doi:10.3969/j.issn.1672-4348.2018.06.008

标号迁移系统的互模拟关系及其性质

唐郑熠[1,2],林佳音[1],黄泽斌[1]

(1.福建工程学院 信息科学与工程学院,福建 福州 350118;
2.福建省大数据挖掘与应用技术重点实验室,福建 福州 350118)

摘要:以标号迁移系统为工具,探讨了系统行为的等价性问题,构建了模拟及互模拟关系的形式化模型,进而将互模拟的概念推广到了系统的层面,进一步探讨了模拟及互模拟关系的性质,揭示了互模拟概念的本质,为其在形式化分析及验证技术中的应用提供了基础。

关键词:系统行为;等价;标号迁移系统;模拟;互模拟

中图分类号:TP393.08　　**文献标志码**:A　　**文章编号**:1672-4348(2018)06-0547-06

Bisimulation relation in labeled transition system and its properties

TANG Zhengyi[1,2], LIN Jiayin[1], HUANG Zebin[1]

(1. School of Information Science and Engineering, Fujian University of Technology, Fuzhou 350118, China;
2.Fujian Provincial Key Laboratory of Big Data Mining and Applications, Fuzhou 350118, China)

Abstract: The equivalence of system's behavior was discussed by using the labeled transition system. The formal model of the relationship between simulation and bisimulation was constructed, and the concept of bisimulation was extended to the level of the whole system. Furthermore, the properties of simulation and bisimulation were discussed, and the essence of bisimulation was revealed, which provides a basis for its application in formal analysis and verification.

Keywords: system behavior; equivalence; labeled transition system; simulation; bisimulation

系统的行为等价性分析是一个困难且微妙的领域,即使两个系统具有相同的行为,但行为发生顺序的不同,也可能导致两个系统之间很大的差异,从而对外部产生不同的影响。在计算机科学领域,自动机理论是应对这一问题的有力工具[1-2],它使用状态、动作和状态迁移来构建系统的形式化模型,通过分析自动机可接受的语言,来判断不同自动机的等价性[3]。进一步的研究发现,自动机语言的等价性并不意味着两个自动机完全等价[4],并由此引入了互模拟的概念[5]。

互模拟本质上是一种态射形式[6],是两个数学结构之间保持结构的过程抽象,比同态更强,但弱于同构。在系统行为的等价性分析中,互模拟可以理解为两个系统能够相互模仿对方,使得在观察者的角度,它们的行为是相同的。互模拟的概念与技术被应用到许多计算机科学的研究课题中,例如,函数语言、证明工具、程序分析等,是形式化理论的重要基础之一。

本文使用标号迁移系统构建了系统行为的形式化模型,并通过标号迁移系统的语言来规约系统行为序列,解释了语言等价不同于行为等价的原因。在此基础上,通过标号迁移系统构建了模

收稿日期:2018-09-02
基金项目:福建省自然科学基金资助项目(2016J05146);福建工程学院科研启动基金资助项目(GY-Z13112, GY-Z13113)
第一作者简介:唐郑熠(1984-),男,福建福州人,副教授,博士,研究方向:形式化方法、数据挖掘。

拟及互模拟概念的形式化模型，进而给出了系统间的互模拟关系。最后，讨论并证明了模拟及互模拟关系的一些性质。

1 标号迁移系统

标号迁移系统实际上是自动机的弱化形式，它不包括初始状态和可接受状态[7]。

定义 1（标号迁移系统） 标号迁移系统定义为一个二元组 LTS $=(Q, A, T)$，其中：Q 是状态集合；A 是标号集合，可视为系统的行为；$T=\{(q, a, q') \mid q, q' \in Q, a \in A\}$ 表示迁移关系。

标号迁移系统的迁移路径是状态与标号的交替序列，迁移路径可以无限延长。

定义 2（迁移路径） 标号迁移系统 LTS 的一条迁移路径表示为 $p=q_0 a_0 q_1 a_1 \cdots$，其中 $q_i \in Q, a_i \in A$，将一个 LTS 的所有迁移路径集合记为 P(LTS)。

