随机模型检测连续时间 Markov 过程

钮 俊[1,2,3] 曾国荪[1,2] 吕新荣[3] 徐 畅[3]
(同济大学计算机科学与技术系 上海 201804)[1]
(嵌入式系统与服务计算教育部重点实验室 上海 201804)[2]
(浙江工商职业技术学院信息工程学院 宁波 315012)[3]

摘 要 功能正确和性能可满足是复杂系统可信要求非常重要的两个方面。从定性验证和定量分析相结合的角度,对复杂并发系统进行功能验证和性能分析,统一地评估系统是否可信。连续时间 Markov 决策过程 CTMDP(Continuous-time Markov decision process)能够统一刻画复杂系统的概率选择、随机时间及不确定性等重要特征。提出用 CTMDP 作为系统定性验证和定量分析模型,将复杂系统的功能验证和性能分析转化为 CTMDP 中的可达概率求解,并证明验证过程的正确性,最终借助模型检测器 MRMC(Markov Reward Model Checker)实现模型检测。理论分析表明,提出的针对 CTMDP 模型的验证需求是必要的,验证思路和方法具有可行性。

关键词 功能性能,连续时间 Markov 决策过程,模型检测,可信验证,可达概率
中图法分类号 TP301 **文献标识码** A

Stochastic Model Checking Continuous Time Markov Process

NIU Jun[1,2,3] ZENG Guo-sun[1,2] LU Xin-rong[3] XU Chang[3]
(Department of Computer Science and Technology, Tongji University, Shanghai 201804, China)[1]
(Embedded System and Service Computing Key Lab of Ministry of Education, Shanghai 201804, China)[2]
(College of Information Engineering, Zhejiang Business Technology Institute, Ningbo 315012, China)[3]

Abstract The trustworthiness of a dynamic system includes the correctness of function and the satisfiability of performance mainly. This paper proposed an approach to verify the function and performance of a system under consideration integratedly. Continuous-time Markov decision process (CTMDP) is a model that contains some aspects such as probabilistic choice, stochastic timing and nondeterminacy, and it is the model by which we verify function properties and analyze performance properties uniformly. We can verify the functional and performance specifications by computing the reachability probabilities in the product CTMDP. We proved the correctness of our approach, and obtained our verification results by using model checker MRMC (Markov Reward Model Checker). The theoretical results show that model checking CTMDP model is necessary and the model checking approach is feasible.

Keywords Function and performance, Continuous-time Markov decision process, Model checking, Trusted verification, Reachability probabilities

研究分析复杂动态系统的可信性,是学术界和工程领域一直关注和研究的焦点。功能正确和性能可满足是复杂系统的可信性要求非常重要的两个方面。模型检测作为一种自动的、不需要人工干预的验证手段,被越来越多的研究者或工程人员用于对系统的安全性、活性、公平性等功能属性进行可信验证[1]。近年来,很多学者也运用测度论、随机过程等手段,采用模型检测技术对系统的性能进行可信评估[2]。

系统的可信要求除了要确保系统功能的正确性,还需要评估系统的服务响应时延、平均无故障时间及设备利用率、信道数据传输率、平均吞吐量、资源共享率等时间或空间特性方面的可用性、可靠性等方面的性质[3]。已经存在的各种形式模型及验证或分析方法,如文献[4]等,大多独立地对系统的功能或性能指标进行分析或验证,割裂了系统本身固有的功能、性能上的统一性。功能与性能的统一性体现在3个方面:①复杂并发系统的功能和性能特征往往是密切相关的,单纯的功能验证或性能分析模型无法有效地对复杂系统进行准确

到稿日期:2010-10-11 返修日期:2011-01-17 本文受863项目(2007AA01Z425,2009AA012201),973计划课题(2007CB316502),国家自然科学基金项目(90718015),NSFC-微软亚洲研究院联合资助项目(60970155),教育部博士点基金项目(20090072110035),上海市优秀学科带头人计划项目(10XD1404400),高效能服务器和存储技术国家重点实验室开放基金项目(2009HSSA06),浙江省宁波市自然科学基金项目(2010A610123),浙江省教育厅科研项目(Y201017075)资助。

钮 俊(1976—),男,博士生,讲师,主要研究方向为模型检测、性能评估,E-mail:tongjinj@gmail.com;曾国荪(1964—),男,博士,教授,博士生导师,主要研究方向为模型检测、可信软件、并行计算;吕新荣(1976—),男,硕士,讲师,主要研究方向为软件体系结构;徐 畅(1981—),男,硕士,讲师,主要研究方向为软件形式化方法。

