl(P)$ 和 $fcl(P)$ 分别定义为：

$$ncl(P)=\{T\in\mathbb{T}^{tot}:np(T)\subseteq np(P)\}$$

$$fcl(P)=\{T\in\mathbb{T}^{tot}:fp(T)\subseteq fp(P)\}$$

根据以上闭包的定义，可以得出属性的闭包有下列性质。

引理 3 设 $P\subseteq\mathbb{T}^{tot}$，则属性 P 的闭包有下列性质：

（1）$ncl(P)=\{T\in\mathbb{T}^{tot}:\forall\,T_1\in np(T),\exists\,T_2\in P,T_1\leq T_2\}$。

（2）$fcl(P)=\{T\in\mathbb{T}^{tot}:\forall\,T_1\in fp(T),\exists\,T_2\in P,T_1\leq T_2\}$。

证明：这里只证明引理 3 性质（1），引理 3 性质（2）的证明类似，故省略。设 $T\in ncl(P)$，则由定义 4 可知，$np(T)\subseteq np(P)$。又由定义 4 可知，对于任意 $T_1\in np(T)\subseteq np(P)$，都存在 $T_2\in P$，这使得 $T_1\leq T_2$。因此，引理 3 性质（1）成立。

根据属性前缀和闭包的定义，我们给出下列命题。

命题 1 设 $P,Q\subseteq\mathbb{T}^{tot}$ 且 $P\subseteq Q$，则下列结论成立：

（1）$np(ncl(P))=np(P)$，$fp(fcl(P))=fp(P)$；

（2）$ncl(P)\subseteq ncl(Q)$，$fcl(P)\subseteq fcl(Q)$；

（3）$ncl(P)\subseteq fcl(P)$。

证明：

（1）首先 $np(P)\subseteq np(ncl(P))$ 显然成立。现在证明 $np(ncl(P))\subseteq np(P)$。设任意 $T\in ncl(P)$，由定义 4 可知，$np(T)\subseteq np(P)$。故 $np(ncl(P))=\bigcup\limits_{T\in ncl(P)}np(T)\subseteq\bigcup\limits_{T\in ncl(P)}np(P)=np(P)$，因此，$np(ncl(P))=np(P)$。

（2）设 $P\subseteq Q$ 且 $T\in ncl(P)$。由引理 3 可知，对于任意的 $T_1\in np(T)$，存在 $T_2\in P\subseteq Q$，使得 $T_1\leq T_2$。故 $T\in ncl(Q)$。因此，$ncl(P)\subseteq ncl(Q)$。

（3）已知 $\mathbb{T}^{f}\subset\mathbb{T}^{nt}$，则对于任意的 $T\in\mathbb{T}^{tot}$，有 $fp(T)\subset np(T)$。设 $T_1\in ncl(P)$，由引理 3 可知，$np(T_1)\subseteq np(P)$，又因为 $fp(T_1)\subset np(T_1)$。故 $fp(T_1)\subset np(P)$，即对于任意的 $T_1'\in fp(T_1)$，存在 $T_2\in P$，这使得 $T_1'\leq T_2$。因此，$T_1\in fcl(P)$。

闭包的概念对于后文中安全性与活性的定义以及相关性质的证明起着至关重要的作用。下文定理刻画了分支时间属性 P 与它的两种闭包 $fcl(P)$ 和 $ncl(P)$ 之间的关系。

定理 1 设 P,P_1 和 P_2 都为一个分支时间属性。设 $cl\in\{ncl,fcl\}$，则下列结论成立：

（1）$cl(\emptyset)=\emptyset$；

（2）$P\subseteq cl(P)$；

(3)$cl(P)=cl(cl(P))$;

(4)$ncl(fcl(P))=fcl(P)$;

