计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.191000175

基于度量线性时态逻辑的近似安全性

蔡 泳 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
(caiyong1710@163.com)

摘 要 近年来,计算机系统的定量验证已经引起了学术界和工业界足够的关注,其中取值于度量空间的系统性质研究为定量验证的发展开辟了一条新途径。在系统验证中常用线性时间属性来刻画系统的性质,而安全性作为线性时间属性中一类至关重要的基础属性,能保证系统在运行过程中不会发生“坏”的事情,其在度量背景下的推广形式也应该得到关注。为此,文中研究伪超度量空间上安全性的扩展问题,首先对已有的度量线性时态逻辑进行适当的补充,使其能充分地刻画度量背景下的线性时间属性;然后引入距离阈值 α,提出一种 α-安全性的概念,从而将经典的安全性提升到伪超度量空间上;最后讨论度量线性时态逻辑与 α-安全性之间的关系。这些结论为取值于度量空间的系统的安全性验证提供了理论依据。

关键词:安全性;模型检测;线性时间属性;线性时态逻辑;伪超度量空间
中图法分类号 TP301

Approximate Safety Properties in Metric Linear Temporal Logic

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

Abstract In recent years, quantitative verification of computer systems has attracted much attention from the academic and industrial communities, where the study of system specifications over metric spaces has offered a new research line for the development of quantitative verification. In system verification, linear time attribute is often used to describe the properties of the system, and security, as one of the most important basic attributes of linear time attribute, can assert that nothing "bad" happens during execution of systems. Hence the extension of safety properties should also be concerned in the context of metrics. This paper investigates safety properties over pseudo-ultrametric spaces. First, metric linear temporal logic (MLTL) is used to characterize linear-time properties in the context of metrics metrics. Then, this paper lifts the notion of safety properties to pseudo-ultrametric spaces, called α-safety properties, by introducing the distance threshold α. Finally, the relationship between MLTL and α-safety properties is discussed. These results provide a theoretical basis for the verification of safety properties in the context of metrics.

Keywords Safety property, Model checking, Linear-time property, Linear temporal logic, Pseudo-ultrametric space

1 引言

模型检测作为计算机系统验证中一种高度自动化的验证技术[1],自提出以来其影响力从学术界辐射到了工业界,目前已成功应用到不同的领域中。在计算机系统验证中,线性时态逻辑[2](Linear Temporal Logic,LTL)用于刻画计算机系统的性质,这些性质又被称为线性时间属性。这是迈向构建模型检测理论重要的一步,现已得到了广泛的应用[3-9]。而线性时间属性中有两类备受关注的属性——安全性和活性,其中对安全性的研究一直是系统验证中的焦点问题,是研究线性时间属性的基础[1]。

安全性保证系统在运行过程中不会发生“坏”事情,其形式化的定义由 Alpern 等[10]给出。迄今为止,学术界对安全性的研究已经取得了许多进展[11-14],并且已有许多有效的方法可以对其进行验证[1]。特别地,Sistla[15]从 LTL 角度对安全性进行了刻画。

随着计算机系统的日趋复杂,许多实际的系统被赋予量化的行为特征。显然,经典的线性时间属性已经难以精确描述带有大量量化信息的系统行为。为此,人们对线性时间属性包括安全性进行了扩展。Li 等[16]基于 Heyting 代数将线性时间属性推广到多值逻辑上,并给出安全性在该逻辑上的形式化定义以及相应的验证方法。之后,Li 等[17]又研究了线

到稿日期:2019-10-27 返修日期:2020-05-08 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, China (2018GXNSFAA281326) and Foundation of Guangxi Key Laboratory of Trusted Software (kx201911).
通信作者:潘海玉(phyu76@126.com)

性时间属性在可能性测度下的推广形式。Katoen 等[18]基于离散时间马尔可夫链研究了安全性的量化扩展问题。此外，形式化验证领域中还有许多类似的推广工作，具体请见文献[19-28]。

线性时间属性在度量背景下的量化扩展也得到了重视。Alfaro 等[29]将系统模型推广到度量空间上，利用线性距离和分支距离来刻画迹包含、迹等价以及(互)模拟关系，并给出了 LTL 在度量空间上一种定量的扩展形式。自然地，安全性在度量背景下也应该得到相应的推广，然而这一研究至今仍未受到关注。

本文研究伪超度量[30-32](Pseudo-ultrametric)上安全性的扩展问题。首先对文献[29]中的度量线性时态逻辑定义进行补充；然后通过引入距离阈值 α，将经典的安全性概念提升到伪超度量空间上，称之为 α-安全性；最后在度量线性时态逻辑与 α-安全性之间建立关系，从该逻辑角度对 α-安全性进行刻画，并表明经典安全性在 LTL 中的刻画形式是本文结论的一种特殊情形。

2 预备知识

本节首先回顾一些概念与定义，这些内容主要来源于文献[1,29-32]。为了便于叙述，约定以下记号：$\mathbf{N}$ 表示自然数集；对于任意 $x,y\in[0,1]$，$x\vee y$ 与 $x\wedge y$ 分别表示 $\max(x,y)$ 与 $\min(x,y)$；设 S 为一个集合，S^* (S^ω)表示由 S 中的元素构成的所有有限(无限)字符串的集合；给定 $\lambda\in S^*\cup S^\omega$，$\lambda'\in S^*$ 与 $i\in\mathbf{N}$，$\lambda'\lambda$，$|\lambda'|$，λ_i 和 λ^i 分别表示 λ' 和 λ 的连接、λ' 的长度、λ 中第 $i+1$ 个元素，以及 λ 的后缀 $\lambda_i\lambda_{i+1}\cdots$；$pref(\lambda)$ 表示 λ 的所有前缀构成的集合。

设 X 为一个非空集合，称函数 $d:X\times X\to[0,1]$ 为 X 上的一个伪超度量，如果对于任意 $x,y,z\in X$，则满足以下 3 个条件：