刻画并分析；②断言一个系统功能正确，蕴涵了在满足既定功能要求的前提下，性能指标也符合需求约束；③当意图为系统进行时间或空间性能的分析时，首要的前提是要保证其功能的正确性。因此，在对系统进行建模时，将动态行为和时间、空间特征统一进行刻画是自然的、直观的、必要的。如果分别建立系统的功能验证模型和性能分析模型，客观上也很难保证两类模型的同一性，即证明其描述的为同一个系统。为了便于分析，本文仅考虑时间性能。

不确定性是大量复杂动态系统的重要特征，用以刻画系统多种不同的运行方式，包括内部不确定性和外部不确定性，可以刻画建模过程中需要考虑到的调度自由、实现自由、外部环境未知、不完全信息等[5]。连续时间 Markov 过程 CTMDP 是一种能够直观地刻画不确定性的随机模型[6]。交互式 Markov 链也能同时刻画动作、时间性能和不确定性，支持组合化操作[7]。尽管已经存在对应的模型验证算法，但绝大多数都是将其转化为均匀 CTMDP，并借用针对 CTMDP 的高效算法实现模型检测。

本文基于已有工作，提出采用带标记的 CTMDP 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换为 CTMDP 中满足验证属性的路径子集可达概率最值的求解，并借助模型检测器 MRMC 实现该计算过程。

1 连续时间 Markov 过程的基本概念

CTMDP 可看作特殊的标记传递系统，能够刻画连续、随机时间和概率转移，同时允许概率选择和不确定选择共存。相对于标记传递系统、Markov 链等模型，它具有更广的适用性。

定义 1(带标记连续时间 Markov 决策过程，CTMDP) CTMDP 为六元组 $C=(S,AP,Act,R,L,v)$，其中 S 和 Act 分别为状态和动作的非空可数有限集，AP 为原子命题集合，$R:S\times Act\times S\to\mathbb{R}_{\geqslant 0}$ 为转移率矩阵，$L:S\to 2^{AP}$ 为状态标记函数，$v\in Distr(S)$ 为初始分布，$Distr(S)$ 为集合 S 上所有概率分布的集合[6]。

在 CTMDP 中，如果动作集 Act 中只存在唯一的动作元素，即在该 CTMDP 中不存在不确定性动作，则可将其看作连续时间 Markov 链。如果 $\lambda=R(s,\alpha,s')>0$，则存在一个从状态 s 到状态 s' 的 α 转移，并且该转移在状态 s 下的停留时间的离开率为 $E(s,\alpha)=\sum_{s'\in S}R(s,\alpha,s')$。如果 $E(s,\alpha)>0$，则称动作 α 在状态 s 是使能的，集合 $Act(s)=\{\alpha\in Act(s)\mid E(s,\alpha)>0\}$ 代表状态 s 的使能动作集合并且确定了状态 s 的所有非确定选择。如果从状态 s 出发，有多个非确定性动作，即 $|Act(s)|>1$，则将进行非确定性选择执行。

CTMDP 中，路径为形如

$$\pi=s_0\xrightarrow{t_0,a_0}s_1\xrightarrow{t_1,a_1}\cdots\xrightarrow{t_{n-1},a_{n-1}}s_n$$

的序列，其中，$s_i\in S,a_i\in Act,t_i\in\mathbb{R}_{\geqslant 0}(i\leqslant n)$，$n$ 为路径的长度，记为 $|\pi|=n$。记 CTMDP 模型 C 中从状态 s 出发所有路径的集合为 $Path^C(s)$。

定义 2(均匀 Markov 过程) 对连续时间 Markov 决策过程 $C=(S,AP,Act,R,L,v)$，如果对所有 $s\in S$ 及 $\alpha\in Act(s)$，存在 $\hat{E}>0$，满足 $E(s,\alpha)=\hat{E}$，则称 C 是均匀的，其中 $\hat{E}$ 称为均匀转出率[6]。

定义 3(带标记连续时间 Markov 链[2]) 带标记连续时间 Markov 链为四元组 (S,AP,L,R)，其中 $R:S\times S\to\mathbb{R}_{\geqslant 0}$ 为转移函数，S、AP、L 的定义与定义 1 中类似。

连续时间 Markov 链中，转移序列

$$s_0\xrightarrow{t_0}s_1\xrightarrow{t_1}s_2\xrightarrow{t_2}\cdots\xrightarrow{t_{n-2}}s_{n-1}\xrightarrow{t_{n-1}}s_n\cdots$$

