软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software, 2022,33(10):3717–3731 [doi: 10.13328/j.cnki.jos.006301]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

随机混成系统稀有属性的统计模型检测方法*

房丙午[1,2], 黄志球[1,3], 谢 健[1,3]

[1](高安全系统的软件开发与验证技术工业和信息化部重点实验室(南京航空航天大学), 江苏 南京 211106)

[2](安徽财贸职业学院 信息工程学院, 安徽 合肥 230601)

[3](南京航空航天大学 计算机科学与技术学院, 江苏 南京 211106)

通信作者: 黄志球, E-mail: zqhuang@nuaa.edu.cn

摘 要: 统计模型检测, 已成为随机混成系统安全性验证的重要方法. 但对安全性要求较高的系统, 其不安全事件和系统失效都是稀有事件. 在这种情况下, 统计模型检测很难采样到满足稀有属性的样本而变得不可行. 针对该问题, 提出了交叉熵迭代学习的统计模型检测方法: 首先, 使用连续时间马尔可夫链表示随机混成系统的路径概率空间, 推导出路径空间上的参数化概率分布函数族; 然后构造了随机混成系统路径空间上的交叉熵优化模型, 提出了在路径空间上迭代学习最优重要性采样分布的算法; 最后给出了基于重要性采样的稀有属性验证算法. 实验结果表明: 该方法能够有效地对随机混成系统的稀有属性进行验证; 且在相同样本数量下, 与一些启发式重要性采样方法相比, 该方法的估计值能够更好地分布在均值附近, 标准方差和相对误差减少超过了一个数量级.

关键词: 随机混成系统; 安全性; 稀有属性; 交叉熵迭代学习; 统计模型检测

中图法分类号: TP311

中文引用格式: 房丙午, 黄志球, 谢健. 随机混成系统稀有属性的统计模型检测方法. 软件学报, 2022, 33(10): 3717–3731. http://www.jos.org.cn/1000-9825/6301.htm

英文引用格式: Fang BW, Huang ZQ, Xie J. Statistical Model Checking for Verification of Rare Properties of Stochastic Hybrid System. Ruan Jian Xue Bao/Journal of Software, 2022, 33(10): 3717–3731 (in Chinese). http://www.jos.org.cn/1000-9825/6301.htm

Statistical Model Checking for Verification of Rare Properties of Stochastic Hybrid System

FANG Bing-Wu[1,2], HUANG Zhi-Qiu[1,3], XIE Jian[1,3]

[1](Key Laboratory for Safety-critical Software Development and Verification, Ministry of Industry and Information Technology (Nanjing University of Aeronautics and Astronautics), Nanjing 211016, China)

[2](College of Information Engineering, Anhui Finance & Trade Vocational College, Hefei 230601, China)

[3](College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211016, China)

Abstract: Statistical model checking (SMC) is an important method for the verification of safety of stochastic hybrid system (SHS), while for the system with extremely high safety requirements, the unsafe events and the failures of the system are rare events. In this case, it is difficult for SMC to draw the samples satisfying the rare properties and the SMC becomes infeasible. To solve this problem, an SMC method based on cross entropy iterative learning is proposed in this study. First, a continuous time Markov chain (CTMC) is used to represent the path probability space of the SHS, and based on the path space, a parameterized probability distribution family is derived. Then, the cross-entropy optimization model on the path space is constructed and an iterative learning algorithm is proposed, which can find the optimal importance distribution in the path space. Finally, an algorithm for verification of rare properties is given. Experimental results show that the proposed method can effectively verify rare properties of the SHS, and compared with some heuristic importance sampling methods, in the same number of samples, the estimated value of the proposed method can be better distributed near the sample mean, and the standard deviation and relative error are reduced by more than an order of magnitude.