(5)$fcl(P_1)\cup fcl(P_2)=fcl(P_1\cup P_2)$。

证明:这里以 $cl=ncl$ 为例,证明以上结论。

(1)首先证明 $\emptyset\subseteq ncl(\emptyset)$,即证明对于任意 $T\in\emptyset\Rightarrow T\in ncl(\emptyset)$。因为空集不包含任何元素,所以 $T\in\emptyset$ 不成立。故 $T\in\emptyset\Rightarrow T\in ncl(\emptyset)$总是成立。接下来证明 $ncl(\emptyset)\subseteq\emptyset$。根据引理 3 可知,设 $T\in\mathbb{T}^{tot}$,若 $T\in ncl(\emptyset)$,则对于任意 $T_1\in np(T)$,不存在 T_2(因为 $\emptyset$ 中没有元素),使得 $T_1\preceq T_2$。故 $ncl(\emptyset)$也为空。因此,$ncl(\emptyset)=\emptyset$。

(2)设 $T\in P$。因为 $np(P)=\bigcup_{T\in P}np(T)$,所以 $np(T)\subseteq np(P)$。由引理 3 可知,$T\in ncl(P)$。因此,$P\subseteq ncl(P)$。

(3)根据定理 1 的证明(2)可知 $ncl(P)\subseteq ncl(ncl(P))$,我们现用反证法证明 $ncl(ncl(P))\subseteq ncl(P)$。假设 $T\in ncl(ncl(P))\backslash ncl(P)$,由引理 3 可知,对于任意 $T_1\in np(T)$,存在 $T_2\in ncl(P)$,使得 $T_1\preceq T_2$,即 $T_1\in np(T_2)$。因为 $T_2\in ncl(P)$,所以存在 $T_3\in P$,使得 $T_1\preceq T_3$。而由 $T\notin ncl(P)$可知,存在 $T_1\in np(T)$,使得不存在 $T_3\in P$ 满足 $T_1\preceq T_3$。这与存在 $T_3\in P$,使得 $T_1\preceq T_3$ 相矛盾。

(4) 由定理 1 的证明(2)可知 $fcl(P)\subseteq ncl(fcl(P))$,又根据命题 1 可知,$ncl(fcl(P))\subseteq fcl(fcl(P))=fcl(P)$。因此,$ncl(fcl(P))=fcl(P)$。

(5) 当 $cl=fcl$ 时,证明如下。首先,由命题 1 可知,$fcl(P_1)\cup fcl(P_2)\subseteq fcl(P_1\cup P_2)$。现证明 $fcl(P\cup Q)\subseteq fcl(P)\cup fcl(Q)$。设 $T\in fcl(P\cup Q)$。现用反证法证明,假设 $T\notin fcl(P)$且 $T\notin fcl(Q)$。下面分两种情况讨论:当 $T\notin fcl(P_1)$时,则存在 $T_1\in fp(T)$,使得不存在 $T_1'\in P$ 满足 $T_1\preceq T_1'$;当 $T\notin fcl(P_2)$时,则存在 $T_2\in fp(T)$,使得不存在 $T_2'\in P$ 满足 $T_2\preceq T_2'$。设 $T_3\in fp(T)$使得 $T_1\preceq T_3$ 和 $T_2\preceq T_3$。因为 T_1 和 T_2 是 T 的有限深度前缀,这样的 T_3 总是存在。通过构造,当 $T\notin fcl(P_1)$时,说明不存在 $T_1'\in P$ 使得 $T_3\preceq T_1'$;当 $T\notin fcl(P_2)$时,说明不存 $T_2'\in P$ 使得 $T_3\preceq T_2'$。综上所述,$T\notin fcl(P_1\cup P_2)$与前提矛盾。因此,$fcl(P_1)\cup fcl(P_2)=fcl(P_1\cup P_2)$。

4 安全性

通俗地说,在系统运行过程中,安全性保证“坏”的事情不会发生。因为我们有两种类型的闭包,所以对应地产生两种安全性:存在安全性(Existential Safety,ES)和泛安全性(Universal Safety,US)。直观来说,存在安全性保证至少存在一个计算没有“坏”事情发生,而泛安全性保证所有计算都不会有“坏”的事情发生。

下面给出两种安全性的形式化定义。

定义 5 设 $P\subseteq\mathbb{T}^{tot}$,对于任意 $T\in\mathbb{T}^{tot}$:

(泛安全性) 称 P 是一个泛安全性当且仅当如果对于任意 $T_1\in fp(T)$,存在 $T_2\in P$,使得 $T_1\preceq T_2$,则 $T\in P$。

(存在安全性) 称 P 是一个存在安全当且仅当如果对于任意 $T_1\in np(T)$,存在 $T_2\in P$,使得 $T_1\preceq T_2$,则 $T\in P$。

由定义 5 可知,一个泛安全性属性 P 是由模糊树 T 构成的集合,同时对于 P 中的任意一棵模糊树的任意一个有限深度前缀,存在一个扩展使得扩展之后的模糊树仍然属于 P。换句话说,若 $T\notin P$,则存在 T 的一个有限深度前缀,对其进行任意扩展都不属于 P,即“坏”的事情发生且是不可挽回的。存在安全性与之类似。

定理 2 在模糊情况下,对安全性提供了一种闭包刻画。

定理 2 设 $P\subseteq\mathbb{T}^{tot}$,则以下结论成立:

(1)P 是一个泛安全性当且仅当 $fcl(P)=P$;

(2)P 是一个存在安全性当且仅当 $ncl(P)=P$。

证明:这里只证明定理 2 中(1),定理 2 中(2)的证明类似,故省略。

($\Rightarrow$)设 P 是一个泛安全性,由定理 1 可知,$P\subseteq fcl(P)$。我们现在证明 $fcl(P)\subseteq P$。设 $T\in fcl(P)$,由引理 3 可知,对于任意 $T_1\in fp(T)$,存在 $T_2\in P$,使得 $T_1\preceq T_2$。又根据定义 5 可知,$T\in P$,故 $fcl(P)\subseteq P$。因此,$fcl(P)=P$。

($\Leftarrow$)设 $fcl(P)=P$ 且 $T\in\mathbb{T}^{tot}$。设 $T\in P$ 且 $T_1\in fp(T)$,则存在 $T_2=T$ 使得 $T_1\preceq T_2$。更进一步,对于任意的 $T_1\in fp(T)$,存在 $T_2\in P$,使得 $T_1\preceq T_2$。由引理 3 可知,$T\in fcl(P)=P$。因此,P 是一个泛安全性。

安全性在操作$\cup$和$\cap$下是封闭的。

引理 4 设 $P,Q\subseteq\mathbb{T}^{tot}$,则以下结论成立:

(1)若 $P\in US$,则 $P\in ES$;

(2)若 $P,Q\in US$,则 $P\cup Q,P\cap Q$ 都为泛安全性;

(3)若 $P,Q\in ES$,则 $P\cup Q,P\cap Q$ 都为存在安全性。

证明:(1)设 $P\in US$,则由定理 2 可知,$fcl(P)=P$。又由定理 1 可知,因为 $P\subseteq ncl(P)$且 $ncl(P)\subseteq fcl(P)$,所以 $ncl(P)\subseteq P$。故 $ncl(P)=P$。因此,$P\in ES$。

引理 4 中的(2)和(3)的证明类似,因此只证明引理 4 中的(2)。由定理 1 知,$fcl(P\cup Q)=fcl(P)\cup fcl(Q)$。已知 P,Q 是泛安全性,则 $fcl(P)\cup fcl(Q)=P\cup Q$。故 $fcl(P\cup Q)=P\cup Q$。因此,根据定理 2 可得,$P\cup Q$ 是一个泛安全性。现在证明 $P\cap Q$ 是一个泛安全性。由定理 1 可知,$P\cap Q\subseteq fcl(P\cap Q)$,因此我们只需要证明 $fcl(P\cap Q)\subseteq P\cap Q$。设 $T\in fcl(P\cap Q)$,由引理 3 可知,对于任意的 $T_1\in fp(T)$,存在 $T_2\in P\cap Q$,使得 $T_1\preceq T_2$。又由定义 5 可知,$T\in P\cap Q$。