表示一条无限路径，其中 t_i 为与 R 有关的函数，表示在状态 s_i 的延迟时间。如果 s_j 为吸收态，则称转移序列 $s_0\xrightarrow{t_0}s_1\xrightarrow{t_1}s_2\xrightarrow{t_2}\cdots\xrightarrow{t_{j-2}}s_{j-1}\xrightarrow{t_{j-1}}s_j$ 为一条有限路径。设 $\tau(\sigma)=\sum_{m=0}^{j-1}t_m$ 表示路径 σ 的花费时间。记 $Path^M(s)$ 表示在连续时间 Markov 链模型 M 中，从状态 s 出发的所有路径的集合。通过构造集合 $Path^M(s)$ 上的 Borel 空间，为路径集合定义概率测度 $Pr^M(s)$[8]。给定 M，从状态 s 出发，在时刻 t 处于状态 s' 的概率用 $\pi^M(s,s',t)$ 表示，即 $\pi^M(s,s',t)=Pr^M(s)\{\sigma\in Path^M(s)\mid\sigma@t=s'\}$ 表示瞬时概率；$\pi^M(s,s')=\lim_{t\to\infty}(\pi^M(s,s',t))$ 表示稳态概率，即一直停留于状态 s' 的概率。

不确定性是 CTMDP 的固有属性，能保证大多数场景下复杂系统的建模需要。在对 CTMDP 进行分析或计算时，需要指定从该状态出发将要执行的具体动作，从而消除掉其所有的不确定性。形式化地，如果状态 s_i 满足 $|Act(s_i)|\geqslant 2$，则需要选择某个具体动作 $\alpha\in Act(s_i)$ 作为下一步将要执行的动作。此时，称状态 s_i 为决策点。决策点下一步将要执行的动作的选择依赖于从初始状态到该状态的路径片段上的历史相关信息和动作的选取方式。

定义 4(调度，Scheduler) 为所有带有不确定性动作的状态指定后继动作、消除不确定性的过程。

一般地，在对某个具体的 CTMDP 的不确定性进行消解的过程中，消解策略是一致的，即所有决策点所采用的调度规则均一致。根据调度对历史信息的依赖程度，可将其分为历史相关性和无记忆性两种。如果调度依赖于历史信息，则称其为历史相关(History-dependent)的，否则称其为无记忆性(Memoryless)。根据不确定性动作的选取方式，调度又可分为随机调度(Randomized)和确定性调度(Deterministic)。因此，调度可分为历史相关的随机调度(HR)、历史相关的确定性调度(HD)、无记忆性的随机调度(MR)和无记忆性的确定性调度(MD)等类型[6]。

显然，由调度的定义可以看出，它是某个从状态空间到动作集合的函数 $d:S\to Act$。并且，通过调度，CTMDP 将被转化成连续时间 Markov 链。对某个 CTMDP 系统，根据调度的历史信息依赖方式及不确定性动作的选取方式，存在多种类型的多个调度，当前所考虑的调度类型下的所有调度的集合记为 D。在本文中，为了便于描述和分析，选取 HD 型调度进行说明。根据前文的说明，HD 型调度可用函数 $d:S^+\to Act$ 表示。由策略 d 诱导的连续时间 Markov 链 M 上的概率测度定义为 $Pr^M(s,d)$。

2 功能属性的自动机表示

在本文中，功能属性表示 CTMDP 模型中的动作序列应该满足的性质或约束，CTMDP 的功能行为由可观动作的执行序列刻画。功能性能验证的核心思想是验证系统在功能满足的前提下，性能指标是否符合期望的限定。因此，对 CTMDP 进行功能和性能的统一验证分为 3 个步骤：①获得从某状态出发且其动作序列满足功能属性的路径集合；②计算路径集合上的需要关注的所有量化的性能指标；③判断这些量化

指标是否满足给定范围。本文将待验证的功能行为用元事件符号的正则式表示。由正则语言和自动机的等价性，将表示功能属性的正则表达式转换为对应的有穷自动机，为下一步在 CTMDP 中标注满足该功能属性的路径集合做准备。

2.1 功能属性的正则表示

根据前面的叙述，从某状态出发，可延伸出多条不同的路径，代表系统所有可能的演化趋势。一条路径表示系统的一次具体执行，即系统所有可能的动态行为中的某个具体事件的发生。暂时只关注路径上的动作，记路径 $\pi=s_0 \xrightarrow{t_0,a_0} s_1 \xrightarrow{t_1,a_1} \cdots \xrightarrow{t_{n-1},a_{n-1}} s_n$ 被抽取时间信息(time-abstract)后的表示形式为

$$\pi'=s_0 \xrightarrow{a_0} s_1 \xrightarrow{a_1} \cdots \xrightarrow{a_{n-1}} s_n$$