* 基金项目: 国家重点研发计划(2016YFB1000802, 2018YFB1003902); 高安全系统软件开发与验证技术工业和信息化部重点实验室(南京航空航天大学)研究项目(NJ2019006)

收稿时间: 2020-03-02; 修改时间: 2020-07-17, 2020-12-04; 采用时间: 2021-01-05

Key words: stochastic hybrid system (SHS); safety; rare properties; cross entropy iterative learning; statistical model checking (SMC)

随机混成系统(stochastic hybrid system, SHS)[1]广泛应用在航空航天、交通运输、医疗卫生和工业控制等安全关键领域. 该类系统在运行时违背安全属性, 将严重威胁人们的生命和财产安全. 由于 SHS 物理层连续变化的行为与决策控制层的离散变化的行为相互交织, 系统的状态空间是无限的. 因此, 对 SHS 进行安全属性验证是一个严峻的挑战[2].

随机模型检测[3]是保证 SHS 安全性的一个重要方法. 随机模型检测通过形式化方法验证系统行为满足安全属性规约的概率. 随机模型检测可分为概率模型检测(probabilistic model checking, PMC)[4,5]和统计模型检测(statistical model checking, SMC)[6,7], PMC 和 SMC 都能够定性和定量地计算随机系统满足给定的时序逻辑属性的概率. 但 PMC 需要穷尽系统所有可能路径, 存在状态空间爆炸问题, 限制了所解决问题的规模[6]. SMC 通过采样 SHS 执行路径, 使用统计分析技术近似地计算目标系统满足时序逻辑属性的概率, 并能给出任意精度的误差界限[6,7]. 因此, SMC 在不需要分析目标系统内部复杂逻辑的情况下验证 SHS 的安全性, 有效地规避了系统的复杂性且不存在状态空间爆炸问题. 目前, SMC 是 SHS 安全属性验证最有效的解决方法之一[8−10].

SMC 主要的计算代价是系统模拟, 对于一般的安全属性验证, 可能仅需要 10^4 数量级的样本即可给出较高精度的概率估计[11]; 对于安全性要求较高的 SHS, 其安全属性的否命题, 亦即系统违背安全属性发生的概率非常小(一般认为发生概率低于 10^{-8}), 称这类安全属性为稀有属性(rare property)[9,12]. 在稀有属性验证的情况下, 为了达到给定的估计精度需要非常大的样本数量. 例如: 根据相对误差计算公式(16), 当稀有属性的概率 p=10^{-8}、相对误差为 0.01 时, SMC 需要样本数 10^{12}, 这是一个非常庞大的样本数量. 出现这种情况是由于传统的 SMC 方法很难采样到满足稀有属性的样本. 针对该问题, 一种有效的途径是尽可能地减小样本方差 $Var[\hat{p}]$[11]. 重要性采样是减少估计方差的有效方法[13,14], 重要性采样的关键问题是寻找一个最优重要性采样分布, 最优重要性采样分布是零方差的估计器, 理论上是存在的, 但在实践中很难获取. 现有的 SMC 方法通过获取一个近似最优的重要性采样分布使得估计方差达到最小, 以加速 SMC 的收敛性. Reijsbergen[15]针对 CTMC 模型, Barbot[16]针对 DTMC 模型, 分别提出了一种基于重要性采样的 SMC 方法, 这两种方法都通过启发式方法获得一个重要性采样分布来完成系统属性的验证. Clarke 和 Zuliani[9,17]假设 SHS 路径的概率分布是呈指数分布的, 使用交叉熵最小化方法在指数分布族中获得一个重要性采样分布, 并给出了 SHS 安全属性验证方法. Jegourel[18]使用参数化的随机卫式命令规约系统模型, 使用交叉熵最小化方法, 基于参数化系统模型获得一个重要性采样分布, 该方法可以通过增加随机卫式命令的个数来更好地近似系统的路径分布. 然而在上述方法中, 最优重要性采样分布不是来自系统路径空间上的分布族, 虽然能以较大的概率采样到稀有属性, 但并不能保证采样的样本分布能够较均匀地覆盖目标区域, 若样本仅集中在满足稀有属性的小部分路径上, 这将会严重低估真实概率.