5 活性

相比安全性,活性断言“好”的事情最终会发生。若一个属性是活性,则它的闭包等于全集。根据所定义的两种属性闭包,可以得到两种不同类型的活性:泛活性(Universal liveness,UL)和存在活性(Existential liveness,EL)。具体定义如下。

定义 6 设 $P\subseteq\mathbb{T}^{tot}$。

(1)称 P 是一个泛活性,如果对于任意的 $T_1\in\mathbb{T}^{f}$,存在 $T_2\in P$,使得 $T_1\preceq T_2$。

(2)称 P 是一个存在活性,如果对于任意的 $T_1\in\mathbb{T}^{nt}$,存在 $T_2\in P$,使得 $T_1\preceq T_2$。

由定义 6 可知,如果模糊分支时间属性 P 是一个泛活性,那么$\mathbb{T}^{f}$中的任意的有限深度树扩展之后仍属于 P。

定理 3 对两种活性进行了闭包刻画。

定理 3 设 $P\subseteq\mathbb{T}^{tot}$,则以下结论成立:

(1)P 是一个泛活性当且仅当 $fcl(P)=\mathbb{T}^{tot}$;

(2)P 是一个存在活性当且仅当 $ncl(P)=\mathbb{T}^{tot}$。

证明:这里只证明定理 3 中的(1),定理 3 中(2)的证明类似,故省略。

(⇒)设 P 是一个泛活性。显然 $fcl(P)\subseteq\mathbb{T}^{tot}$,现只需要证明$\mathbb{T}^{tot}\subseteq fcl(P)$。设 $T\in\mathbb{T}^{tot}$,对任意的 $T_1\in fp(T)$。因为 P 是一个泛活性,所以存在 $T_2\in P$,使得 $T_1\preceq T_2$。因此 $T\in fcl(P)$。

(⇐)设 $fcl(P)=\mathbb{T}^{tot}$。用反证法。假设 P 不是泛活性。由定义 6 可知,存在 $T_1\in\mathbb{T}^{f}$,对所有 $T_2\in P$,使得 $T_1\not\preceq T_2$。设 $T\in\mathbb{T}^{tot}$ 且 $T_1\in fp(T)$,则 $T\notin ncl(P)$,这与假设 $fcl(P)=\mathbb{T}^{tot}$ 相矛盾。

根据定理 3,我们可以得到 $P\cup\overline{fcl(P)}$ 和 $P\cup\overline{ncl(P)}$ 分别为一个泛活性和一个存在活性。

引理 5 设 $P\subseteq\mathbb{T}^{tot}$,则以下结论成立:

(1)$P\cup\overline{fcl(P)}$ 是一个泛活性;

(2)$P\cup\overline{ncl(P)}$ 是一个存在活性;

(3)若 $P\in EL$,则 $P\in UL$。

证明:这里只给出引理 5 中(1)和(3)的证明。

引理 5 中(1)的证明:由定理 1 可知:

$$\begin{aligned}ncl(P\cup\overline{fcl(P)})&=ncl(P)\cup ncl(\mathbb{T}^{tot}\backslash ncl(P))\\&\supseteq P\cup(\mathbb{T}^{tot}\backslash ncl(P))\\&=\mathbb{T}^{tot}\end{aligned}$$

因此,$ncl(P\cup\overline{fcl(P)})=\mathbb{T}^{tot}$。

引理 5 中(3)的证明:若 $P\in EL$,由定理 3 可知,则 $ncl(P)=\mathbb{T}^{tot}$。又由定理 1 可知,$ncl(P)\subseteq fcl(P)$。故$\mathbb{T}^{tot}\subseteq fcl(P)$。因此 $fcl(P)=\mathbb{T}^{tot}$。

若两个属性是子集关系且子集为活性,则它的超集也为活性,同时我们也给出了活性在交和并运算下仍然是活性的证明方法。

引理 6 设 $P,Q\subseteq\mathbb{T}^{tot}$,则以下结论成立:

(1)若 $P\subseteq Q$ 且 $P\in UL$,则 $Q\in UL$;

(2)若 $P\subseteq Q$ 且 $P\in EL$,则 $Q\in EL$;