该表示可看作状态和动作的交互序列。从某状态出发，可能存在多个不同的后继动作；不同的状态也可能具有同名的后继动作。因此，路径需用状态及从该状态出发的动作的有序对的序列来表示。在本文中，这种有序对被称为元事件，它刻画系统在某状态的某个可能的局部行为。

定义 5(元事件) 表示系统的局部行为，由状态及从该状态出发的可能动作构成的二元有序对表示，记为(s_i,α_i)，其中 $s_i\in S$ 表示系统状态，$\alpha_i\in Act(s_i)\in S$ 表示从状态 s_i 出发的可能动作。

所有元事件的集合记为 *atomic_events*，表示系统所有可能的局部行为。集合 *atomic_events* 中的元素也被称为元事件符号。将路径用元事件符号的序列表示后，一条路径就可用集合 *atomic_events* 上的“字”(word)来表示。

定义 6(路径) 集合 *atomic_events* 上的有限或无限字，分别表示有限路径或无限路径。可由元事件$(s_i,\alpha_i)(i\geqslant 0)$构成的执行序列表示，即 $e_1,\cdots,e_n,\cdots=(s_1,\alpha_1),\cdots,(s_n,\alpha_n),\cdots$，其中，$e_i\in atomic\_events$。

在本文中，用集合 *atomic_events* 上的正则文法来定义满足某种规则的字，即代表其动作序列满足某种规则的所有路径的集合。

定义 7(功能属性的正则表示) $\wp ::=\varepsilon(|a\_e|\wp,\wp|\wp+\wp|\wp^*$，其中，$\wp$ 表示功能属性规范，ε 表示空路径，$a\_e\in atomic\_events$ 为元事件符号，$\wp,\wp$ 表示两个功能属性规范的顺序组合，$\wp+\wp$ 刻画选择，$\wp^*$ 表示闭包运算。

表达功能属性的正则表达式 $\wp$ 规定了路径上的动作序列应该满足的性质，它对应原始模型中的某个路径集合，该集合中所有路径上的动作序列满足该性质。用 $Path^C(\wp)$ 表示连续时间 Markov 决策过程 C 中满足路径规范 $\wp$ 所限定的所有路径的集合。通过判断一条路径 ζ 是否属于该集合，可确定该路径的动作序列是否满足 $\wp$ 限定的约束。

2.2 功能属性到自动机的转换

根据前面的说明，我们需要标注出在 CTMDP 中满足功能属性的路径的集合。因此，根据正则表达式和有限自动机的等价性，需要将路径规范转化为自动机，该自动机的输入符号集为集合 *atomic_events*。根据自动机理论，该转换过程很容易实现[9]。

定义 8(属性自动机) 属性自动机为五元组 $A=(Z,\Sigma,\delta,Z_0,F)$，其中 Z 是状态的有限集，$\Sigma\subseteq atomic\_events$，$\delta:Z\times\Sigma\to 2^Z$ 为转移函数，$Z_0\subseteq Z$ 为初始状态集合，$F\subseteq Z$ 为接收状态集合，$L(A)\subseteq(\Sigma)^*$ 表示 A 的可接受语言。

设 $\sigma=(s_1,e_1),\cdots,(s_n,e_n)$ 为某条路径，可获得 σ 在自动机中的运行情况，即路径所表达的行为的一次匹配判断[10]。路径 σ 可能被自动机接受，也可能被拒绝。如果路径在自动机中的一次运行，最后进入集合 F 中的状态，则表明该路径被自动机接受，这也说明该路径上的行为满足自动机所表示的行为规范。设连续时间 Markov 决策过程 C 中被表示功能属性 $\wp$ 的自动机 A 接受的路径集合为 $Path^C(A)$，由正则语言与自动机理论可知，$Path^C(\wp)=Path^C(A)$。因此，可将该自动机作为 C 中某些满足用正则规范 $\wp$ 表示的有限路径的接受器。通过路径自动机，可以得到满足特定行为规范的所有路径的集合。为了描述方便，需要将转移函数扩展为 δ'：$2^Z\times Path^C\to 2^Z$，即参数为状态集合和路径[7,8]，而非前面的状态和单个元事件符号。由于在自动机中，单个状态不能触发状态的转移，因此 $\delta'(Z',s)=Z'$。对于从状态 s 出发并紧跟着动作 α 的路径，有

$$\delta'(Z',sa\sigma')=\delta'\Big(\bigcup_{z'\in Z'}\bigcup_{s\models\Psi}\delta(z',\Psi a),\sigma'\Big)$$