针对上述问题, 本文通过连续时间马尔可夫链(continuous time Markov chain, CTMC)来表示 SHS 路径概率空间, 使用交叉熵迭代学习方法在 SHS 路径空间的参数化分布族中获得一个近似最优的重要性采样分布, 从而给出稀有属性高效的采样方法, 以解决基于 SMC 的 SHS 稀有属性验证问题. 主要贡献包括以下 3 个方面.

(1) 通过定义在 SHS 状态空间上的 CTMC 表示 SHS 的执行语义, 给出了 SHS 执行路径的概率空间表示, 推导出 SHS 路径空间的参数化分布函数族. 在此基础上构建了 SHS 路径空间上的交叉熵优化模型;

(2) 针对 SHS 路径空间上的交叉熵优化模型, 提出了模型求解方法并给出了迭代学习算法. 算法采样 SHS 路径样本, 在参数化分布族中学习一个最优重要性采样分布. 基于最优重要性采样分布, 给出了安全属性验证的 SMC 算法;

(3) 通过对可修构件系统和汽车燃油容错控制系统上的安全属性验证, 证实了本文方法的有效性. 对于稀有属性验证, 在相同样本数量下, 与状态无关重要性采样方法相比, 本文方法的估计值更好地分布在均值附近, 标准方差和相对误差减少超过一个数量级.

本文第 1 节介绍 SMC 以及稀有属性验证研究的相关进展. 第 2 节给出 SHS 路径概率空间的相关定义以

及该空间上的参数化分布函数族的表示. 第 3 节构造 SHS 路径空间上的交叉熵模型. 第 4 节给出交叉熵模型迭代学习算法和安全性验证算法. 第 5 节对本文提出的方法进行实验论证和比较. 第 6 节总结全文并提及未来的工作.

1 相关工作

SMC 可简单地描述如下: 给定系统模型$\mathcal{M}$以及一个有界线性时序逻辑(bounded linear temporal logic, BLTL)[11]描述的系统属性φ, 使用蒙特卡洛采样、模型检测和统计分析技术定性或定量验证以下两个问题[19,20].

- $\mathcal{M}$满足属性φ的概率是否大于等于阈值θ, $\mathcal{M}\vDash \Pr_{\geqslant\theta}(\varphi)$;
- $\mathcal{M}$满足属性φ的概率 $\Pr(\mathcal{M}\vDash\varphi)$.

在 SMC 中, 对$\mathcal{M}$模拟运行获得一个随机执行路径σ, 然后通过 BLTL 模型检测器判别σ是否满足属性φ, 通过多次模拟获取一定数量的样本, 使用统计方法对样本进行统计分析, 评估系统满足属性的概率, 并给出置信区间或估计的误差界限. 令 $I(\sigma)$表示 BLTL 模型检测器的输出结果, 如果$\sigma\vDash\varphi$, 则 $I(\sigma)=1$; 否则为 0. $I(\sigma)$是一个贝努利随机变量, 因此, $\mathcal{M}$的行为可由参数为 p 的贝努利分布来建模, $\Pr(I(\sigma)=1)=p$, $\Pr(I(\sigma)=0)=1-p$, 参数 p 表示模型$\mathcal{M}$满足 BLTL 属性φ的概率. 由贝努利分布可知, $p=E[I(\sigma)]$, $Var[I(\sigma)]=p(1-p)$. 由于 p 值是未知的, 因此, SMC 的目标是估计 p 的值.

SMC 可分为假设检验和参数估计两类: 假设检验用于判定系统满足时序逻辑属性的概率是否大于等于给定阈值, 属于定性的结果; 参数估计给出系统满足时序逻辑属性的近似概率, 属于定量的结果. SMC 定性算法包括单次抽样方案(single sampling plan, SSP)算法[20]、序贯概率比检验(sequential probability ratio test, SPRT)算法[20]和贝叶斯的假设检验(Bayesian hypothesis testing, BHT)算法[11], SMC 定量算法主要包括近似概率模型检测(approximate probabilistic model checking, APMC)[21]算法和贝叶斯区间估计(Bayesian interval estimation testing, BIET)算法[11]. Kim 对 SSP、SPRT、BHT 和 BIET 这 4 种算法的性能及应用性进行了详细的实验比较[19].