一条迁移路径中的所有迁移标号构成的有序串称为单词。

定义 3（标号串） 一条迁移路径 $p=q_0 a_0 q_1 a_1 \cdots$ 产生一个标号串 $w(p)=a_0 a_1 \cdots$。

为了表达的方便，将标号串的无限重复部分记为 $[a_i a_{i+1} a_{i+2} \cdots a_j]^*$。

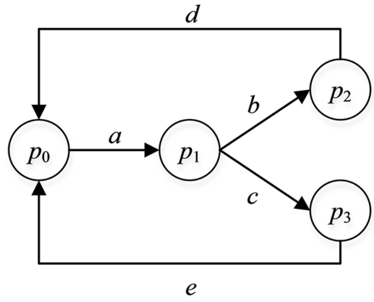
由此，可以定义标号迁移系统的语言。

定义 4（语言） 对于一个标号迁移系统 LTS，其语言 $L(\text{LTS})=\{w(p) \mid p \in P(\text{LTS})\}$ 可以通过指定起始状态和终止状态来表示语言的一个子集，即受限子语言。

定义 5（受限子语言） 对于标号迁移系统 LTS，其受限语言子集满足：$L(\text{LTS}, q, q')=\{w(p) \mid p=q_0 a_0 q_1 a_1 \cdots a_{n-1} q_n \in P(\text{LTS}) \wedge q_0=q \wedge q_0=q'\}$，在不至产生混淆的情况下，可以简记为 $L(q, q')$。

标号迁移系统是最常用的构建系统行为的形式化模型，它包含了系统的状态信息、行为信息以及状态之间的变化信息。标号迁移系统可以扩展为各种不同的形式化建模工具，例如确定/非确定型自动机、Büchi 自动机、时间自动机等。

使用标号迁移系统描述的饮品自动售卖机的模型如图 1 所示。



a 表示投入 10 元现金，b 表示选择购买茶饮，c 表示选择购买咖啡，d 表示弹出茶饮；e 表示弹出咖啡

图 1 饮品自动售卖机的标号迁移系统模型

Fig.1 Labeled transition system of a brverage vending machine

它的一个受限子语言表示为：

$$L_1(p_0, p_0)=\{[abd]^*, [ace]^*\}$$

标号迁移系统的语言记录了系统的行为序列，相同的行为序列意味着相同的行为。因此当两个标号迁移系统具有相同的语言时，可以认为它们是等价的。

进一步的研究发现，相同的语言并不一定意味着等价[4]。另一种饮品自动售卖机的标号迁移系统模型如图 2 所示。

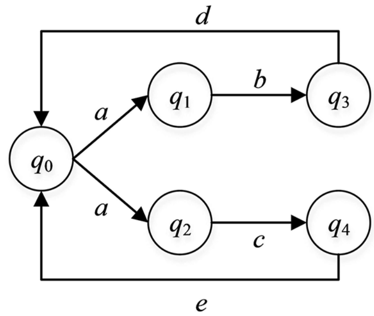


图 2 另一个饮品自动售卖机的标号迁移系统模型

Fig.2 Labeled transition system of another beverage vending machine

图 2 中的标号与图 1 中的标号具有相同的含义。

该标号迁移系统的一个受限子语言是 $L_2(q_0, q_0)=\{[abd]^*, [ace]^*\}$，显然，$L_1(p_0, p_0)=L_2(q_0, q_0)$。相同的语言意味着相同的行为及执行顺序，因此两个系统对外提供的应是等效的功能。

进一步分析发现，两者的功能并不是实质等效的。$L_1(p_0, p_0)$ 表示投入 10 元现金后，可以选择咖啡或茶饮，然后售卖机弹出对应的饮品；而 $L_2(q_0, q_0)$ 表示投入 10 元现金后，售卖机会随机

进入售卖咖啡或售卖茶饮的状态,用户并没有选择的机会。显然这两个标号迁移系统虽然具有相同的受限子语言,但在受限子语言所限定的路径迁移范围内,它们不是实质等价的。

上述例子表明:两个系统具有相同语言(即行为序列),并不意味着两者是等价的,因此需要另一种更强的等价性概念。由此,产生了互模拟的概念。

2　标号迁移系统的互模拟关系

2.1　模拟关系

比较图 1 和图 2 中的标号迁移系统,可以发现尽管状态 p_0和 q_0可以接受相同的行为标号,但所迁移到的状态却明显不同:

p_0接受标号 a 后所迁移到 p_1,p_1既可以接受标号 b,也可以接受标号 c。q_0接受标号 a 后,要么迁移到 q_1,q_1只能接受标号 b;要么迁移到 q_2,q_2只能接受标号 c。