式中，Ψ 为 Σ 中的有限字，为所有可能出现于 Σ 中的公式集合。

经过扩展的转移函数表示路径 σ 从 Z' 状态出发的一次运行后达到的状态集合。通过该函数，可以判断当前路径的功能行为是否满足给定的行为规范，即功能性的匹配判断。类似于文献[10]的结论，得到下面的命题。

命题 1 设 C 为考虑的连续时间 Markov 决策过程，$\wp$ 为表示功能属性的正则式，$A=(Z,\Sigma,\delta,Z_0,F)$ 是其对应的路径自动机。自动机 A 所代表的路径集合为模型 C 中行为上符合 $\wp$ 的所有路径的集合，即

$$Path^C(\wp)=\{\sigma\in Path^C(A)\,|\,\delta'(Z_0,\sigma)\cap F\neq\emptyset\}$$

该命题表达了如何判定某条路径的功能行为满足指定的规范。这个式子表明了模型 C 中被正则式 $\wp$ 接受的路径的集合。因此，模型 C 中满足条件 $\delta'(Z_0,\sigma)\cap F\neq\emptyset$ 的路径为符合正则式 $\wp$ 所表示的规范的路径。因此，根据路径规范及路径自动机，从模型中就可以找到满足该行为约束的路径集合。

3 描述验证性质的时态逻辑的语法语义

在模型验证中，系统的待验证性质用某种时态逻辑公式表示。本文中，基于 CTMDP 模型，为了验证系统的功能和时间性能，需要一种能表达功能和性能的形式规范语言。用该语言书写的公式不仅能够表达用正则式表示的功能属性的约束，同时能刻画连续时间性能。在常见的表达系统功能性质的时态逻辑(如 LTL、CTL 和 CTL*)中，用状态迹(trace)表示系统的动态演化过程，不能描述性能约束；在时间性能验证方面，表示性能属性的时态逻辑，如 PCTL、PTCTL 和 CSL (Continuous Stochastic Logic)等用基于状态公式的 X 算子和 U 算子表示基于路径的功能属性。本文采用一种扩展于 CSL 的时态逻辑 pathCSL[9] 统一描述功能和连续时间性能属性，特别地，功能属性部分用正则式来表示。通过定性和定量相结合的方式，统一刻画系统的功能和性能属性。

定义 9(状态公式的语法)

$$\Phi ::=q\,|\,\neg\Phi\,|\,\Phi\wedge\Phi\,|\,S_{\bowtie p}(\Phi)\,|\,P_{\bowtie p}(\wp^{\leqslant t})$$

式中，Φ 表示状态公式，q 表示原子命题，式子$\leqslant t$ 相当于$[0,$

$t]$；$S_{\infty p}(\Phi)$表示系统最终处于$\{s\in S|s\vDash\Phi\}$中状态的概率满足限定∞p；$P_{\infty p}(\wp^{\leqslant t})$表示功能和性能的统一验证规范：行为属性满足$\wp$且执行时间满足$\leqslant t$的概率，$p\in[0,1]$满足限定$\infty p$，$\infty\in\{<,\leqslant,>,\geqslant\}$。

状态公式通过其语义进行解释。形式化地，其规则定义如下。

定义 10(状态公式的语义)

$C,s\vDash q$ iff $q\in L(s)$

$C,s\vDash\neg\Phi$ iff $C,s\nvDash\Phi$

$C,s\vDash\Phi_1\wedge\Phi_2$ iff $(C,s\vDash\Phi_1)\wedge(C,s\vDash\Phi_2)$

$C,s\vDash S_{\infty p}(\Phi)$ iff $\pi^C(s,Sat^C(\Phi))\infty p$

$C,s\vDash P_{\infty p}(\wp^{\leqslant t})$ iff $\forall d\in D.\ Prob(C,s,d)(\wp^{\leqslant t})\infty p$

其中$Prob(C,s,d)(\wp^{\leqslant t})=Pr^M(s,d)\{\zeta\in Path^C(\wp)|\tau(\zeta)\leqslant t\}$表示在策略$d$下从$s$出发并满足公式$\wp^{\leqslant t}$的概率，$M$为$C$在当前策略$d$下所诱导产生的连续时间 Markov 链，$Sat^C(\Phi)=\{s\in S|C,s\vDash\Phi\}$表示公式$\Phi$的可满足集合。