目前, SMC 稀有属性验证的主要方法有重要性采样方法、重要性分割(importance splitting)方法以及统计学习的方法.

- 重要性采样是解决稀有属性验证的有效方法. 针对 CTMC 和 DTMC 随机模型, Reijsbergen[15]和 Barbot[16]分别通过启发式方法获得一个重要性采样分布来完成该两类模型的属性验证. 针对 Stateflow/Simulink 模型, Clarke[9]提出交叉熵最小化重要性采样的 SMC 方法, 验证了该类系统的安全属性; Zuliani[17]使用文献[9]中的 SMC 方法对一类离散时间 SHS 的安全属性进行了验证; Clarke 和 Zuliani 提出的方法都假设系统路径空间的分布呈指数分布, 通过简单地增大系统参数的失效率, 一次性抽取若干条满足稀有属性的路径来计算指数分布的最优参数, 从而获取一个重要性采样分布; Jegourel[18]使用随机卫式命令规约系统的随机模型, 该模型可以通过增加命令的个数(参数个数)来近似系统的路径分布, 使用交叉熵最小化方法在随机模型中获得一个重要性采样分布. 然而, 上述方法获得的最优重要性采样分布不是来自系统路径空间的分布族, 实质是一种启发式重要性采样方法;
- 重要性分割方法[22]也是一种降低估计方差的方法. Jegourel[23]基于重要性分割方法提出了面向小概率事件验证的 SMC 算法. 基本思想是: 将系统逻辑属性分解为嵌套属性, 使其概率更容易估计, 减少了验证所需的样本路径的数量. 为了提高性能, 需要将属性分解为许多不同概率级别, 在分解过程中, 复制或消除路径取决于它们的中间行为, 当分解结束时, 给出属性被满足的概率估计值. 重要性分割方法本质上是启发式, 依赖于模型, 缺少理论结果支撑;
- 将统计学习方法应用于 SMC 也是一个重要的研究方向. 杜[24]提出一种基于支持向量机二分类器的学习型 SMC 框架, 使用代价敏感和重采样方法来解决支持向量机的非平衡数据学习问题, 实现了在相对较少的样本数量下预测和评估小概率事件发生的概率. 但该方法没有给出如何获取稀有属性样本. Kumar[25]针对多失效区域的硬件电路小概率属性验证, 假设系统失效分布为高斯混合模型, 使用变分贝叶斯方法, 从高斯混合模型中学习一个最优重要性采样分布, 但该最优重要性采样分布也不是

来自系统路径空间的分布族. Kalajdzic[26]提出一种基于反馈控制原理的 SMC 方法, 该方法学习一个信息物理融合系统的模型, 使用重要性采样来估计系统状态以及重要性分割来控制系统, 从而可以推断出系统满足给定属性的概率.

本文提出的方法从 SHS 路径概率空间出发构建交叉熵优化模型, 使用迭代学习方法从路径空间的参数化分布簇中获得一个最优重要性采样分布, 保证了最优重要性采样分布来自于 SHS 路径概率空间上的分布族, 迭代学习方法保证该分布较均匀地覆盖不安全路径分布区域. 因此, 稀有属性验证的精度和效率得到显著的提升.