显然,从 p_0的角度看,它所接受的标号及所发生的迁移,保留了 q_0可能接受的标号及产生的迁移。但反过来,q_0却做不到这一点。由此,产生了模拟关系的概念。

定义 6(模拟关系)[8]　对于标号迁移系统 LTS = (Q, A, T),设 S 是 Q 上的一个二元关系,即 $S = \{(p, q) \mid p, q \in Q\}$;对于任意$(p, q) \in S$,总满足:

(1)对于任意$(p, a, p') \in T$,总是存在 $q' \in Q$,使得$(q, a, q') \in T$,且$(p', q') \in S$;则称 S 为 LTS 上的一个模拟关系,$(p, q) \in S$ 称为一个模拟对。

(2)如果 S 是一个模拟关系,则对于$(p, q) \in S$,称 q 可以模拟 p,或 p 可以被 q 模拟。

从定义 6 可知,如果状态 p 可以被状态 q 模拟,则意味着:

(1)p 能够接受的所有标号也能够被 q 接受。

(2)如果 p 接受一个标号后迁移到状态 p',q 接受相同标号后迁移到状态 q',p'同样能被 q'模拟。

以上两个条件保证了以 p 开始的迁移路径上的所有输入标号,都被以 q 开始的迁移路径所保留。

同时,由模拟关系的定义可知,如果 p 没有任何可接受的标号,即从 p 不产生任何迁移,则 p 可以被任意状态模拟。

显然,对于图 1 和图 2 中的标号迁移系统,存在以下模拟关系:

$S = \{(q_0, p_0), (q_1, p_1), (q_2, p_1), (q_3, p_2), (q_4, p_3)\}$

要证明一个二元关系 S 是模拟关系,就必须对任意$(p, q) \in S$,证明其在 S 中是模拟对。将图 1 中的标号迁移 LTS_1和 LTS_2合并为:$LTS = LTS_1 \cup LTS_2 = \{Q = Q_1 \cup Q_2, A = A_1 \cup A_2, T = T_1 \cup T_2\}$

下面证明 q_0可以被 p_0模拟,而反之不成立。

命题 1　在 LTS 中,q_0可以被 p_0模拟。

证明　(1)对于$(q_0, a, q_1) \in T$,存在$(p_0, a, p_1) \in T$,且$(q_1, p_1) \in S$。

(2)对于$(q_0, a, q_2) \in T$,存在$(p_0, a, p_1) \in T$,且$(q_2, p_1) \in S$。

证毕。

命题 2　在 LTS 中,p_0不能被 q_0模拟。

证明　(1)对于$(p_0, a, p_1) \in T$,存在$(q_0, a, q_1) \in T$ 或是$(q_0, a, q_2) \in T$。

(2)但$(p_1, q_1) \notin S \wedge (p_1, q_2) \notin S$,即无论是 q_1或 q_2,都不能模拟 p_1。

证毕。

2.2　互模拟关系

互模拟关系是比模拟关系更强的等价性表达,它要求两个状态可以相互模拟[8]。

定义 7(互模拟关系)　对于标号迁移系统 LTS = (Q, A, T),如果 S 是 LTS 上的一个模拟关系,且 S^{-1}也是 LTS 上的模拟关系,则称 S 为 LTS 上的一个互模拟关系,$(p, q) \in S$ 称为一个互模拟对。

具有互模拟关系的 LTS 如图 3 所示。

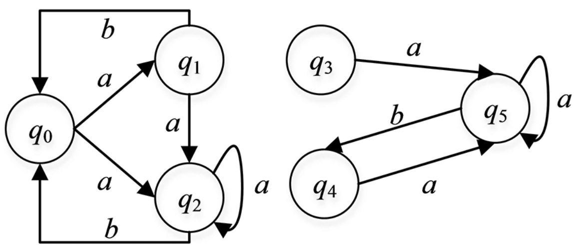


图 3　具有互模拟关系的 LTS

Fig.3　A LTS with bisimulation relations

在这个 LTS 上,具有互模拟关系:

$R = \{(q_0, q_3), (q_0, q_4), (q_1, q_5), (q_2, q_5)\}$

要证明一个二元关系 R 是互模拟关系,就必须对任意$(p, q) \in R$,证明其在 S 中是互模拟对。

证明一个有序对(p, q)是互模拟对,分为两步:

(1)证明(p, q)在关系 R 中是模拟对。

(2)证明(q, p)在关系 R^{-1}中是模拟对。

需要注意的是,互模拟对要求两个状态在一个关系及其对应的逆关系中能够相互模拟,而不是任意两个没有关联的关系。

由此,引出了状态等效的概念[4]。

定义 8(状态等效) 对于标号迁移系统 $LTS = (Q, A, T)$中的状态 p、q,如果存在一个互模拟关系 R,且满足$(p, q) \in R$,则称 p、q 是状态等效,记为 $p \leftrightarrow q$。

状态等效意味着两个状态可以在同一映射模式中视为等效。

2.3 系统间的互模拟关系

互模拟关系是基于状态定义的,关注的是两个状态之间的等效性。这个概念可以扩展到整个标号迁移系统。

定义 9(系统模拟关系) 对于两个标号迁移系统 $LTS_1 = (Q_1, A_1, T_1)$和 $LTS_2 = (Q_2, A_2, T_2)$,如果存在一个二元关系 $S = \{(p, q) \mid p \in Q_1 \wedge q \in Q_2\}$,并满足:

(1)$\forall p \in Q_1: \exists (p, q) \in S$。

(2)$\forall (p, q) \in S$,满足:$\forall (p, a, p') \in T_1: \exists (q, a, q') \in T_2 \wedge (p', q') \in S$。

则称 S 为 LTS_1和 LTS_2之间的一个模拟关系,记为 $LTS_1 \xleftarrow{S} LTS_2$。

如果存在 $LTS_1 \xleftarrow{S} LTS_2$,则称 LTS_2可以模拟 LTS_1。这意味着 LTS_1中的所有行为路径,都被保留在 LTS_2中,因此 LTS_1的行为可以被 LTS_2完整地模拟。

相应的,可以进一步定义系统互模拟关系。

定义 10(系统互模拟关系) 对于两个标号迁移系统 $LTS_1 = (Q_1, A_1, T_1)$和 $LTS_2 = (Q_2, A_2, T_2)$,如果存在二元关系 $R = \{(p, q) \mid p \in Q_1 \wedge q \in Q_2\}$,使得 $LTS_1 \xleftarrow{R} LTS_2$,且 $LTS_2 \xleftarrow{R^{-1}} LTS_1$,则称 R 为 LTS_1和 LTS_2之间的一个互模拟关系,记为 $LTS_1 \xleftrightarrow{R} LTS_2$。

两个标号迁移系统存在互模拟关系,意味着它们可以相互模拟彼此的行为,从而对外表现出行为上的等价性。

以标号迁移系统构建系统的行为模型,通过证明模型之间是否存在互模拟关系,可以验证系统行为的等价性。有关系统性质的讨论,为互模拟关系的证明提供了基础定理,并有助于自动证明及验证算法的设计,从而为互模拟概念在形式化分析及验证技术中的应用提供基础。

3 互模拟关系的性质

下面讨论模拟及互模拟关系的一些重要性质,并给出证明。

性质 1 模拟关系的逆关系未必是模拟关系。

证明 设 $S = \{(p, q) \mid p, q \in Q\}$为标号迁移系统 $LTS = (Q, A, T)$上的模拟关系,则 $S^{-1} = \{(q, p) \mid p, q \in Q\}$。

由于 S 是 LTS 上的模拟关系,则:

对于$(p, q) \in S$,$\forall a \in A: (p, a, p') \in T$

$\Rightarrow (q, a, q') \in T \wedge (p', q') \in S$

对于$(q, p) \in S^{-1}$,$\forall a \in A: (q, a, q') \in T$,存在两种可能:

(1)满足$(p, a, p') \in T$,由于$(p', q') \in S$,则$(q', p') \in S$,则 S^{-1}也是 LTS 上的模拟关系。

(2)不满足$(p, a, p') \in T$,则 S^{-1}不是 LTS 上的模拟关系。

证毕。

性质 2 互模拟关系的逆关系仍然是互模拟关系。

证明 设 S 为标号迁移系统 $LTS = (Q, A, T)$上的模拟关系。那么,S 为 LTS 上的模拟关系,S^{-1}为 LTS 上的模拟关系。由于$(S^{-1})^{-1} = S$,所以 S^{-1}的逆关系也是模拟关系。所以 S^{-1}仍然是互模拟关系。