在对 CTMDP 进行功能和时间性能的模型检测中，以带标记的 CTMDP $C=(S,AP,Act,R,L,v)$和 pathCSL 状态公式Φ作为输入，返回满足该公式的集合$Sat^C(\Phi)\subseteq S$。除$P_{\infty p}(\wp^{\leqslant t})$外，其它算子的处理与 Markov 链中一样[10]。对该特殊算子，需要确定在所有可能的调度d下$P_{\infty p}(\wp^{\leqslant t})$是否成立。直观地，需要计算在所有调度下满足$\wp^{\leqslant t}$的所有路径集合的概率，并求其最大值或最小值，进而判断是否满足限定∞p。具体验证过程中，需要根据关系比较算子的类型来确定求解何种最值。显然，如果比较算子为$\leqslant$或$<$，则$Sat(P_{\infty p}(\wp^{\leqslant t}))=\{s\in S|p^{\max}(s,\wp^{\leqslant t})\infty p\}$；如果比较算子为$\geqslant$或$>$，则$Sat(P_{\infty p}(\wp^{\leqslant t}))=\{s\in S|p^{\min}(s,\wp^{\leqslant t})\infty p\}$，其中

$$p^{\max}(s,\wp^{\leqslant t})\overset{def}{=}\sup_{d\in D}[Prob(C,s,d)(\wp^{\leqslant t})] \tag{1}$$

$$p^{\min}(s,\wp^{\leqslant t})\overset{def}{=}\inf_{d\in D}[Prob(C,s,d)(\wp^{\leqslant t})] \tag{2}$$

因此，公式$P_{\infty p}(\wp^{\leqslant t})$的模型检测问题最终要转化为在连续时间 Markov 决策过程中最大(或最小)可达概率的计算。我们的做法是通过表达路径规范的$\wp$的路径自动机在连续时间 Markov 决策过程中的匹配运行，即可获得路径自动机与 CTMDP 的同步过程。在其中标注满足功能约束规范的路径集合，并计算该集合中时间消耗满足时间约束t的路径子集的概率。由于在确定性调度下连续时间 Markov 决策过程会诱导产生对应的连续时间 Markov 链，因此直观地，可通过已知的在连续时间 Markov 链中求概率的方法进行求解，然后再比较，得到最大、最小值。但这将导致算法的复杂度比较高，因为该过程需要强力遍历所有的可能调度。

4 模型检测连续时间 Markov 过程

4.1 构造功能属性自动机与 CTMDP 的同步过程

模型检测过程与文献[10]类似。功能属性自动机限定了行为规范满足特定规范的路径集合，结合时态逻辑 pathCSL 的语义，为了得到满足功能属性的路径集合，可将表示动作约束的功能属性自动机作为验证模型中路径集合的接受器：在原始 CTMDP 模型中模拟自动机的运行，构造二者的同步演化过程；给模型中满足行为规范的路径添加特殊标记，即得到模型中满足该行为规范的路径集合。同步演化过程是 CTMDP 与自动机的积模型，定义如下。

定义 11(同步 Markov 过程) 带标记的 Markov 过程$C=(S,AP,Act,R,L,v)$与自动机$A=(Z,\Sigma,\delta,Z_0,F)$的同步积为

$$C\times A=(S^{C\times A},AP^{C\times A},Act^{C\times A},R^{C\times A},L^{C\times A},v^{C\times A})$$

其中，

$S^{C\times A}=\{(s,Z')|s\in S\wedge Z'\in 2^Z\}$；

$Act^{C\times A}=Act$；

$AP^{C\times A}=AP\cup\{accept\}$；

如果$Z\cap F\neq\emptyset$，则$L^{C\times A}((s,Z'))=L(s)\cup\{accept\}$，否则$L^{C\times A}((s,Z'))=L(s)$；

如果$Z_2=\delta'(Z_1,s_1\xrightarrow{a}s_2)$，则$R^{C\times A}((s_1,Z_1),a,(s_2,Z_2))=R(s_1,a,s_2)$，否则$R^{C\times A}((s_1,Z_1),a,(s_2,Z_2))=0$；

$v^{C\times A}=v$；

在同步演化过程的定义中，状态由两部分构成，即原始模型中的某个状态和路径自动机中的某些状态。为了标志某条路径是否被自动机接受，新增加原子命题 *accept*，动作集合不变。转移函数的定义是为了模拟自动机在模型中的演化情况。同步过程中的一条路径模拟原始模型中对应路径在属性自动机中从某些状态出发的运行情况。如果状态(s,Z')有 *accept* 标志，即$accept\in L^{C\times A}(s,Z')$，则由命题 1 的结论可知，所有终止于该状态的路径上的行为规范都满足路径自动机所定义的路径行为约束。基于文献[10]，同理可得下面命题。