2 SHS 路径概率空间

定义 1. 随机混成系统[1]SHS 是一个元组 $SHS=(L,X,E,Init,Inv,D,G,R)$, 其中,

- L 是系统中离散状态的有限集合(控制模式);
- $X\subseteq\mathbb{R}^n$ 是系统中连续变量状态空间;
- $E\subset L\times L$ 是系统中离散变迁的集合;
- $Init:L\times X\to[0,1]$是定义在 $L\times X$ 上的概率测度, 表示初始状态概率分布;
- $Inv:L\to 2^X$ 表示从离散状态集 L 到连续状态空间的映射, 对于任意一个 $l\in L$, 称 $Inv(l)$是 l 的不变式集;
- $D:L\to(X\to X)$是一个向量域映射, 该映射为每一个控制模式 $l\in L$ 赋予一组随机微分方程(stochastic differential equation, SDE), 用来描述对应不同控制模式 l 的连续随机动态行为, $\mathrm{d}x(t)=f(l,x(t))\mathrm{d}t+g(l,x(t))\mathrm{d}B_t$. 其中, B_t 是一个定义在实数域上的标准的维纳(Wiener)过程, 假设对于所有 $l\in L$, $f(l,\cdot)$和 $g(l,\cdot)$是有界的并且是 Lipschitz 连续的;
- $G:E\to 2^X$ 为每个离散变迁分配一个卫式条件, 满足下列条件: ① 对于每一个 $e=(l,l')\in E$, $G(\mathrm{e})$表示 $\partial Inv(l)$上的可测子集; ② 对于每一个 $l\in L$, $\{G(e):e=(l,l')\in E,l'\in L\}$是$\partial Inv(l)$的不相交的子集;
- $R:E\times X\to\mathcal{P}(X)$是一个重置映射, $\mathcal{P}(X)$是定义在 X 上的概率测度集合, 连续变量根据概率分布被重置.

根据定义, SHS 混成状态空间为 $L\times X$, 令$(l,x)\in L\times X$ 表示混成状态. SHS 的连续动态性是根据当前控制模式上的 SDE 进行演变, 离散动态性是指当连续变量达到不变式的边界时, 根据离散变迁上的卫式条件, 从一个控制模式迁移到另一个控制模式.

令 $x_l(t)$是初始状态为 $x_l(0)$的 SDE 解, $\tau(l)=\inf\{t\in\mathbb{R}_{>0},x_l(t)\notin Inv(l)\}$表示在控制模式 l 中, 连续变量的演变首次违背不变式的时间, 也就是首次退出控制模式 l 的时间. 下面给出描述 SHS 执行语义的随机过程定义.

定义 2(SHS 执行语义). 一个在 SHS 状态空间上的随机过程$(l(t),x(t))\in L\times X$ 被称为 SHS 的随机执行, 如果存在一个停时序列 $T_0=0<T_1<T_2<\ldots$, 使得对于每一个 $k\in\mathbb{N}$:

- $(l_0,x_0)\in L\times X$, 表示 SHS 的初始状态;
- $t\in[T_k,T_{k+1})$, $l(t)=l(T_k)$是一个常量, $x(t)$是 $\mathrm{d}x(t)=f(l(T_k),x(t))\mathrm{d}t+g(l(T_k),x(t))\mathrm{d}B_t$ 的一个连续的解;
- $T_{k+1}=T_k+\tau(l(T_k))$;
- $x(T_{k+1})$的概率分布由重置映射 $R(e_k,x(T_{k+1}^-))$ 确定, 其中, $e_k=(l(T_k),l(T_{k+1}))\in E$, $x(T_{k+1}^-)=\lim\limits_{t\to T_{k+1}}x(t)$.

定义 3(SHS 路径). SHS 的一条执行路径是从初始状态(l_0,x_0)开始的一个无限序列$\sigma=((l_0,x_0),t_0),((l_1,x_1),t_1),\ldots$, 其中, $(l_i,x_i)\in L\times X$表示 SHS 状态, $t_i\in\mathbb{R}_{\geqslant 0}$表示在状态$(l_i,x_i)$的停留时间, $Pref(\sigma)$表示σ所有前缀集合, $Paths^{\omega}$表示系统的所有无限路径集合, $Paths^{*}$表示系统的所有有限路径集合.