(1) $d(x,x)=0$；

(2) $d(x,y)=d(y,x)$；

(3) $d(x,z)\leqslant d(x,y)\vee d(y,z)$。

二元组 (X,d) 表示一个伪超度量空间，在不致混淆时，(X,d) 简记为 X。除非特别声明，否则本文讨论的集合 X 是有限的。

设 AP 为原子命题集，函数 $v:AP\to X$ 称为 AP 的一个赋值。AP 在伪超度量空间 X 上的所有赋值的集合记为 $V(AP)$。一个度量线性时间属性 (Metric Linear-Time Property，MLT Property) P 是 $(V(AP))^\omega$ 的一个子集，即 $P\subseteq(V(AP))^\omega$。

命题距离 PD 刻画赋值之间的关系，其定义为：

对于任意 $u,v\in V(AP)$，有：

$$PD(u,v)=\max_{p\in AP}d(u(p),v(p))$$

迹距离 TD 刻画 $(V(AP))^\omega$ 中串之间的关系，定义为：

对于任意 $\sigma,\rho\in(V(AP))^\omega$，有：

$$TD(\sigma,\rho)=\sup_{i\in\mathbf{N}}PD(\sigma_i,\rho_i)$$

线性距离 D 刻画 MLT 属性之间的关系，定义为：

对于任意 $P_1,P_2\subseteq(V(AP))^\omega$，有：

$$D(P_1,P_2)=\sup_{\sigma\in P_1}\inf_{\rho\in P_2}TD(\sigma,\rho)$$

记 $D(\sigma,P_1)$ 为 $\inf\limits_{\rho\in P_1}TD(\sigma,\rho)$。

3 α-安全性

本节首先对文献[29]中引入的度量线性时态逻辑的定义做适当的补充；然后，将经典的安全性概念提升到伪超度量空间上，定义一种近似安全性；最后，在度量线性时态逻辑与所定义的近似安全性之间建立关系。

下面给出度量线性时态逻辑的语法定义，这是 LTL 正范式(Positive Normal Form)[1]的一种定扩展形式。

定义 1 给定原子命题集 AP 与伪超度量空间 X，AP 上的度量线性时态逻辑 (Metric Linear Temporal Logic，MLTL) 公式的语法递归定义如下：

$$\varphi::=\text{true}\mid\text{false}\mid M(p,c)\mid\varphi_1\wedge\varphi_2\mid\varphi_1\vee\varphi_2\mid X\varphi\mid G\varphi\mid\varphi_1U\varphi_2$$

其中，$p\in AP$，$c\in X$。

下面给出 MLTL 公式在 $(V(AP))^\omega$ 上的语义解释。

定义 2 设 φ 为一个 MLTL 公式，φ 在 $(V(AP))^\omega$ 上的语义解释是一个映射 $\|\varphi\|:(V(AP))^\omega\to[0,1]$，递归定义如下：

对于任意 $\sigma\in(V(AP))^\omega$，有：

$$\|\text{true}\|(\sigma)=1$$

$$\|\text{false}\|(\sigma)=0$$

$$\|M(p,c)\|(\sigma)=d(\sigma_0(p),c)$$

$$\|\varphi_1\wedge\varphi_2\|(\sigma)=\min(\|\varphi_1\|(\sigma),\|\varphi_2\|(\sigma))$$

$$\|\varphi_1\vee\varphi_2\|(\sigma)=\max(\|\varphi_1\|(\sigma),\|\varphi_2\|(\sigma))$$

$$\|X\varphi\|(\sigma)=\|\varphi\|(\sigma^1)$$

$$\|G\varphi\|(\sigma)=\inf_{i\in\mathbf{N}}\|\varphi\|(\sigma^i)$$

$$\|\varphi_1U\varphi_2\|(\sigma)=\sup_{i\in\mathbf{N}}\inf_{0\leqslant j<i}(\|\varphi_1\|(\sigma^j)\wedge\|\varphi_2\|(\sigma^j))$$

此外，根据 MLTL 公式的定义，可以衍生出运算符 F 和 W，它们分别被定义为：

$$F\varphi=\text{true}\,U\varphi$$

$$\varphi_1W\varphi_2=(\varphi_1U\varphi_2)\vee G\varphi_1$$

相应地，可以得到它们在 $(V(AP))^\omega$ 上的语义解释，具体内容如下。

引理 1 对于任意 $\sigma\in(V(AP))^\omega$，有：

(1) $\|F\varphi\|(\sigma)=\sup\limits_{i\in\mathbf{N}}\|\varphi\|(\sigma^i)$；

(2) $\|\varphi_1W\varphi_2\|(\sigma)=\sup\limits_{i\in\mathbf{N}}\inf\limits_{0\leqslant j<i}(\|\varphi_1\|(\sigma^j)\wedge\|\varphi_2\|(\sigma^j))\vee\inf\limits_{k\in\mathbf{N}}\|\varphi_1\|(\sigma^k)$。

证明：由定义 2 知(2)显然成立，以下为(1)的证明过程。

$$\begin{aligned}\|F\varphi\|(\sigma)&=\|\text{true}\,U\varphi\|(\sigma)\\&=\sup_{i\in\mathbf{N}}\inf_{0\leqslant j<i}(\|\text{true}\|(\sigma^j)\wedge\|\varphi\|(\sigma^i))\\&=\sup_{i\in\mathbf{N}}\inf_{0\leqslant j<i}(1\wedge\|\varphi\|(\sigma^i))\\&=\sup_{i\in\mathbf{N}}\|\varphi\|(\sigma^i)\end{aligned}$$

给定一个 MLTL 公式 φ 与阈值 $\alpha\in[0,1]$，φ 在 α 约束下表示一个 MLT 属性。

$$L_\alpha(\varphi)=\{\sigma\in(V(AP))^\omega:\|\varphi\|(\sigma)>\alpha\}$$

注 1：(1)本文的 MLTL 公式是在文献[29]提出的度量线性时态逻辑的基础上，增加了 true、false 以及运算符 U 的定

义，其中 true 在 $(V(AP))^{\omega}$ 上用于刻画 $(V(AP))^{\omega}$ 本身；根据定义 2，当 $\alpha<1$ 时，$L_{\alpha}(\text{true})=(V(AP))^{\omega}$。由于 LTL 正范式中的 p 和 $\neg p$ 在 MLTL 中由 $M(p,0)$ 与 $M(p,1)$ 来刻画，且 MLTL 不再使用经典情形中的 $\neg$ 算子，自然地，定义 1 中增加了 false 用于刻画空集 $\emptyset$。同时，LTL 中的算子 U 作为一种常用的运算符，也应该有相应的扩展。