命题 2 给定连续时间 Markov 决策过程$C=(S,AP,Act,R,L,v)$和路径规范$\wp$对应的自动机$A=(Z,\Sigma,\delta,Z_0,F)$，则$Prob(C,s,d)(\wp^{\leqslant t})$的值为在积模型$C\times A$中从状态$(s,Z_0)$出发，在时间$t$内达到目标状态(*accept* 状态)的概率。

4.2 带有时间约束可达概率最值的计算[6]

由前面的描述可知，需要求解在积模型中可达概率的上(或下)确界，即求式(1)、式(2)。积模型亦为 CTMDP 模型，故最终需要在 CTMDP 中求解可达概率的上(或下)确界，根据最优调度的存在性，即需求可达概率的最大(或最小)值。文献[4]提出的计算方法，其基本思想是首先假定能使概率取得最值的调度d_0存在。理论上已经证明，该值只与调度d_0前面的k个不确定动作的选取有关。在第k个不确定动作选择点，不确定动作选择的依据是使得从状态s出发，经过最多一步转移到达集合B中状态的概率为最大。当$1<i<k$时，需满足执行完第$i<j<k$步选择，满足从状态s出发，经过最多$k-i+1$步转移到达集合B中的概率为最大。依此类推，可获得满足条件的最优调度d_0，最终求得可达概率的最值。

4.3 模型检测过程

设对于 CTMDP 模型C以及需要验证的状态公式Φ，简单公式q、$\neg\Phi$、$\Phi\wedge\Phi$、$S_{\infty p}(\Phi)$很容易求解。对于复杂公式$P_{\infty p}(\wp^{\leqslant t})$，求解过程相对来说比较复杂。模型检测步骤如下：

- 对模型C进行均匀化处理；
- 根据正则语言与自动机相关理论，求功能属性正则式$\wp$对应的有穷自动机A；
- 构造自动机A与模型C的积过程模型$C\times A$，并标注可达状态；
- 运用模型检测器 MRMC(Markov Reward Model Checker)对积模型$C\times A$进行带有时间约束上界的可达概率求解。

(下转第 125 页)

proaches, technologies and research issues[J]. The VLDB Journal - The International Journal on Very Large Data Bases, 2007, 16(3): 389-415

[2] Harel D, Maoz S. Assert and Negate Revisited: Modal Semantics for UML Sequence Diagrams[J]. Software and Systems Modeling, 2008, 7(2): 237-252

[3] OASIS. Web Service Business Process Execution Language Version 2.0 Specification[EB/OL]. http://docs.oasis-open.org/wsbpel/2.0/wsbpel-v2.0.pdf. 2007

[4] Jhala R, Majumdar R. Software model checking[J]. ACM Comput Surv, 2009, 41: 1-54

[5] Object Management Group(OMG). UML: Superstructure version 2.0 [S]. 2005

[6] 李雯睿. 基于 uMSD 的 Web 服务组合验证技术研究[D]. 南京: 河海大学, 2010

[7] Kupferman O, Vardi M. Weak alternating automata are not that weak[J]. ACM Trans. Comput. Log, 2001, 2(3): 408-429

[8] Holzmann G J. The SPIN Model Checker: Primer and Reference Manual[M]. Addison-Wesley, 2004

[9] 范贵生, 虞慧群, 陈丽琼, 等. 基于 Petri 网的服务组合故障诊断与处理[J]. 软件学报, 2010, 21(2): 231-247

[10] Lohmann N, Massuthe P, Stahl C, et al. Analyzing interacting WS-BPEL processes using flexible model generation[J]. Data & Knowledge Engineering, 2008, 64(1): 38-54

[11] Dijkman R M, Dumas M, Ouyang C. Semantics and analysis of business process models in BPMN[J]. Information and Software Technology, 2008, 50(12): 1281-1294

[12] 侯丽珊, 金芝, 吴步丹. 需求驱动的 Web 服务建模及其验证: 一个基于本体的方法[J]. 中国科学 E 辑, 2006, 36(10): 1189-1219

[13] Foster H, Uchitel S, Magee J, et al. WS-Engineer: A Tool for Model-based Verification of Web Service Compositions and Choreography[C]// IEEE International Conference on Software Engineering(ICSE 2006). Shanghai, China, 2006

[14] Abouzaid F, Mullins J. A calculus for generation, verification and refinement of bpel specifications[J]. Electronic Notes in Theoretical Computer Science, 2008, 200(3): 43-65

