第 39 卷 第 5 期
Vol.39 No.5

计 算 机 工 程
Computer Engineering

2013 年 5 月
May 2013

• 开发研究与工程应用 •　文章编号：1000—3428(2013)05—0318—04　文献标识码：A　中图分类号：TP311

基于综合性能的 Markov 过程验证与分析

纪明宇[1,2]，王海涛[3]，陈志远[1]

(1. 哈尔滨工程大学计算机科学与技术学院，哈尔滨 150001；2. 东北林业大学信息与计算机工程学院，哈尔滨 150040；
3. 东北农业大学继续教育中心，哈尔滨 150030)

摘　要：面向复杂信息系统综合性能的形式化验证问题，以数据传输系统为例，使用一种基于改进的马尔可夫判定过程验证分析方法进行复杂信息系统的性能验证。在综合各种连续随机逻辑变体基础上，采用一种表达能力更强的时序逻辑来表示系统模型的复杂性质，运用自动机技术建模路径公式，通过构造积模型完成模型与自动机的同步演化，并给出相应的算法描述。实例结果验证了该方法可有效地扩大模型检测技术的应用范围。

关键词：综合性能；形式化验证；马尔可夫过程；时序逻辑；自动机；积模型

Verification and Analysis of Markov Process Based on Integrated Performance

JI Ming-yu[1,2], WANG Hai-tao[3], CHEN Zhi-yuan[1]

(1. College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China;
2. College of Information and Computer Engineering, Northeast Forestry University, Harbin 150040, China;
3. Continuing Education Center, Northeast Agricultural University, Harbin 150030, China)

【Abstract】Facing the problem of synthesizes performance formal verification for complex information system, this paper uses the data transmission system as example and applies a new property verification method based on improved Markov decision process to verify the performance of the system. A new more expressive temporal logic is used to describe system model properties on the basis of all kinds of continuous stochastic logic variants. By using automata to express logic path formula, the corresponding algorithm is described based on product model which realizes the simultaneous evolution of the model and the automata. Example result verifies the method can effectively expand the application scope of the model checking technology.

【Key words】integrated performance; formal verification; Markov process; temporal logic; automata; product model
DOI: 10.3969/j.issn.1000-3428.2013.05.071

1　概述

复杂信息系统的功能正确性与性能可满足性作为复杂系统可信性要求的两个非常重要的方面，日益成为学术界关注的热点问题。在复杂系统运行演化的过程中，时刻伴随着系统状态的变化和资源的消耗，人们总是希望系统能够在尽可能短的时间，消耗尽可能少的资源的情况下，实现既定的功能。这就要求系统的设计、测试过程要综合运用定性分析和定量验证的手段，对系统的可信性[1]加以保证，单纯的功能验证或性能分析均无法有效地得到复杂系统准确的分析结果。

形式化方法被认为是系统定量验证方面可行、有效的方法之一。近年来，模型检测技术被很多学者用于对系统性能进行可信评估[2]。使用此方法在对系统模型进行定量验证分析的过程中，通常首先将系统建模为熟悉的常用模型，之后将这些模型构造转换为基于状态层面上的模型，然后采用一种相对容易的方式，完成系统的定量验证。

连续时间 Markov 链[3](Continuous Time Markov Chain, CTMC)因其具有描述连续时间特征的能力，已被广泛应用于现实的系统模型。连续时间 Markov 判定过程[4](Continuous Time Markov Decision Process, CTMDP)在 CTMC 的基础上，引入动作迁移，可以描述系统状态变化过程中的不确定性特征，基于某种调度策略，CTMDP 可以转化为 CTMC。交互式 Markov 链[5]正交地结合了传统的进程代数模型和连