(2)当伪超度量空间 $X=(\{0,1\},d)$ 且 α 取值为 0 时，MLT 属性即为经典的线性时间属性，此时 MLTL 公式的语义退化为 LTL 公式的语义，其中不出现时序运算符如 X，G 与 U 的公式，称为命题逻辑公式。

接下来研究安全性在度量背景下的推广形式，首先简单回顾一下经典安全性的定义。

定义 3[1]　设 $P\subseteq(2^{AP})^{\omega}$，称 P 为一个安全性，如果对于任意 $\lambda\in(2^{AP})^{\omega}\backslash P$，存在前缀 $\overset{\wedge}{\lambda}\in pref(\lambda)$，使得对于任意 $\lambda'\in(2^{AP})^{\omega}$，有 $\lambda\lambda'\notin P$，则 $\overset{\wedge}{\lambda}$ 被称为 P 的一个坏前缀。

下面通过引入距离阈值 α 来定义一种近似安全性，这类安全性是 MLT 属性的一个子集，称之为 α-安全性。

定义 4　设阈值 $\alpha\in[0,1]$，P 为 AP 上的一个 MLT 属性。称 P 为 α-安全性，如果对于任意 $\sigma\notin P$，存在前缀 $\overset{\wedge}{\sigma}\in pref(\sigma)$，使得对于任意 $\sigma'\in(V(AP))^{\omega}$，有 $D(\overset{\wedge}{\sigma}\sigma',P)>\alpha$，则 $\overset{\wedge}{\sigma}$ 被称为 P 的一个坏前缀。

注 2：当伪超度量空间 $X=(\{0,1\},d)$ 时，对于一个 0-安全性 P，由定义 4 知任意 $\sigma\notin P$ 都存在前缀 $\overset{\wedge}{\sigma}\in pref(\sigma)$，使得对任意 $\sigma'\in(V(AP))^{\omega}$ 有 $D(\overset{\wedge}{\sigma}\sigma',P)>0$，即 $\overset{\wedge}{\sigma}\sigma'\notin P$。因此，0-安全性刻画了经典的安全性。

根据定义 4，不同的 α-安全性之间也有一定的关系，具体内容如下。

命题 1　给定一个 α-安全性 P，若 $\alpha'\in[0,1]$ 且 $\alpha'\leqslant\alpha$，则 P 也是一个 α'-安全性。

证明：因为 P 是一个 α-安全性，由定义 4 知对于任意 $\sigma\notin P$，存在前缀 $\overset{\wedge}{\sigma}\in pref(\sigma)$，使得对于任意 $\sigma'\in(V(AP))^{\omega}$，有 $D(\overset{\wedge}{\sigma}\sigma',P)>\alpha\geqslant\alpha'$。再根据定义 4 可得 P 是一个 α'-安全性。

特别地，$(V(AP))^{\omega}$ 是一个 1-安全性，此时根据命题 1，对于任意 $\alpha\in[0,1]$，$(V(AP))^{\omega}$ 也是一个 α-安全性；对于空集 $\emptyset$，将它定义为一个特殊的 α-安全性。

下面给出了一个伪超度量空间的实例。

例 1　设 $[0,1]_f$ 为 $[0,1]$ 的一个有限子集，$X_1=([0,1]_f,d_1)$，其中 d_1 被定义为：

对于任意 $x,y\in[0,1]_f$，有：

$$d_1(x,y)=\begin{cases}y\vee(1-x), & x<y\\ 0, & x=y\\ x\vee(1-y), & x>y\end{cases}$$

本文证明 d_1 满足伪超度量的 3 个条件。设 $x,y,z\in[0,1]_f$，显然 $d_1(x,x)=0$ 且 $d_1(x,y)=d_1(y,x)$ 成立。对于伪超度量条件(3)的证明，分以下情形进行讨论：

(1)当 $x=y$ 时，有 $d_1(x,y)=0\leqslant d_1(x,z)\vee d_1(z,y)$。

(2)当 $x=z$ 时，有 $d_1(x,y)=d_1(z,y)$。由此可得 $d_1(x,y)\leqslant d_1(x,z)\vee d_1(z,y)$。$y=z$ 这一情形与此类似，故省略。

(3)当 $x<y<z$ 时，有 $y\vee(1-x)\leqslant z\vee(1-x)$，进而有 $y\vee(1-x)\leqslant z\vee(1-x)\vee z\vee(1-y)$，即 $d_1(x,y)\leqslant d_1(x,z)\vee d_1(z,y)$。$y<x<z$ 这一情形与此类似，故省略。

(4)当 $x<z<y$ 时，有 $y\vee(1-x)=(1-x)\vee y$，进而有 $y\vee(1-x)\leqslant z\vee(1-x)\vee y\vee(1-z)$，即 $d_1(x,y)\leqslant d_1(x,z)\vee d_1(z,y)$。$y<z<x$ 这一情形与此类似，故省略。

(5)当 $z<x<y$ 时，有 $y\vee(1-x)\leqslant y\vee(1-z)$，进而有 $y\vee(1-x)\leqslant x\vee(1-z)\vee y\vee(1-z)$，即 $d_1(x,y)\leqslant d_1(x,z)\vee d_1(z,y)$。$z<y<x$ 这一情形与此类似，故省略。