(3)若 $P\in UL$ 或 $Q\in UL$,则 $P\cup Q\in UL$;

(4)若 $P\in EL$ 或 $Q\in EL$,则 $P\cup Q\in EL$;

(5)若 $P,Q\in UL$ 且 $P\cap Q\neq\emptyset$,则 $P\cap Q\in UL$;

(6)若 $P,Q\in EL$ 且 $P\cap Q\neq\emptyset$,则 $P\cap Q\in EL$。

证明:我们只给出引理 6 中(1),(3)和(5)的证明,引理 6 中(2),(4)和(6)的证明类似,故省略。

引理 6 中(1)的证明:若 $P\in UL$,根据定理 3 可知,$fcl(P)=\mathbb{T}^{tot}$。因为$P\subseteq Q$,所以由命题 1 可知 $fcl(P)\subseteq fcl(Q)$。故$\mathbb{T}^{tot}\subseteq fcl(Q)$。因此 $fcl(Q)=\mathbb{T}^{tot}$。

引理 6 中(3)的证明:若 $P\in UL$,根据定理 3 知,则 $fcl(P)=\mathbb{T}^{tot}$。又因为 $fcl(P\cup Q)=fcl(P)\cup fcl(Q)$,所以 $fcl(P\cup Q)=\mathbb{T}^{tot}$。因此,$P\cup Q$ 是一个泛活性。

引理 6 中(5)的证明:设 $T_1\in\mathbb{T}^{f}$ 是任意一棵有限深度树,因为 $P\cap Q\neq\emptyset$,所以设 $T\in P\cap Q$,通过在 T_1 的所有叶子结点连接 T 之后得到 $T_2\in\mathbb{T}^{tot}$。因为 P 和 Q 都是泛活性属性,所以 $T_2\in P$ 且 $T_2\in Q$。因此 $T_2\in P\cap Q$。

6 安全性和活性的交

本节将研究安全性与活性之间的关系,给出每个属性可以表达为安全性和活性的交的分解结果。

定理 4 设 $P\subseteq\mathbb{T}^{tot}$,则下列结论成立:

(1)$P=fcl(P)\cap(P\cup fcl(P))$;

(2)$P=ncl(P)\cap(P\cup ncl(P))$;

(3)$P=ncl(P)\cap(P\cup fcl(P))$。

证明:这里只给出定理 4 中(1)和(3)的证明,定理 4 中(2)的证明类似,故省略。

定理 4 中(1)的证明:由定理 2 可知,$fcl(P)$是一个泛安全性,又由引理 5 中的(1)可知 $P\cup\overline{fcl(P)}$是一个泛活性。观察到:

$$\begin{aligned}&fcl(P)\cap(P\cup\overline{fcl(P)})\\&=(fcl(P)\cap P)\cup(fcl(P)\cap\overline{fcl(P)})\\&=P\cup(fcl(P)\cap\overline{fcl(P)})\\&=P\cup\emptyset=P\end{aligned}$$

因此,P 是一个泛安全性和泛活性的交。

定理 4 中(3)的证明:根据定理 2 可知,$ncl(P)$是一个存在安全性,又由引理 5 可知 $P\cup\overline{fcl(P)}$是一个泛活性。因为 $ncl(P)\subseteq fcl(P)$,观察到:

$$\begin{aligned}&ncl(P)\cap(P\cup\overline{fcl(P)})\\&=(ncl(P)\cap P)\cup(ncl(P)\cap\overline{fcl(P)})\\&=P\cup(ncl(P)\cap\overline{fcl(P)})\\&=P\cup\emptyset=P\end{aligned}$$

所以,P 是一个存在安全性和泛活性的交。

下面将考虑全体安全性和全体活性的交的结果。

引理 7 全体安全性和全体活性的交有以下 3 种情况:

(1)$US\cap UL=\{\mathbb{T}^{tot}\}$;

(2)$ES\cap EL=\{\mathbb{T}^{tot}\}$;