SMC 不关注 SHS 的结构, 只需采样 SHS 的执行路径, 避免了 SHS 的动态演化的复杂性. SHS 随时间演变的行为可由系统的路径来表征. 根据 SHS 的执行语义, SHS 的执行路径产生过程如下: 在当前离散模式 l_i 内, 连续变量 x_i 按照 l_i 的 SDE 进行演变, 当 x_i 演变满足卫式条件, 即 $x_i(t)\in G(l_i,l_{i+1})$时, 迁移到下一个控制模式 l_{i+1}, x_{i+1} 的初始值由随机重置核 R 给定. l_i 停留时间 $t_i=\inf\{t\in\mathbb{R}_{>0},x_i(t)\notin Inv(l_i)\}$, t_i 是一个随机变量, 其值取决于 l_i 的 SDE、初始值 $x_i(0)$和 $Inv(l_i)$. 依此类推, 从 SHS 执行路径的生成过程可知, SHS 的下一个状态取决于当前状态

和当前状态停留时间. 因此, SHS 的执行路径可以看作是由定义在混成状态空间上的连续时间马尔可夫过程所产生. 由于停留在l_i时间越长, 从l_i迁移的概率越大, 可进一步假设在l_i停留时间服从指数分布. 那么, 连续时间马尔可夫过程变成 CTMC.

令G_l表示从l出发所有边的卫式条件集合, $G_l=\{G(e):e=(l,l')\in E,l'\in L\}$, 其中, $G(e)\in\partial Inv(l)$, $G(e_i)\cap G(e_j)=\varnothing$, $i\neq j$, l中连续变量演变到满足各卫式条件的时间分别为$\tau_1,\tau_2,...,\tau_{|G_l|}$, 则在$l$中的停留时间$t_l=\min\{\tau_1,\tau_2,...,\tau_{|G_l|}\}$. 假设$\tau_1,\tau_2,...,\tau_{|G_l|}$分别服从参数为$\{\lambda_{ll'},l'\in L,(l,l')\in E\}$的指数分布, 则在$l$中的停留时间$t_l$服从参数为$\sum_{l'\in L,(l,l')\in E}\lambda_{ll'}$的指数分布. 在上述假设下, SHS 的执行路径可由 CTMC 随机过程生成.

定义 4(SHS 路径生成模型). SHS 状态空间上的路径生成模型是一个$CTMC=(S,\iota_{init},\boldsymbol{\lambda},\boldsymbol{P})$, 其中,

- $S=\{(l,x(0))|l\in L,x(0)\in X\wedge x(0)\in Inv(l)\}$, $x(0)$表示控制模式l中的连续变量的初始值, 并且对于任意两个状态(l,x')、(l,x''), 如果$x,x''\in Inv(l)$, 则(l,x')、(l,x'')属于同一个离散混成状态$(l,x(0))$;
- $\iota_{init}:S\to[0,1]$表示初始状态的概率分布且$\sum_{s\in S}s=1$;
- $\lambda:S\times S\to\mathbb{R}_{\geqslant 0}$是迁移速率函数, 所有迁移速率函数值构成迁移速率矩阵, 记作$\boldsymbol{\lambda}$;
- $\boldsymbol{P}:S\times S\to[0,1]$是迁移概率矩阵.

对于所有的$s,s'\in S$, $\boldsymbol{P}(s,s')=\begin{cases}\dfrac{\lambda_{ss'}}{\lambda_s}, & s\neq s'\\ 1, & s=s'\end{cases}$, 其中, $\lambda_s=\sum_{s'\in S}\lambda_{ss'}$. 由定义 4 可知: 已知 CTMC 结构, 其行为由迁移速率矩阵$\boldsymbol{\lambda}$控制, $\boldsymbol{\lambda}$值来自于 SHS. 对于简单的 SDE, 可以获得$\boldsymbol{\lambda}$解析解(参见第 3.3 节); 对于复杂的 SDE, 通过对每个离散控制模式的模拟运行, 采样该控制模式迁移到下一个控制模式的时间, 使用最大似然估计获得$\boldsymbol{\lambda}$的估计值. 下面给出 SHS 路径生成模型的柱集[27]和路径概率空间[28]的定义.