证毕。

性质 3[4] 状态等效关系是等价关系。

证明 设$\leftrightarrow = \{(p, q) \mid p, q \in Q\}$是标号迁移系统 $LTS = (Q, A, T)$上的状态等效关系。

(1)$\leftrightarrow$是自反的,即$\forall p \in Q: p \leftrightarrow p$。

设关系 $R = \{(p, p) \mid p \in Q\}$,

$\forall a \in A: (p, a, p') \in T$

$\Rightarrow (p, a, p') \in T, (p', p') \in R$

所以 R 是 LTS 上的模拟关系。

由于 $R^{-1} = R$,所以 R^{-1}也是 LTS 上的模拟关

系。因此 R 是互模拟关系，并且 $(p, p) \in R$。

(2)$\leftrightarrow$是对称的，即$\forall p, q \in Q$: $p \leftrightarrow q \Rightarrow$

$q \leftrightarrow p$

$p \leftrightarrow q \Rightarrow$在 LTS 上存在互模拟关系，使得$(p, q) \in R$。

由于 R 是互模拟关系，所以 R^{-1} 也是互模拟关系，且满足$(q, p) \in R^{-1}$，所以 $q \leftrightarrow p$。

(3)$\leftrightarrow$是传递的，即$\forall p, q, r \in Q$:

$p \leftrightarrow q \wedge q \leftrightarrow r \Rightarrow p \leftrightarrow r$

$p \leftrightarrow q \Rightarrow \exists$互模拟关系 R_1，使得：

$$(p, q) \in R_1$$

$q \leftrightarrow r \Rightarrow \exists$互模拟关系 R_2，使得：

$$(q, r) \in R_2$$

设关系 $S = R_1 \circ R_2 =$

$\{(p, r) \mid \exists p, q, r: (p, q) \in R_1 \wedge (q, r) \in R_2\}$

(1)先证明 S 是模拟关系：

R_1是互模拟关系

$\Rightarrow \forall a \in A: (p, a, p') \in T$

$\Rightarrow (q, a, q') \in T \wedge (p', q') \in R_1$。

R_2是互模拟关系

$\Rightarrow \forall a \in A: (q, a, q') \in T$

$\Rightarrow (r, a, r') \in T \wedge (q', r') \in R_2$。

因此，

$\forall a \in A: (p, a, p') \in T$

$\Rightarrow (q, a, q') \in T$

$\Rightarrow (r, a, r') \in T, (p', q') \in R_1 \wedge (q', r') \in R_2$

$\Rightarrow (p', r') \in S$。

所以 S 是模拟关系。

(2)再证明 S^{-1}也是模拟关系：

$S^{-1} = \{(r, p) \mid (p, q) \in R_1 \wedge (q, r) \in R_2\}$，

R_1是互模拟关系

$\Rightarrow R_1^{-1}$ 是互模拟关系 $\wedge (q, p) \in R_1^{-1}$

$\Rightarrow \forall a \in A: (q, a, q') \in T$

$\Rightarrow (p, a, p') \in T \wedge (q', p') \in R_1^{-1}$。

R_2是互模拟关系

$\Rightarrow R_2^{-1}$ 是互模拟关系 $\wedge (r, q) \in R_1^{-1}$

$\Rightarrow \forall a \in A: (r, a, r') \in T$

$\Rightarrow (q, a, q') \in T \wedge (r', q') \in R_1^{-1}$。

因此：

$\forall a \in A: (r, a, r') \in T$

$\Rightarrow (q, a, q') \in T$

$\Rightarrow (p, a, p') \in T, (p', r') \in R_1 \circ R_2$

$\Rightarrow (r', p') \in S^{-1}$。

从而证明 S 是互模拟关系，即 $p \leftrightarrow r$。

由于$\leftrightarrow$是自反的、对称的、传递的，故$\leftrightarrow$是等价关系。

证毕。

性质 4　互模拟关系的并集仍然是互模拟关系。

证明　设 R_1 和 R_2 为标号迁移系统 LTS 上的互模拟关系，LTS $= (Q, A, T)$。

$S = R_1 \cup R_2 = \{(p, q) \mid p, q \in Q\}$，

$\forall (p, q) \in S$: $(p, q) \in R_1 \vee (p, q) \in R_2$

$\Rightarrow (p, q)$是互模拟对。

所以 S 是互模拟关系。

证毕。

性质 5　$\mathrm{LTS}_1 \xleftarrow{S} \mathrm{LTS}_2 \wedge \mathrm{LTS}_2 \xleftarrow{R} \mathrm{LTS}_3 \Rightarrow \mathrm{LTS}_1 \xleftarrow{S \circ R} \mathrm{LTS}_3$。