综上所述，d_1 是 $[0,1]_f$ 上的一个伪超度量，因此 X_1 是一个伪超度量空间。

下面给出一个 α-安全性的简单例子。

例 2　设 $AP=\{p\}$，$V(AP)$ 为 AP 在 X_1 上所有赋值的集合，P_{safe} 为 AP 上的一个 MLT 属性且表示“原子命题 p 被赋予的值总是在 $[0,0.3)$ 或 $(0.7,1]$ 范围内浮动”。P_{safe} 为 0.7-安全性。其原因如下：设 $\sigma\notin P_{\text{safe}}$，则存在 $k\in\mathbf{N}$ 使得 $0.3\leqslant\sigma_k(p)\leqslant0.7$。令 $\rho\in P_{\text{safe}}$，必然有 $\rho_k(p)<0.3$ 或者 $\rho_k(p)>0.7$。当 $\rho_k(p)<0.3$ 时，由 PD 的定义知：

$$\begin{aligned}PD(\sigma_k,\rho_k)&=d_1(\sigma_k(p),\rho_k(p))\\&=\sigma_k(p)\vee(1-\rho_k(p))\\&>0.7\end{aligned}$$

当 $\rho_k(p)>0.7$ 时，有：

$$\begin{aligned}PD(\sigma_k,\rho_k)&=d_1(\sigma_k(p),\rho_k(p))\\&=\rho_k(p)\vee(1-\sigma_k(p))\\&>0.7\end{aligned}$$

不妨设 $\overset{\wedge}{\sigma}=\sigma_0,\cdots,\sigma_k$，然后将 $\overset{\wedge}{\sigma}$ 扩展为 $\sigma'\in(V(AP))^{\omega}$。由此可得：

$$\begin{aligned}TD(\sigma',\rho)&=\sup_{i\in\mathbf{N}}PD(\sigma_i',\rho_i)\\&\geqslant PD(\sigma_k,\rho_k)\\&>0.7\end{aligned}$$

因为 X_1 是有限集 $[0,1]_f$ 上的伪超度量空间，故：

$$D(\sigma',P_{\text{safe}})=\inf_{\rho'\in P_{\text{safe}}}TD(\sigma',\rho')>0.7$$

换句话说，σ 中存在前缀 $\overset{\wedge}{\sigma}$，将 $\overset{\wedge}{\sigma}$ 扩展为 σ'，有 $D(\sigma',P_{\text{safe}})>0.7$，根据定义 4 可得 P_{safe} 是一个 0.7-安全性。

接下来研究定义 1 与定义 4 之间的关系，实现从 MLTL 角度对 α-安全性的刻画。首先给出 α-安全性公式的概念，一个 α-安全性公式在 α 约束下描述一个 α-安全性。

定义 5　设 φ 为一个 MLTL 公式，$\alpha\in[0,1]$。称 φ 为 α-安全性公式，如果 $L_{\alpha}(\varphi)$ 是一个 α-安全性。

注 3：注意到当伪超度量空间 $X=(\{0,1\},d)$ 且 α 取值为 0 时，α-安全性即为经典的安全性，自然地，此时的 α-安全性公式即为 LTL 安全性公式[15]。

定理 1 作为本文的主要结论，给出了 MLTL 公式刻画 α-安全性的语法特征。

定理 1　设 AP 中的原子命题被赋值为伪超度量空间 X 上的元素，$p\in AP$，$c\in X$ 且 $\alpha\in[0,1]$。true，false 和 $M(p,c)$ 是 α-安全性公式，且如果 φ_1 与 φ_2 是 α-安全性公式，则 $\varphi_1\wedge$

φ_2, $\varphi_1 \vee \varphi_2$, $X\varphi_1$, $G\varphi_1$ 和 $\varphi_1 W \varphi_2$ 都是 α-安全性公式。

证明：设 φ 为一个 MLTL 公式，对 φ 采用结构归纳法来证明定理 1。

基础：当 φ = true 时，由定义 2 知对于任意 $\sigma \in (V(AP))^{\omega}$，有 $\| \varphi \|(\sigma)=1$。若 $\alpha=1$，则根据 $L_{\alpha}(\varphi)$ 的定义可得 $L_{\alpha}(\varphi)=\emptyset$。若 $\alpha<1$，则有 $L_{\alpha}(\varphi)=(V(AP))^{\omega}$。因为 $\emptyset$ 和 $(V(AP))^{\omega}$ 都是 α-安全性，所以 φ 是一个 α-安全性公式。

当 φ = false 时，由定义 2 知对于任意 $\sigma \in (V(AP))^{\omega}$，有 $\| \varphi \|(\sigma)=0$。根据 $L_{\alpha}(\varphi)$ 的定义可得 $L_{\alpha}(\varphi)=\emptyset$。因为 $\emptyset$ 是一个 α-安全性，所以 φ 是一个 α-安全性公式。

当 $\varphi=M(p,c)$ 时，设 $\sigma \notin L_{\alpha}(\varphi)$，由 $L_{\alpha}(\varphi)$ 的定义知 $\| \varphi \|(\sigma) \leqslant \alpha$。根据定义 2，有 $d(\sigma_0(p),c) \leqslant \alpha$。令 $\rho \in L_{\alpha}(\varphi)$，由 $L_{\alpha}(\varphi)$ 的定义知 $\| \varphi \|(\rho)>\alpha$，即 $d(\rho_0(p),c)>\alpha$。注意到 d 是一个伪超度量，根据 $d(\rho_0(p),c) \leqslant d(\sigma_0(p),\rho_0(p)) \vee d(\sigma_0(p),c)$ 可得 $d(\sigma_0(p),\rho_0(p))>\alpha$。此时将 σ_0 扩展为 $\sigma' \in (V(AP))^{\omega}$，因此有：

$$\begin{aligned} TD(\sigma',\rho) &= \sup_{i \in \mathbf{N}} PD(\sigma_i',\rho_i) \\ &\geqslant PD(\sigma_0,\rho_0) \\ &= \max_{r \in AP} d(\sigma_0(r),\rho_0(r)) \\ &\geqslant d(\sigma_0(p),\rho_0(p)) \\ &> \alpha \end{aligned}$$

换句话说，将 σ_0 扩展为 σ'，对于 $L_{\alpha}(\varphi)$ 中的串 ρ，有 $TD(\sigma',\rho)>\alpha$。因为 X 是有限的，故：

$$D(\sigma',L_{\alpha}(\varphi))=\inf_{\rho' \in L_{\alpha}(\varphi)} TD(\sigma',\rho')>\alpha$$