定义 5(柱集). 柱集是有限路径$\hat{\sigma}=(s_0,t_0),...,(s_{k-1},t_{k-1}),(s_k,t_k)\in Path^*$扩展成的所有无限路径的集合, 表示为$Cyl(\hat{\sigma})=\{\sigma\in Paths^{\omega}\mid\hat{\sigma}\in Pref(\sigma)\}$.

定义 6(路径概率空间). 路径概率空间是一个元组$(Paths^{\omega}(s_0),\mathcal{F},\Pr)$, 其中, $\mathcal{F}=\{Cyl(\hat{\sigma})\mid\hat{\sigma}\in Paths^*\}$是包含所有有限路径张成的柱集的最小$\Sigma$代数, $I_0,I_1,\ldots,I_{k-1}$是非负实数集上非空的区间序列. Pr 是在$\mathcal{F}$上的唯一概率测度, 可归纳定义如下:

$$\left.\begin{aligned}&\Pr(Cyl(s_0))=\iota_{init}(s_0)\\&\Pr(Cyl(s_0,I_0,s_1,...,I_{k-1},s_k))=\Pr(Cyl(s_0,I_0,s_1,...,I_{k-2},s_{k-1}))\boldsymbol{P}(s_{k-1},s_k)(\mathrm{e}^{-\lambda_{s_{k-1}}a}-\mathrm{e}^{-\lambda_{s_{k-1}}b})\\&\text{其中, }k>0,\ a=\inf I_{k-1},\ b=\sup I_k\end{aligned}\right\}\tag{1}$$

SMC 主要考虑在有界时间$[0,T]$内的系统执行路径, 从系统初始状态(s_0,t_0)出发, $[0,T]$时间内的系统执行路径$\sigma=(s_0,t_0),\ldots,(s_{k-1},t_{k-1}),(s_k,t_k)$, 其中, $t_j\geqslant 0$, $\sum_{j=0}^{k-1}t_j<T$, $t_k=T-\sum_{j=0}^{k-1}t_j$, $k>0$表示在$[0,T]$时间内系统发生状态转换的次数, k是一个随机变量, 其值随σ不同而变化. 根据定义 6, 引理 1 给出了 SHS 路径空间上的参数化分布函数族.

引理 1. 令$\boldsymbol{\Theta}$表示系统的参数空间, $f(\sigma,\boldsymbol{\lambda})$表示通过参数$(\boldsymbol{\lambda}\in\boldsymbol{\Theta})$区分不同概率测度的一个参数化分布函数族. 在$[0,T]$时间内, SHS 执行路径$\sigma=(s_0,t_0),\ldots,(s_{k-1},t_{k-1}),(s_k,t_k)$参数化分布函数族:

$$f(\sigma,\boldsymbol{\lambda})=\iota_{init}(s_0)\prod_{l,m\in S}(\lambda_{lm})^{c_{lm}}\prod_{l\in S}\mathrm{e}^{-\lambda_l\tau_l}\tag{2}$$

其中, c_{lm}表示在σ中从状态l到状态m的转换次数, τ_l表示在σ中状态l的持续时间之和, $\lambda_l=\sum_{m\in S}\lambda_{lm}$.

证明: 将递归定义的概率测度公式(1)应用到有限路径, 并在各自的时间区间内对停留时间求导可以递推构造公式(2).

- 在$[0,T]$时间内只观测到状态s_0, $\sigma=(s_0,t_0)$, $t_0=T$, 则$f(\sigma,\boldsymbol{\lambda})=\iota_{init}(s_0)\mathrm{e}^{-\lambda_{s_0}T}$;