(3)$US\cap EL=\{\mathbb{T}^{tot}\}$。

证明:这里只给出引理 7 中(1)的证明,引理 7 中(2)和(3)的证明类似,故省略。若 $P\in US\cap UL$,则 $P\in US$ 且 $P\in UL$。由定理 2 和定理 3 可知,$P=fcl(P)$且 $fcl(P)=\mathbb{T}^{tot}$。因此 $P=\mathbb{T}^{tot}$。

下面给出一些性质,并阐述安全性 、活性以及属性的闭包之间的关系。

命题 2 设 $P,P_{\text{usafe}},P_{\text{esafe}},P_{\text{ulive}}$ 和 P_{elive} 分别为分支时间属性、泛安全性、存在安全性、泛活性和存在活性,则下列结论成立:

(1)若 $P=P_{\text{usafe}}\cap P_{\text{ulive}}$,则 $fcl(P)\subseteq P_{\text{usafe}}$ 且 $P_{\text{ulive}}\subseteq P\cup\overline{fcl(P)}$;

(2)若 $P=P_{\text{esafe}}\cap P_{\text{elive}}$,则 $fcl(P)\subseteq P_{\text{esafe}}$ 且 $P_{\text{elive}}\subseteq P\cup\overline{fcl(P)}$;

(3)若 $P=P_{\text{esafe}}\cap P_{\text{ulive}}$,则 $fcl(P)\subseteq P_{\text{esafe}}$ 且 $P_{\text{ulive}}\subseteq P\cup\overline{fcl(P)}$;

证明:这里只给出命题 2 中(1)的证明,命题 2 中(2)和(3)的证明类似,故省略。设 $P=P_{\text{usafe}}\cap P_{\text{ulive}}$,则 $P\subseteq P_{\text{usafe}}$。由引理 6 可知,$fcl(P)\subseteq fcl(P_{\text{usafe}})$。因为 P_{usafe} 是一个泛安

全性，所以 $fcl(P_{usafe})=P_{usafe}$。故 $fcl(P)\subseteq P_{usafe}$。要证明 $P_{ulive}\subseteq P\cup\overline{fcl(P)}$，只需要证明 $fcl(P_{ulive})\subseteq fcl(P\cup\overline{fcl(P)})$。因为 P_{ulive} 是一个泛活性，所以 $fcl(P_{ulive})=\mathbb{T}^{tot}$。又由定理 1 可知：

$$\begin{aligned}fcl(P\cup\overline{fcl(P)})&=fcl(P)\cup fcl(\overline{fcl(P)})\\&\supseteq fcl(P)\cup\overline{fcl(P)}\\&=\mathbb{T}^{tot}\end{aligned}$$

因此，$P_{ulive}\subseteq P\cup\overline{fcl(P)}$。

结束语 本文研究了分支时间属性中安全性和活性在模糊背景下的一种推广形式。首先通过引入模糊树的概念，定义了模糊树之间的前缀关系；然后定义出两种闭包操作，对安全性和活性提供了一种闭包刻画，同时定义了两种安全性和两种活性；最后证明了每个分支时间属性，或是存在安全性和存在活性的交，或是泛安全性和泛活性的交，或是存在安全性和泛活性的交。

未来的工作中，我们将考虑分支时间属性，特别是安全性和活性的逻辑刻画，并研究相关的验证算法。

参 考 文 献

[1] WANG J, ZHAN N J, FENG X Y, et al. Overview of formal methods[J]. Journal of Software, 2019, 30(1): 33-61.

[2] BAIER C, KATOEN J P. Principles of model checking [M]. Cambridge, MA: The MIT Press, 2008.

[3] LIN H M, ZHANG W H. Model checking: theories, techniques and applications[J]. Acta Electronica Sinica, 2002, 30(12A): 1907-1912.

[4] WANG Z Z. Survey of Model Checking[J]. Computer Science, 2013, 40(Z6): 1-14.

[5] WEI O, SHI Y F, XU B F, et al. Abstract Modeling Formalisms in Software Model Checking[J]. Journal of Computer Research and Development, 2015, 52(7): 1580-1603.