基金项目：国家自然科学基金资助项目(71001023)；中央高校基本科研业务费专项基金资助项目(DL11BB08)
作者简介：纪明宇(1980－)，男，讲师、博士研究生，主研方向：形式化验证，模型检测；王海涛，讲师；陈志远，讲师、博士研究生
收稿日期：2012-05-07　**修回日期：**2012-07-16　**E-mail：**50117019@qq.com

续时间马尔科夫链模型，可同时刻画动作、时间和不确定性，非常适合于对大型并发系统进行分析。

本文基于 CTMDP，使用支持状态与迁移回报的连续时间 Markov 判定过程(Continuous Time Markov Decision Process with state and transition rewards, strCTMDP)作为复杂信息系统功能验证和性能分析模型，将功能、性能的可信验证最终转化为 trCTMRP 中满足特定性质的路径子集可达概率的求解，并对算法的实现过程加以描述。

2 strCTMDP 基本概念

定义 1 CTMDP

CTMDP 为六元组 $M=(S, ACT, AP, L, \boldsymbol{R}, v)$，其中，$S$ 表示状态集合；ACT 是动作标记集合；$L: S \to 2^{AP}$ 为状态标记函数；AP 表示原子命题的有限集；$\boldsymbol{R}: S \times ACT \times S \to \boldsymbol{R}_{\geqslant 0}$ 为迁移率矩阵；$v \in Distr(S)$ 为初始分布集合。

定义 2 strCTMDP

strCTMDP 是六元组 $M=(S, ACT, AP, L, \boldsymbol{R}, \boldsymbol{N})$，其中，$S=\{(s',\rho)\,|\,s' \in S'\}$ 表示状态回报对偶集合；S' 为状态集合；$\rho: S' \to \boldsymbol{R}_{\geqslant 0}$ 是状态回报结构，用于描述驻留于该状态时的单位时间资源消耗；ACT 是动作标记集合；AP 表示原子命题的有限集；$L: S \to 2^{AP}$ 是状态标记函数；$\boldsymbol{R}: S \times ACT \times S \to \boldsymbol{R}_{\geqslant 0}$ 代表迁移率矩阵；$\boldsymbol{N}: S \times ACT \times S \to \boldsymbol{R}_{\geqslant 0}$ 为迁移回报矩阵。

在模型中，如果 $R(s_1,a,n,s_2)=\lambda>0$，则在 s_1 与 s_2 存在一个动作 a 的迁移，迁移率满足 λ 的指数分布，迁出 s_1 状态的迁移资源消耗为 n。

3 连续随机回报逻辑的语法和语义

在模型检测过程中，模型所需验证的性质一般通过某种时序逻辑公式来表示，其中比较常用的就是采用连续随机逻辑(Continuous Stochastic Logic, CSL)[6]，它可以描述 CTMC 模型中连接时间和概率特征性质，但对模型迁移过程中资源消耗和动作特征缺少足够的描述能力。近年来，基于 CSL 的不同特征上的扩展被学者们相继提出，其中连续随机回报逻辑[7](Continuous Stochastic Reward Logic, CSRL)在 CSL 的基础上加入了状态资源消耗的描述，得到了一定的应用，但未对迁移过程中动作回报特征加以考虑。文献[8]中的连续随机逻辑因其不具备描述基于动作的随机迁移的能力，故不适用于本文的系统模型性质描述。支持动作及状态标记的连续随机逻辑[9](CSL with actions and state labels, asCSL)尽管能够使系统迁移同时具有动作及随机性的描述，但该逻辑不具备对系统状态迁移过程中资源的消耗进行描述的能力。

本文为了验证 strCTMDP 模型的综合性能，采用了支持动作序列的连续随机回报逻辑(Continuous Stochastic Reward Logic with action sequences, aCSRL)，其中路径公式功能属性可通过自动机加以表示，aCSRL 语法通过定义 3 和定义 4 给出。

定义 3 aCSRL 状态公式

aCSRL 状态公式的语法形式：

$$\phi ::= \text{true}\,|\,q\,|\,\neg\phi\,|\,\phi \vee \phi\,|\,S_{\Delta p}(\phi)\,|\,P_{\Delta p}(\alpha_J^I)$$