根据定义 4 可得，σ_0 为 $L_{\alpha}(\varphi)$ 的坏前缀，$L_{\alpha}(\varphi)$ 是一个 α-安全性。因此，φ 是一个 α-安全性公式。

归纳：当 $\varphi=\varphi_1 \wedge \varphi_2$ 时，设 $\sigma \notin L_{\alpha}(\varphi)$，由 $L_{\alpha}(\varphi)$ 的定义知 $\| \varphi \|(\sigma) \leqslant \alpha$，即：

$$\min(\| \varphi_1 \|(\sigma), \| \varphi_1 \|(\sigma)) \leqslant \alpha$$

不失一般性，设 $\| \varphi_1 \|(\sigma) \leqslant \alpha$，由 $L_{\alpha}(\varphi_1)$ 的定义知 $\sigma \notin L_{\alpha}(\varphi_1)$。因为 φ_1 是一个 α-安全性公式，所以 $L_{\alpha}(\varphi_1)$ 是一个 α-安全性，进而知 σ 中存在 $L_{\alpha}(\varphi_1)$ 的坏前缀 $\hat{\sigma}$，将 $\hat{\sigma}$ 扩展为无限字符串 $\sigma' \in (V(AP))^{\omega}$，有 $D(\sigma',L_{\alpha}(\varphi_1))>\alpha$。令 $\rho \in L_{\alpha}(\varphi)$，由 $L_{\alpha}(\varphi)$ 的定义知：

$$\min(\| \varphi_1 \|(\sigma), \| \varphi_1 \|(\sigma))>\alpha$$

显然有 $\| \varphi_1 \|(\rho)>\alpha$。再根据 $L_{\alpha}(\varphi_1)$ 的定义可得 $\rho \in L_{\alpha}(\varphi_1)$。注意到：

$$D(\sigma',L_{\alpha}(\varphi_1))=\inf_{\rho' \in L_{\alpha}(\varphi_1)} TD(\sigma',\rho')>\alpha$$

故 $TD(\sigma',\rho)>\alpha$。换句话说，将 $\hat{\sigma}$ 扩展为 σ'，对于 $L_{\alpha}(\varphi)$ 中的串 ρ，有 $TD(\sigma',\rho)>\alpha$。由此可得：

$$D(\sigma',L_{\alpha}(\varphi))=\inf_{\rho' \in L_{\alpha}(\varphi)} TD(\sigma',\rho')>\alpha$$

根据定义 4 知，$\hat{\sigma}$ 为 $L_{\alpha}(\varphi)$ 的坏前缀，$L_{\alpha}(\varphi)$ 是一个 α-安全性。因此，φ 是一个 α-安全性公式。

当 $\varphi=\varphi_1 \vee \varphi_2$ 时，设 $\sigma \notin L_{\alpha}(\varphi)$，由 $L_{\alpha}(\varphi)$ 的定义知 $\max(\| \varphi_1 \|(\sigma), \| \varphi_2 \|(\sigma)) \leqslant \alpha$，即 $\| \varphi_1 \|(\sigma) \leqslant \alpha$ 且 $\| \varphi_2 \|(\sigma) \leqslant \alpha$，进而有 $\sigma \notin L_{\alpha}(\varphi_1)$ 且 $\sigma \notin L_{\alpha}(\varphi_2)$。因为 φ_1 和 φ_2 都是 α-安全性公式，所以 σ 中存在 $L_{\alpha}(\varphi_1)$ 和 $L_{\alpha}(\varphi_2)$ 的坏前缀 $\hat{\sigma}$ 和 $\hat{\sigma}'$。不失一般性，设 $|\hat{\sigma}| \geqslant |\hat{\sigma}'|$，则 $\hat{\sigma}$ 也是 $L_{\alpha}(\varphi_2)$ 的坏前缀。将 $\hat{\sigma}$ 扩展为 $\sigma' \in (V(AP))^{\omega}$，有：

$$D(\sigma',L_{\alpha}(\varphi_1))>\alpha$$

$$D(\sigma',L_{\alpha}(\varphi_2))>\alpha$$

令 $\rho \in L_{\alpha}(\varphi)$，根据 $L_{\alpha}(\varphi)$ 的定义可得 $\max(\| \varphi_1 \|(\sigma), \| \varphi_2 \|(\sigma))>\alpha$。不失一般性，设 $\| \varphi_1 \|(\rho)>\alpha$，此时有 $\rho \in L_{\alpha}(\varphi_1)$。注意到 $D(\sigma',L_{\alpha}(\varphi_1))>\alpha$，故 $TD(\sigma',\rho)>\alpha$。由此可得：

$$D(\sigma',L_{\alpha}(\varphi))=\inf_{\rho' \in L_{\alpha}(\varphi)} TD(\sigma',\rho')>\alpha$$

根据定义 4 知，$\hat{\sigma}$ 为 $L_{\alpha}(\varphi)$ 的坏前缀，$L_{\alpha}(\varphi)$ 是一个 α-安全性。因此，φ 是一个 α-安全性公式。

当 $\varphi=X\varphi_1$ 时，设 $\sigma \notin L_{\alpha}(\varphi)$，由 $L_{\alpha}(\varphi)$ 的定义知 $\| \varphi_1 \|(\sigma^1) \leqslant \alpha$，进而有 $\sigma^1 \notin L_{\alpha}(\varphi_1)$。因为 φ_1 是一个 α-安全性公式，所以 σ^1 中存在 $L_{\alpha}(\varphi_1)$ 的坏前缀 $\hat{\sigma}$，将 $\hat{\sigma}$ 扩展为串 $\sigma' \in (V(AP))^{\omega}$，有 $D(\sigma',L_{\alpha}(\varphi_1))>\alpha$。令 $\rho \in L_{\alpha}(\varphi)$，由 $L_{\alpha}(\varphi)$ 的定义知 $\| \varphi_1 \|(\rho^1)>\alpha$，进而有 $\rho^1 \in L_{\alpha}(\varphi_1)$。因为：

$$D(\sigma',L_{\alpha}(\varphi_1))>\alpha$$

故 $TD(\sigma',\rho^1)>\alpha$。注意到 $\sigma_0\hat{\sigma} \in pref(\sigma)$ 且 $\hat{\sigma} \in pref(\sigma')$，故 $\sigma_0\sigma'$ 也可视作 $\sigma_0\hat{\sigma}$ 的一个扩展。由此可得：

$$\begin{aligned} TD(\sigma_0\sigma',\rho) &= TD(\sigma_0\sigma',\rho_0\rho^1) \\ &\geqslant TD(\sigma',\rho^1) \\ &> \alpha \end{aligned}$$