[6] HAN Y J, ZHOU Q L, ZHU W J. Survey on DNA-computing Based Methods of Computation Tree Logic Model Checking[J]. Computer Science, 2019, 46(11): 25-31.

[7] LIU Y, LI X D, MA Y. Model abstraction for stochastic model checking[J]. Journal of Software, 2015, 26(8): 1853-1870.

[8] LIU Y, LI X D, MA Y, et al. Survey for Stochastic Model Checking[J]. Chinese Jour-nal of Computers, 2015, 38(11): 2145-2162.

[9] CHECHIK M, DEVEREUX B, EASTERBRO-OK S, et al. Multi-valued symbolic model-checking[J]. ACM Transactions on Software Engineering and Methodology, 2003, 12(4): 371-408.

[10] LI Y M. Quantitative model checking of linear-time properties based on generalized possibility measures[J]. Fuzzy Sets and Systems, 2017, 320: 17-39.

[11] DENG H, XUE Y, LI Y L, et al. Computation Tree Logic CTL* Based on Possibility Measure and Possibilistic Bisimulation[J]. Computer Science, 2012, 39(10): 258-263.

[12] LEI L H, WANG J. Parallelization of LTL model checking based on possibility measure [J]. Computer Science, 2018, 45(4): 71-75.

[13] PAN H Y, LI Y M, CAO Y Z, et al. Model checking fuzzy computation tree logic[J]. Fuzzy Sets and Systems, 2015, 262: 60-77.

[14] PAN H Y, LI Y M, CAO Y Z, et al. Model checking computation tree logic over finite lattices[J]. Theoretical Computer Science, 2016, 612(C): 45-62.

[15] LIANG C J, LI Y M. Model checking of fuzzy linear temporal logic based on generalized possibility measures[J]. Acta Electronica Sinica, 2017, 45(12): 2971-2977.

[16] FARAN R, KUPFERMAN O. Spanning the spectrum from safety to liveness[J]. Acta Informatica, 2018, 55(8): 703-732.

[17] ALPERN B, DEMERS A J, SCHNEIDER F B. Safety without stuttering[J]. Information Proce-ssing Letters, 1986, 23(4): 177-180.

[18] KUPFERMAN O, VARDI M Y. Model checking of safety properties[J]. Formal Methods in System Design, 2001, 19(3): 291-314.

[19] LAMPORT L. Proving the Correctness of Multip-rocess Programs[J]. IEEE Transactions on Software Engineering, 1977, SE-3(2): 125-143.

[20] ALPERN B, SCHNEIDER F B. Defining liveness[J]. Information Processing Letters, 1985, 21(4): 181-185.

[21] ALPERN B, SCHNEIDER F B. Recognizing safety and liveness [J]. Distributed Computing, 1987, 2(3): 117-126.

[22] SISTLA A P. Safety, liveness and fairness in temporal logic[J]. Formal Aspects of Computing, 1994, 6(5): 495-511.

[23] LI Y M, DROSTE M, LEI L H. Model checkin-g of linear-time properties in multi-valued systems [J]. Information Sciences, 2017, 377: 51-74.

[24] MANOLIOS P, TTEFLER R. Safety and liven-ess in branching time[C]// In LICS. IEEE Computer Society, 2001: 366-374.

[25] BOUAJJANI A, FERNANDEZ J C. Safety for branching time semantics[C]// 18th ICALP. LNCS 510, 1991: 76-92.

[26] KATOEN J P, LEI S, ZHANG L. Probably safe or live[C]// Eacsl Conference on Computer Science Logic. 2014: 1-10.

[27] ZHANG X H, WU D P, DAI J H. Fuzzy Mathematics and Rough Set Theory [M]. Beijing: Tsinghua University Press, 2012.

[28] MANTACI S, RESTIVO A. Codes and equations on trees [J]. Theoretical Computer Science, 2001, 255(1/2): 483-509.

SHI Tie-zhu, born in 1995, master. His main research interests include formal verification and so on.

PAN Hai-yu, born in 1976, Ph.D, associate professor, M.S supervisor, is a member of China Computer Federation. His main research interests include formal verification and so on.