[15] 雷丽晖, 段振华. 一种基于扩展有限自动机验证组合 Web 服务的方法[J]. 软件学报, 2007, 18(12): 2980-2990

[16] Diaz G, Cambronero M, Tobarra M L, et al. Analysis and Verification of Timed Properties Applied to Web Service Compositions [C]// Proc. WS-FM. 2006: 178-192

(上接第 115 页)

通过以上步骤，可获得在模型 C 的状态空间中公式 $P_{\infty p}(\wp^{\leq t})$ 的可满足集合。其中，对于验证步骤的第一步，设某信息系统的抽象模型如图 1 所示。该模型具有 4 个状态，用圆圈表示，状态的标记分别为 $\{init\}$、$\{try\}$、$\{succ\}$、$\{false\}$。转移用箭头表示，箭头旁的组合符号分别表示该转移的触发动作和转移率。

由图 1 可知，在 $\{try\}$ 状态中存在不确定的两个动作 E、D。该模型经过均匀化处理后，结果如图 2 所示。

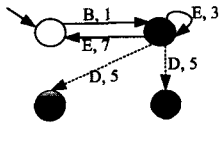

图 1　原始模型

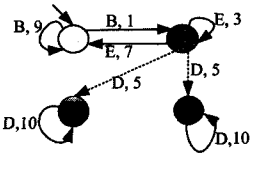

图 2　均匀处理后的模型

模型检测器 MRMC 为荷兰 Twente 大学、德国亚琛大学等合作开发的针对随机、概率系统的模型检测工具[11]，目前可免费使用。它支持的模型有 Markov 链、Markov 过程以及各种带有回报结构(Reward Structure)的变体[12]。特别地，它支持具有内部不确定性的连续时间 Markov 决策过程对于 CSL 公式的模型检测，正好满足本文的验证需要。在积模型中的可达概率求解，可直接用 MRMC 得出结果，并进一步得到可满足集合。限于篇幅，图 1、2 所示模型的具体验证过程不再给出。上述模型检测算法的复杂度分析过程可参考相关文献。

结束语　本文从理论上分析了对 CTMDP 模型进行功能性能验证的可行性，并给出了验证方法。验证过程分为如下步骤：首先，建立系统的 CTMDP 模型；其次，将待验证的功能和性能的统一性质用 pathCSL 表示；然后，将表示功能属性的正则式转换成有穷自动机，与 CTMDP 模型进行求积；最后，运用模型检测器 MRMC 获得满足验证属性的状态空间子集。如果关注的状态不满足期望属性，则改进 CTMDP 模型，从而提高设计的有效性。上述子过程均可通过已有的成熟方法进行。分析表明，本文提出的基于 CTMDP 模型的验证方法和步骤是可行的。下一步将研究带有回报结构的 Markov 过程的功能性能验证方法。

参 考 文 献

[1] Clarke E M, Grumberg O, Peled D A. Model Checking [M]. Cambridge: MIT Press, 2000

[2] Baier C, Haverkort B, Hermanns H, et al. Model-checking algorithms for continuous time Markov chains[J]. IEEE Transaction on Software Engineering, 2003, 29(6): 524-541

[3] 郭兵, 沈艳, 邵子立. 绿色计算的重定义与若干探讨[J]. 计算机学报, 2009, 32(12): 2311-2319

[4] 董威, 王戟, 齐治昌. UML Statecharts 的模型检验方法[J]. 软件学报, 2003, 14(4): 750-756

[5] Puterman M L. Markov Decision Processes: Discrete Stochastic Dynamic Programming[M]. New Jersey: John Wiley & Sons, 1994

[6] Baier C, Hermanns H, Katoen J-P, et al. Efficient computation of time-bounded reachability probabilities in uniform continuous-time Markov decision processes[J]. Theoretical Computer Science, 2005, 345(1): 2-26

[7] Hermanns H. Interactive Markov Chains[D]. Friedrich-Alexander-University. Erlangen-Nurnberg, 1998

[8] Baier C, Katoen J-P. Principles of Model Checking[M]. Massachusetts: The MIT Press, 2008

[9] Cloth L, Haverkort B, Hermanns H, et al. Model Checking path CSL[C]// Proc. of PMCCS-6. Illinois USA: September 2003: 19-22

[10] 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

[11] Markov Reward Model Checker Version 1.4.1 Manual[OL]. http://www.mrmc-tool.org/downloads/MRMC/Specs/. 2009

[12] 钮俊, 曾国荪, 陈波. 一种刻画功能和时间空间性能的同意验证模型 atsFPM[J]. 计算机学报, 2009, 32(4): 740-750