其中，$q \in AP$ 为原子命题；$p \in [0,1]$ 表示概率值；Δ 表示比较操作符；$I=[t,t'] \subseteq \boldsymbol{R}_{\geqslant 0}$ 及 $J=[t,t'] \subseteq \boldsymbol{R}_{\geqslant 0}$ 分别代表时间区间和回报值区间；a_J^I 表示路径公式；ϕ 表示状态公式集；$S_{\Delta p}(\phi)$ 为稳态概率算子，表示最终满足停留于 ϕ 状态的路径集合的概率满足 Δp；$P_{\Delta p}(a_J^I)$ 为瞬时概率算子，表示状态序列满足路径公式 a_J^I 的所有路径集合的概率满足 Δp。

定义 4 aCSRL 的路径公式

aCSRL 的路径公式 α 的语法形式为：

$$\alpha ::= \varepsilon\,|\,(\phi,b)\,|\,\alpha;\alpha\,|\,\alpha \cup \alpha\,|\,\alpha^*$$

其中，α 用来表示路径性质，它的基本形式是接受有限字的正则集合，输入字的形式为 (ϕ,b)；ϕ 为状态公式；$b \in Act$ 或者 $b=\surd$，$\surd$ 表示将被立即执行且不改变模型当前状态的伪动作。

4 模型检测过程说明

对于给定的 aCSRL 路径公式 α 和 strCTMDP 模型 M，首先将路径公式性质表示为自动机[10]，将其作为原始 strCTMDP 模型中路径集合的接收器，然后构造原始 strCTMDP 模型和路径公式自动机的同步进化积模型，进而计算积模型下指定的时间间隔、回报间隔下到达指定状态的概率。对于 aCSRL 状态公式，本文主要讨论 $P_{\Delta p}(a_J^I)$ 形式的处理方法。

对于 M 中的每一个状态 s，s 出发的路径满足 α_J^I 的概率用 $Prob^M(s,\alpha_J^I)$ 表示，其中：

$$Prob^M(s,\alpha_J^I)=Pr^M\{\varsigma \in Path_\omega^M(s)\,|\,M,\varsigma|=\alpha_J^I\}$$

定义 5 路径公式自动机 A

路径公式自动机表示为 $A=(Z,\Sigma',\delta,Z_0,F)$，其中 Z 是一个有限状态集；Σ' 是一个有限字母集合；$\delta: Z \times \Sigma' \to 2^Z$ 为迁移函数；$Z_0 \subseteq Z$ 是初始状态集合；$F \subseteq Z$ 表示接受状态集合；$L(A) \subseteq (\Sigma')^*$ 代表 A 所接受的语言。

这里自动机 A 作为模型 M 中有限路径的接受集，设模型 M 中有路径 $\sigma=s \xrightarrow{a,t,n} \sigma'$。假设当前自动机状态为 z，那么 A 中发生迁移 $z \xrightarrow{\phi,b} z'$ 移动至下一状态，当且仅当路径 σ 中状态 $s|=\phi$，且 $b=a$。如果对于路径 σ，A 没有相应的迁移发生，则表示 A 拒绝该路径。当 A 达到某一个终止状态，且路径 σ 同时到达路径的最后一个状态，则表示自动机接受路径 σ。

5 同步进化积模型

本节给出路径公式自动机 A 和 strCTMDP 模型 M 的同步进化积的形式化定义 $M \times A$。

定义 6 同步进化积 $M \times A$

设 $M=(S, ACT, AP, L, \boldsymbol{R}, \boldsymbol{N})$是一个 strCTMDP，$A=(Z, \Sigma', \delta, Z_0, F)$ 为非确定有限自动机，则它们的同步进化积形式化定义如下：

$$M \times A=(S^*, ACT^*, AP^*, L^*, \boldsymbol{R}^*, \boldsymbol{N}^*)$$

其中，$S^*=\{(s,Z') \mid s=(s',\rho) \in S \wedge Z' \in 2^Z\}$；$ACT^*=ACT$；$AP^*=AP \bigcup \{accept\}$。