换句话说，σ 中存在前缀 $\sigma_0\hat{\sigma}$，将 $\sigma_0\hat{\sigma}$ 扩展为 $\sigma_0\sigma'$，对于 $L_{\alpha}(\varphi)$ 中的串 ρ，有：

$$TD(\sigma_0\sigma',\rho)>\alpha$$

由此可得：

$$D(\sigma_0\sigma',L_{\alpha}(\varphi))=\inf_{\rho' \in L_{\alpha}(\varphi)} TD(\sigma_0\sigma',\rho')>\alpha$$

根据定义 4 知，$\sigma_0\hat{\sigma}$ 为 $L_{\alpha}(\varphi)$ 的坏前缀，$L_{\alpha}(\varphi)$ 是一个 α-安全性。因此，φ 是一个 α-安全性公式。

当 $\varphi=G\varphi_1$ 时，设 $\sigma \notin L_{\alpha}(\varphi)$，由 $L_{\alpha}(\varphi)$ 的定义知，存在 $j \in \mathbf{N}$，使得 $\| \varphi_1 \|(\sigma^j) \leqslant \alpha$，进而有 $\sigma^j \notin L_{\alpha}(\varphi_1)$。因为 φ_1 是一个 α-安全性公式，所以 σ^j 中存在 $L_{\alpha}(\varphi)$ 的坏前缀 $\hat{\sigma}$，将 $\hat{\sigma}$ 扩展为 $\sigma' \in (V(AP))^{\omega}$，有 $D(\sigma',L_{\alpha}(\varphi_1))>\alpha$。令 $\rho \in L_{\alpha}(\varphi)$，根据 $L_{\alpha}(\varphi)$ 的定义可得 $\| \varphi_1 \|(\rho^j)>\alpha$，进而有 $\rho^j \in L_{\alpha}(\varphi_1)$。因为 $D(\sigma',L_{\alpha}(\varphi_1))>\alpha$，所以 $TD(\sigma',\rho^j)>\alpha$。不妨设 $\hat{\sigma}'=\sigma_0,\cdots,\sigma_{j-1}$。注意到，$\hat{\sigma}'\hat{\sigma} \in pref(\sigma)$，故 $\hat{\sigma}'\sigma'$ 也可视为 $\hat{\sigma}'\hat{\sigma}$ 的一个扩展。由此可得：

$$\begin{aligned} TD(\hat{\sigma}'\sigma',\rho) &= \sup_{0 \leqslant i<j} PD(\sigma_i,\rho_i) \vee \sup_{k \in \mathbf{N}} PD(\sigma'_k,\rho_k^j) \\ &\geqslant TD(\sigma',\rho^j) \\ &> \alpha \end{aligned}$$

换句话说，σ 中存在前缀 $\hat{\sigma}'\hat{\sigma}$，将 $\hat{\sigma}'\hat{\sigma}$ 扩展为 $\hat{\sigma}'\sigma'$，对于 $L_{\alpha}(\varphi)$ 中的串 ρ，有：

$$TD(\hat{\sigma}'\sigma',\rho)>\alpha$$

因此，

$$D(\hat{\sigma}'\sigma',L_{\alpha}(\varphi))=\inf_{\rho' \in L_{\alpha}(\varphi)} TD(\hat{\sigma}'\sigma',\rho')>\alpha$$

根据定义4知，$\overset{\wedge}{\sigma}'\overset{\wedge}{\sigma}$为$L_\alpha(\varphi)$的坏前缀，$L_\alpha(\varphi)$是一个$\alpha$-安全性，故$\varphi$是一个$\alpha$-安全性公式。

当$\varphi=\varphi_1 W\varphi_2$时，设$\sigma\notin L_\alpha(\varphi)$，根据$L_\alpha(\varphi)$的定义可得$\inf\limits_{i\in\mathbf{N}}\|\varphi_1\|(\sigma^i)\leqslant\alpha$且$\sup\limits_{i\in\mathbf{N}}\inf\limits_{0\leqslant j<i}(\|\varphi_1\|(\sigma^j)\wedge\|\varphi_2\|(\sigma^j))\leqslant\alpha$，故存在$k\in\mathbf{N}$，使得$\|\varphi_1\|(\sigma^k)\leqslant\alpha$且对于任意$0\leqslant j\leqslant k$，$\|\varphi_2\|(\sigma^j)\leqslant\alpha$。因为$\varphi_1$和$\varphi_2$都是$\alpha$-安全性公式，所以$\sigma^k$中存在$L_\alpha(\varphi_1)$与$L_\alpha(\varphi_2)$的坏前缀$\overset{\wedge}{\sigma}$和$\overset{\wedge}{\sigma}'$。不失一般性，设$|\overset{\wedge}{\sigma}|\geqslant|\overset{\wedge}{\sigma}'|$，则$\overset{\wedge}{\sigma}$也是$L_\alpha(\varphi_2)$的坏前缀。将$\overset{\wedge}{\sigma}$扩展为$\sigma'\in(V(AP))^\omega$，有：

$D(\sigma',L_\alpha(\varphi_1))>\alpha$

$D(\sigma',L_\alpha(\varphi_2))>\alpha$

令$\rho\in L_\alpha(\varphi)$，根据$L_\alpha(\varphi)$的定义以及$\varphi_1 W\varphi_2$的语义解释，我们分以下两种情形进行讨论：