证明　设 $S = \{(p, q) \mid p \in Q_1 \wedge q \in Q_2\}$，$R = \{(q, r) \mid q \in Q_2 \wedge r \in Q_3\}$，

$S \circ R = \{(p, r) \mid \exists p, q, r: (p, q) \in S \wedge (q, r) \in R\}$。

设 $\mathrm{LTS}_1 = (Q_1, A_1, T_1)$，$\mathrm{LTS}_2 = (Q_2, A_2, T_2)$，$\mathrm{LTS}_3 = (Q_3, A_3, T_3)$：

$\mathrm{LTS}_1 \xleftarrow{S} \mathrm{LTS}_2$

$\Rightarrow \forall p \in Q_1: \exists (p, q) \in S \wedge \forall (p, q) \in S: \forall (p, a, p') \in T_1: \exists (q, a, q') \in T_2 \wedge (p', q') \in S$。

$\mathrm{LTS}_2 \xleftarrow{R} \mathrm{LTS}_2$

$\Rightarrow \forall q \in Q_2: \exists (q, r) \in R \wedge \forall (q, r) \in R: \forall (q, a, q') \in T_2: \exists (r, a, r') \in T_3 \wedge (q', r') \in R$。

由此：

(1)$\forall p \in Q_1: \exists (p, q) \in S \wedge \forall q \in Q_2: \exists (q, r) \in R \Rightarrow \forall p \in Q_1: \exists (p, r) \in S \circ R$。

(2)$\forall (p, a, p') \in T_1$

$\Rightarrow \exists (q, a, q') \in T_2$

$\Rightarrow \exists (r, a, r') \in T_3$。

且$(p', q') \in S \wedge (q', r') \in R$

$\Rightarrow (p', r') \in S \circ R$，

从而有 $\forall (p, r) \in S \circ R: \forall (p, a, p') \in T_1: \exists (r, a, r') \in T_3 \wedge (p', r') \in S \circ R$。

证毕。

4　结语

本文通过标号迁移系统来构建系统行为模

型,探讨了系统行为等价性的问题,并籍此构建了模拟及互模拟关系的形式化模型,同时将模拟及互模拟关系扩展到了不同系统之间,最后探讨了模拟及互模拟关系的一些性质。本文的工作为互模拟的概念搭建了形式化框架,扩展了它的适用面,同时通过对其性质的讨论和证明,更进一步地揭示了互模拟概念的本质。

参考文献:

[1] PIN J E. Elements of automata theory by Jacques Sakarovitch[J]. Bulletin of Symbolic Logic, 2011, 17(1): 122-124.

[2] LAMPERTI G, ZANELLA M, ZHAO X. Introduction to diagnosis of active systems[M]. Berlin: Springer-Verlag, 2018: 19-43.

[3] TANG Z Y, WANG J S, CHEN Y, et al. The redundancy problem in composition of parallel finite automata and its optimization method[C]//The Euro-China Conference on Intelligent Data Analysis And Applications. Malaga, Spain: Springer, 2017: 359-367.

[4] MILNER R. Communication and mobile systems: the π-calculus[M]. Cambridge: Cambridge University Press, 1999: 17-26.

[5] SANGIORGI D. On the origins of bisimulation and coinduction[J]. ACM Transactions on Programming Languages & Systems, 2009, 31(4): 1-41.

[6] 李娜, 姚丛军. 互模拟的一些基本性质[J]. 云南师范大学学报(哲学社会科学版), 2010, 42(5): 68-73.

[7] 蔡烜, 郑一源. 一种计算有限标号转移系统模拟关系的算法[J]. 上海交通大学学报, 2009(11): 1784-1787.

[8] SANGIORGI D. A theory of bisimulation for the π-calculus[J]. Acta Informatica, 1996, 33(1): 69-97.

(特约编辑:黄家瑜)