标记函数表示为：

$$L^*(<s,Z'>)=\begin{cases} L(s) \cup \{accept\} & \text{if } Z' \cap F=\varnothing \\ L(s) & \text{其他情况} \end{cases}$$

迁移率矩阵为：

$$\boldsymbol{R}^*(<s_1,Z_1>,a,n,<s_2,Z_2>)=$$

$$\begin{cases} \boldsymbol{R}(s_1,a,n,s_2) & \text{if } Z_2=\delta'^M(Z_1,\ s_1 \xrightarrow{a,t,n} s_2) \\ 0 & \text{其他情况} \end{cases}$$

其中，$\delta'^M(Z_1, s_1 \xrightarrow{a,t,n} s_2)$ 表示 Z_1 中的每一个状态输入 $s_1 \xrightarrow{a,t,n} s_2$ 后所到达的状态集的并集。

6 计算方法

构造后，$Prob^M(s,\alpha_J^I)$ 可以通过在同步进化积 $M \times A$ 中计算路径公式 $\Diamond_J^I accept$ 的概率来实现。而同步进化积模型下某一状态 s 在约束条件限制下到达接受状态的概率 $P^{M\times A}(s,\Diamond_J^I accept)$ 又与积模型时间空间约束下的直到算子公式具有等价关系，此种直到形式的概率值可采用下文提出的计算方法计算得出。

积模型下时间空间约束下的直到算子公式记为 $PUIJs\varphi\psi$，该值的计算分为以下几种情况：

$$\begin{cases} 1 \quad \text{如果} s \text{满足} \psi \text{并且} inf(I)=inf(J)=0 \\ \int_0^{supX(s,s_i)} \sum_{s_i \in S} W(s,s_i,act,x) \cdot PU(I-x)(J-(\rho(s) \times \\ x+N(s,s_i,act)))s_i\varphi\psi \mathrm{d}x \quad \text{如果} s \text{满足} \phi \wedge \neg\psi \\ \mathrm{e}^{-E(s)\cdot infL(s)}+\int_0^{infL(s)} \sum_{s_i \in S} W(s,s_i,act,x) \cdot PU(I-x) \\ (J-\rho(s) \times x)s_i\varphi\psi \mathrm{d}x \quad \text{如果} s \text{满足} \phi \wedge \psi \\ 0 \quad \text{其他} \end{cases}$$

符号说明：

符号 $L(s)$ 表示在当前状态 s 停留，消耗的累积回报满足 J 的停留时间集合；$X(s,s_i)$ 表示在当前状态 s 停留后发生动作 act 迁移至 s^* 状态，消耗的累积回报满足 J 的停留时间集合；$W(s,s_i,x,act)$ 表示在从状态 s 基于动作 act 在时间 x 内移动至 s_i 的概率密度。

算法 strCTMDP 模型下 aCSRL 状态公式满意集算法 sat_aCSRL_state_formula(M,Φ)

```
{
//输入 M 表示 strCTMDP 模型，Φ 为 aCSRL 状态公式
 //输出满意集 sat
 sat=空集
 if(Φ=P_ΔP(α^I_J))
 {
  if (Δ ∈ {≤,<})
  {if (sup P^{M×A}(s, ◊^I_J accept) Δ p)
   sat=sat ∪ {s};
  }
  if (Δ ∈ {≥,>})
   {
     if(inf P^{M×A}(s,◊^I_J accept) Δ p)
    sat=sat ∪ {s};
   }
  if (Δ p={[n1,n2] |n1,n2≥0 且 n1<n2})
    {if(inf P^{M×A}(s,◊^I_J accept)≥n1 且 sup P^{M×A}(s,◊^I_J accept)≤n2)
    sat=sat ∪ {s};
    }
  }
  //由于篇幅有限，此处暂不对其他情况状态公式满意集计//
算方法进行具体说明
 }
```