(1)ρ满足$\inf\limits_{i\in\mathbf{N}}\|\varphi_1\|(\rho^i)>\alpha$。此时，$\|\varphi_1\|(\rho^k)>\alpha$成立，故$\rho^k\in L_\alpha(\varphi_1)$。注意到$D(\sigma',L_\alpha(\varphi_1))>\alpha$，从而有$TD(\sigma',\rho^k)>\alpha$。不妨设$\overset{\wedge}{\sigma}''=\sigma_0\cdots\sigma_{k-1}$，于是有$TD(\overset{\wedge}{\sigma}''\sigma',\rho)\geqslant TD(\sigma',\rho^k)>\alpha$。

(2)ρ满足：

$$\sup_{i\in\mathbf{N}}\inf_{0\leqslant j<i}(\|\varphi_1\|(\rho^j)\wedge\|\varphi_2\|(\rho^j))>\alpha$$

即存在$k'\in\mathbf{N}$，使得：

$$\inf_{0\leqslant j<k'}(\|\varphi_1\|(\rho^j)\wedge\|\varphi_2\|(\rho^{k'}))>\alpha$$

若$k'>k$，显然$(\|\varphi_1\|(\rho^k)\wedge\|\varphi_2\|(\rho^{k'}))>\alpha$成立。由此知$\|\varphi_1\|(\rho^k)>\alpha$，故$\rho^k\in L_\alpha(\varphi_1)$。此时该情形与上一情形类似，同理可得$TD(\overset{\wedge}{\sigma}''\sigma',\rho)>\alpha$。若$k'=k$，则有$\|\varphi_2\|(\rho^k)=\|\varphi_2\|(\rho^{k'})>\alpha$，由此知$\rho^k\in L_\alpha(\varphi_2)$。注意到$D(\sigma',L_\alpha(\varphi_2))>\alpha$，故$TD(\sigma',\rho^k)>\alpha$。由此可得：

$$TD(\overset{\wedge}{\sigma}''\sigma',\rho)\geqslant TD(\sigma',\rho^k)>\alpha$$

若$k'<k$，已知$0\leqslant j\leqslant k$有$\|\varphi_2\|(\sigma^j)\leqslant\alpha$，故$\|\varphi_2\|(\sigma^{k'})\leqslant\alpha$。因为$\varphi_2$为$\alpha$-安全性公式，故$\sigma^{k'}$中存在$L_\alpha(\varphi_2)$的坏前缀$\overset{\wedge}{\sigma}''$，将$\overset{\wedge}{\sigma}''$扩展为：$\sigma''=\sigma_{k'}\cdots\sigma_{k-1}\overset{\wedge}{\sigma}'\cdots\in(V(AP))^\omega$，有$D(\sigma'',L_\alpha(\varphi_2))>\alpha$。由$\|\varphi_2\|(\rho^{k'})>\alpha$知$\rho^{k'}\in L_\alpha(\varphi_2)$，从而有$TD(\sigma'',\rho^{k'})>\alpha$。注意到$\overset{\wedge}{\sigma}''\sigma'=\sigma_0\cdots\sigma_{k-1}\overset{\wedge}{\sigma}'\cdots$，由此知$TD(\overset{\wedge}{\sigma}''\sigma',\rho)\geqslant TD(\sigma'',\rho^{k'})>\alpha$。

综上所述，σ中存在前缀$\overset{\wedge}{\sigma}''\overset{\wedge}{\sigma}$，将$\overset{\wedge}{\sigma}''\overset{\wedge}{\sigma}$扩展为$\overset{\wedge}{\sigma}''\sigma'$，对于$L_\alpha(\varphi)$中的串$\rho$，有：

$$TD(\overset{\wedge}{\sigma}''\sigma',\rho)>\alpha$$

因此

$$D(\overset{\wedge}{\sigma}''\sigma',L_\alpha(\varphi))=\inf_{\rho'\in L_\alpha(\varphi)}TD(\overset{\wedge}{\sigma}''\sigma',\rho')>\alpha$$

根据定义4知，$\overset{\wedge}{\sigma}''\overset{\wedge}{\sigma}$为$L_\alpha(\varphi)$的坏前缀，$L_\alpha(\varphi)$是一个$\alpha$-安全性，故$\varphi$是一个$\alpha$-安全性公式。

至此，定理1证明完毕。

当MLTL公式退化为LTL公式时，可以得到推论1。该推论已在文献[15]中被提出，是对经典安全性的刻画。

推论1　每个命题逻辑公式都是0-安全性公式，且如果φ_1与φ_2是0-安全性公式，则$\varphi_1\wedge\varphi_2$，$\varphi_1\vee\varphi_2$，$X\varphi_1$，$G\varphi_1$和$\varphi_1 W\varphi_2$都是0-安全性公式。

下面给出一个MLTL公式实例来刻画例2中提出的α-安全性。

例3　对于例2中的0.7-安全性P_{safe}，可以理解为原子命题p被赋予的值总是与0.5保持一定的距离进行波动。使用MLTL公式描述该属性，设$\varphi=GM(p,0.5)$且$\alpha=0.7$，此时有：

$$L_\alpha(\varphi)=\{\sigma:\|GM(p,0.5)\|(\sigma)>0.7\}$$

下面证明$L_\alpha(\varphi)=P_{\text{safe}}$。

首先采用反证法证明$L_\alpha(\varphi)\subseteq P_{\text{safe}}$。设存在$\sigma\in L_\alpha(\varphi)$且$\sigma\notin P_{\text{safe}}$。由$\sigma\notin P_{\text{safe}}$知存在$k\in\mathbf{N}$，使得$0.3\leqslant\sigma_k(p)\leqslant 0.7$，进而有$d_1(\sigma_k(p),0.5)\leqslant 0.7$。由定义2知：

$$\|M(p,0.5)\|(\sigma^k)=d_1(\sigma_k(p),0.5)\leqslant 0.7$$

由此可得：

$$\|GM(p,0.5)\|(\sigma)=\inf_{i\in\mathbf{N}}\|M(p,0.5)\|(\sigma^i)\leqslant 0.7$$

根据$L_\alpha(\varphi)$的定义知$\sigma\notin L_\alpha(\varphi)$。这与已知$\sigma\in L_\alpha(\varphi)$矛盾。