7 实例构造

下面将同步进化积应用于简单数据传输系统，给出对应的系统模型、路径公式及同步进化积模型。

简单数据传输系统对应的 strCTMDP 如图 1 所示。为了简化描述，图 1 中用状态编号 s_i 代替了状态回报对，省略了状态回报表示。模型中状态与原子命题的对应信息见表 1。

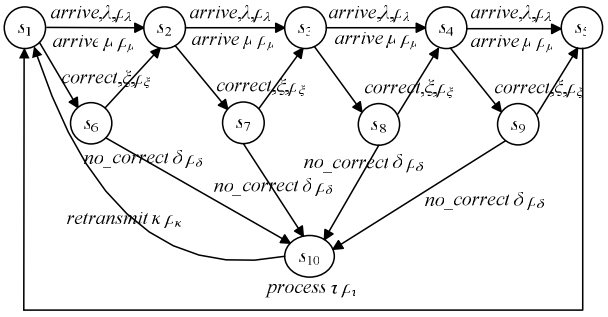

图 1 简单数据传输系统 strCTMDP 模型

表 1 状态信息描述

状态	状态回报对	原子命题	状态	状态回报对	原子命题
s_1	(s_1', ρ_1)	empty	s_6	(s_6', ρ_6)	error
s_2	(s_2', ρ_2)	ϕ	s_7	(s_7', ρ_7)	error
s_3	(s_3', ρ_3)	ϕ	s_8	(s_8', ρ_8)	error
s_4	(s_4', ρ_4)	ψ	s_9	(s_9', ρ_9)	error
s_5	(s_5', ρ_5)	full	s_{10}	(s_{10}', ρ_{10})	error

在图 1 所示模型中，取 aCSRL 路径公式 α 为((true, arrive)∪(true, arrive); (error, correct))*; (Ψ, arrive); (error, correct); (full, √)。它表示数据传输系统中数据包中的最后一个数据为被改正后的数据，而之前所有接收的数据要么为无错数据，要么为改正后的正确数据。α 对应的有限自动机如图 2 所示，此处假定动作迁移是基于某一确定的策略下进行的，两者的同步进化积如图 3 所示。