下面证明$P_{\text{safe}}\subseteq L_\alpha(\varphi)$。设$\sigma\in P_{\text{safe}}$，则对于任意$k\in\mathbf{N}$，有$\sigma_k(p)<0.3$或$\sigma_k(p)>0.7$。由此可得$d_1(\sigma_k(p),0.5)>0.7$。由定义2知：

$$\|M(p,0.5)\|(\sigma^k)=d_1(\sigma_k(p),0.5)>0.7$$

换句话说，对于任意$k\in\mathbf{N}$都有$\|M(p,0.5)\|(\sigma^k)>0.7$。因此：

$$\|GM(p,0.5)\|(\sigma)=\inf_{i\in\mathbf{N}}\|M(p,0.5)\|(\sigma^i)>0.7$$

根据$L_\alpha(\varphi)$的定义可得$\sigma\in L_\alpha(\varphi)$。

结束语　本文研究了经典安全性的一种量化推广形式。通过引入距离阈值α，基于伪超度量空间定义了一种α-安全性；随后在MLTL公式与α-安全性之间建立了关系。研究表明，一个只使用$\wedge$，$\vee$，X，G和W运算符的MLTL公式，在α约束下所表示的MLT属性是一个α-安全性。本文的研究成果为度量背景下系统的安全性验证提供了理论支撑。

在未来的工作中，我们将考虑计算机系统验证中另一类备受关注的属性——活性，并研究其在度量背景下的推广形式，以及它与MLTL公式之间的关系。

参 考 文 献

[1] BAIER C, KATOEN J P. Principles of model checking[M]. The MIT Press, 2008.

[2] MANNA Z, PNUELI A. The temporal logic of reactive and concurrent systems: Specification [M]. Springer-verlag, 1992.

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

[4] WANG X B, DUAN Z H. Model checking for temporal logic programs[J]. Computer Science, 2009, 36(10): 164-167.

[5] WANG Z Z. Survey of model checking[J]. Computer Science, 2013, 40(6A): 1-14.

[6] HOU G, ZHOU K J, YONG J W, et al. Survey of state explosion problem in model checking [J]. Computer Science, 2013, 40(6A): 77-86.

[7] ZHU C Y, CHANG L, XU Z B, et al. Model checking of temporal description logic ALC-LTL based on label Büchi automata [J]. Computer Science, 2013, 40(10): 166-171.

[8] BU L, XIE D B. Formal verification of Hybrid system[J]. Jour-

nal of Software, 2014, 25(2): 219-233.
[9] WANG J, ZHAN N J, FENG X Y, et al. Over-view of formal methods[J]. Journal of Software, 2019, 30(1): 33-61.
[10] ALPERN B, SCHNEIDER F B. Defining liveness[J]. Information Processing Letters, 1985, 21(4): 181-185.
[11] ALPERN B, SCHNEIDER F B. Recognizing safety and liveness [J]. Distributed Computing, 1987, 2(3): 117-126.
[12] KUPFERMAN O, VARDI M Y. Model checking of safety properties[J]. Formal Methods in System Design, 2001, 19(3): 291-314.
[13] FARAN R, KUPFERMAN O. Spanning the spectrum from safety to liveness[J]. Acta Informatica, 2018, 55(8): 703-732.
[14] KUPFERMAN O, VARDI G. On relative and probabilistic finite counterability [J]. Formal Methods in System Design, 2018, 52(2): 117-146.
[15] SISTLA A P. Safety, liveness and fairness in temporal logic[J]. Formal Aspects of Computing, 1994, 6(5): 495-511.
[16] LI Y M, DROSTE M, LEI L H. Model checking of linear-time properties in multi-valued systems [J]. Information Sciences, 2017, 377: 51-74.
[17] LI Y M. Quantitative model checking of linear-time properties based on generalized possibility measures [J]. Fuzzy Sets and Systems, 2017, 320: 17-39.
[18] KATOEN J P, LEI S, ZHANG L. Probably safe or live[C]// Eacsl Conference on Computer Science Logic. 2014: 1-10.
[19] FAHRENBERG U, LARSEN K G, THRANE C R. A quantitative characterization of weighted Kripke structures in temporal logic [C]// Doctoral Workshop on Mathematical & Engineering Methods in Computer Science. DBLP, 2009.
[20] PAN H Y. Lattice-valued quantitative verification of state transition systems [D]. Shanghai: East China Normal University, 2012.
[21] 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.
[22] 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.
[23] 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.
[24] LIANG C J, LI Y M. The model checking problem of computing tree logic based on generalized possibility measures[J]. Acta Electronica Sinica, 2017, 45(11): 2641-2648.
[25] FAN Y H, LI Y M. The realizability of fuzzy linear temporal logic[J]. Acta Electronica Sinica, 2018, 46(2): 341-346.
[26] FAN Y H, LI Y M, PAN H Y. Computation tree logic model checking for nondeterminisitc fuzzy Kripke structure[J]. Acta Electronica Sinica, 2018, 46(1): 152-159.
[27] LEI L H, WANG J. Parallelization of LTL model checking based on possibility measure [J]. Computer Science, 2018, 45(4): 71-75.
[28] ZHU Y, YUAN H J, QIAN J Y, et al. Some notes on fuzzy alternating-time temporal logic [J]. Journal of Frontiers of Computer Science and Technology, 2018, 12(12): 2033-2040.
[29] ALFARO L D, FAELLA M, STOELINGA M. Linear and branching system metrics[J]. IEEE Transactions on Software Engineering, 2009, 35(2): 258-273.
[30] CAO Y Z, SUN S X, WANG H Q, et al. A behavioral distance for fuzzy-transition sys-tems[J]. IEEE Transactions on Fuzzy Systems, 2013, 21(4): 735-747.
[31] BU T M, WU H Y, CHEN Y X. Computing behavioural distance for fuzzy transition systems[C]// International Symposium on Theoretical Aspects of Software Engineering. IEEE Computer Society, 2017.
[32] CHEN T L, HAN T T, CAO Y Z. Polynomial-time algorithms for computing distances of fuzzy transition systems [J]. Theoretical Computer Science, 2018, 727: 24-36.

CAI Yong, born in 1995, master. His main research interests include formal verification.

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.