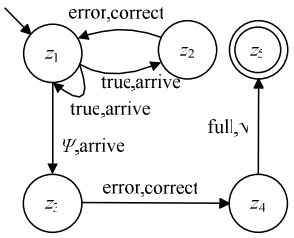

图 2　路径公式自动机表示

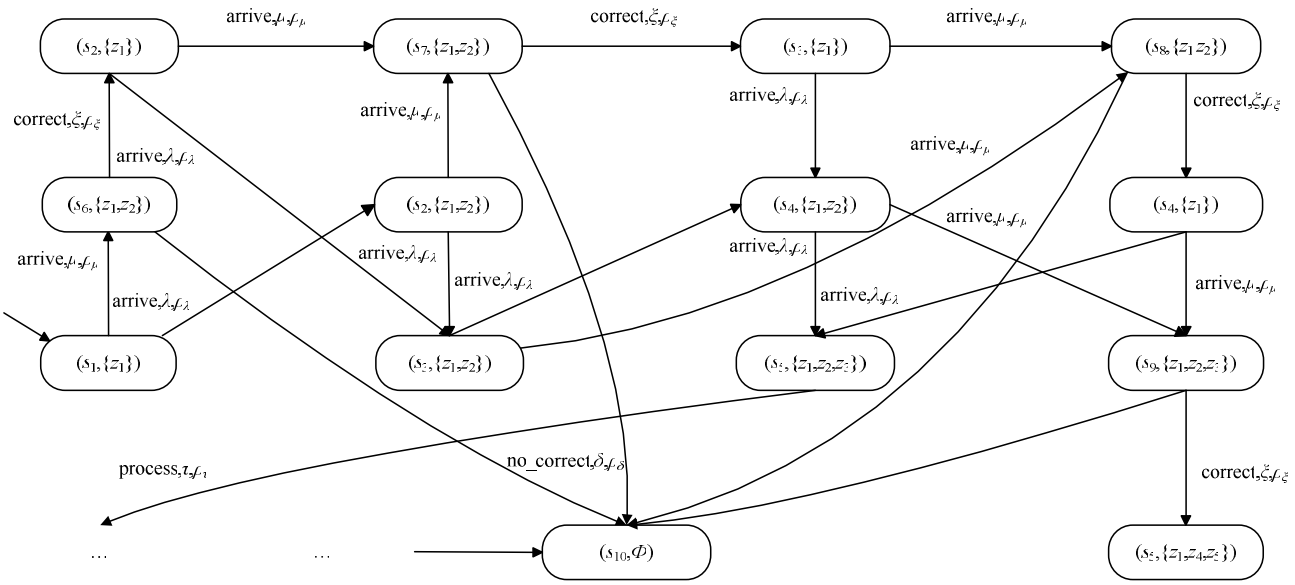

图 3　同步进化积

图 3 中不相关的状态被省略了，可以得出状态(s_5,{z_1, z_4, z_5})为构造所得的同步进化积的唯一接受状态。

8　结束语

本文使用了一种兼顾时间、空间等综合特征的复杂系统模型验证方法进行了实例验证分析，实例构造分析结果表明，此方法可有效地扩大模型检测技术的应用范围。下一步将对此方法中同步积模型的处理进行更深入的研究。

参考文献

[1] 赵会群, 孙　晶. 一种SOA软件系统可信性评价方法研究[J]. 计算机学报, 2010, 33(11): 2202-2210.

[2] 骆翔宇, 谭　征, 苏开乐, 等. 一种基于认知模型检测的 Web 服务组合验证方法[J]. 计算机学报, 2011, 34(6): 1041-1062.

[3] Zahmati A S, Fernando X, Grami A. A Continuous-time Markov Chain Model and Analysis for Cognitive Radio Networks[J]. Journal of Communication Networks and Distributed Systems, 2012, 8(3): 195-212.

[4] 钮　俊, 曾国荪, 王　伟. 基于模型检测的时间空间性能验证方法[J]. 计算机学报, 2010, 33(9): 1621-1633.

[5] 庄　琾, 蔡　勉, 沈昌祥. 基于交互式马尔可夫链的可信动态度量研究[J]. 计算机研究与发展, 2011, 48(8): 1464-1472.

[6] Buchholz P, MoritzHahn E, Hermanns H, et al. Model Checking Algorithms for CTMDPs[C]//Proc. of the 23rd International Conference on Computer Aided Verification. Berlin, Germany: Springer, 2011: 225-242.

[7] Flum J, GrädEl E, WilkE T. Logic and Automata: History and Perspectives[M]. Amsterdam, the Netherlands: Amsterdam University Press, 2008.

[8] Cloth L, Katoen J P, Khattri M, et al. Model Checking Markov Reward Models with Impulse Rewards[C]//Proc. of International Conference on Dependable Systems and Networks. [S. l.]: IEEE Computer Society, 2005: 722-731.

[9] Baier C, Cloth L, Haverkort B, et al. Model Checking Markov Chains with Actions and State Labels[J]. IEEE Transactions on Software Engineering, 2007, 33(4): 209-224.

[10] 初佃辉, 孟凡超, 战德臣, 等. 基于有限自动机的多层次构件行为匹配模型[J]. 软件学报, 2011, 22(11): 2668-2683.

编辑　顾逸斐