- 在[0,T]时间内观测序列σ=(s_0,t_0),(s_1,t_1), t_1=T−t_0, 则 $f(\sigma,\boldsymbol{\lambda})=\iota_{init}(s_0)\lambda_{s_0s_1}\mathrm{e}^{-\lambda_{s_0}t_0}\mathrm{e}^{-\lambda_{s_1}(T-t_0)}$;
- 在[0,T]时间内观测序列 $\sigma=(s_0,t_0),...,(s_{k-1},t_{k-1}),(s_k,t_k)$, $t_k=T-\sum_{j=0}^{k-1}t_j$, 则:

$$f(\sigma,\boldsymbol{\lambda})=\iota_{init}(s_0)\prod_{j=0}^{k-1}\lambda_{s_js_{j+1}}\mathrm{e}^{-\lambda_{s_j}t_j}\mathrm{e}^{-\lambda_{s_k}(T-t_j)} \tag{3}$$

由于在[0,T]时间内系统发生状态转换的次数 k 是一个随机变量, 其值随σ不同而变化, 因此, 令 c_{lm} 表示在σ中从状态 l 到状态 m 的转换次数, τ_l 表示在σ中状态 l 的持续时间之和, 则由公式(3)得到公式(2). □

3 SHS 路径空间的交叉熵模型

3.1 最优重要性采样分布

最优重要性采样分布是使得估计方差最小的重要性采样分布. 假设在 SHS 的路径概率空间中, 路径σ真实的概率分布为 $f(\sigma)$, 重要性采样概率分布为 $g(\sigma)$, $g(\sigma)$能以较大的概率采样到满足稀有属性的样本. 在稀有属性验证情况下, 难以直接从 $f(\sigma)$中采样到满足稀有属性的样本, 重要性采样方法从 $g(\sigma)$中采样. 根据 SMC 和重要性采样原理, SHS 满足稀有属性的概率 p=E_f[$I(\sigma)$]可重写如下:

$$p=E_f[(I(\sigma)]=\int I(\sigma)f(\sigma)\mathrm{d}\sigma=\int I(\sigma)\frac{f(\sigma)}{g(\sigma)}g(\sigma)\mathrm{d}\sigma=\int I(\sigma)W(\sigma)f(\sigma)\mathrm{d}\sigma=E_g[(I(\sigma)W(\sigma)] \tag{4}$$

其中, 似然比 $W(\sigma)=\dfrac{f(\sigma)}{g(\sigma)}$. 重要性采样方法从 $g(\sigma)$中采样, 然后利用似然比进行加权修正, 保证 p 的估计值是无偏的. 从重要性概率分布 $g(\sigma)$中随机采样 N 个独立的执行路径$\sigma_1,\sigma_2,\ldots,\sigma_N$, 可得 p 的无偏估计和估计的方差分别由公式(5)和公式(6)表示:

$$\hat{p}=\frac{1}{N}\sum_{i=1}^{N}I(\sigma_i)W(\sigma_i) \tag{5}$$

$$Var_g[\hat{p}]=\frac{1}{N}(E_g[(I^2(\sigma)W^2(\sigma)]-p^2) \tag{6}$$

重要性采样的关键问题是: 寻找一个最优重要性采样分布, 使得估计方差达到最小. 令公式(6)等于 0 并解出 $g(\sigma)$, 得到零方差的最优重要性采样分布:

$$g^*(\sigma)=I(\sigma)\frac{f(\sigma)}{p} \tag{7}$$

但 $g^*(\sigma)$依赖于真实值 p, 而 p 的值是未知的, 因此无法从 $g^*(\sigma)$中进行采样. 最优重要性采样分布理论上是存在的, 但在实践中找到最优重要性采样分布是非常困难的. 本文采用交叉熵迭代学习方法从 SHS 路径空间的参数化分布族中寻找一个最接近 $g^*(\sigma)$的重要性采样分布, 通过从近似最优的重要性概率分布进行采样, 以达到减小估计误差和加速 SMC 算法收敛的目的.

3.2 交叉熵优化模型

本节通过最小化两个概率分布之间的交叉熵, 从而找到最优重要性采样分布. 根据交叉熵[29,30]的定义, 定义 7 给出了 SHS 路径空间上的交叉熵的定义.

定义 7(交叉熵). SHS 路径空间Ω上的两个概率分布 $p(\sigma)$和 $q(\sigma)$之间的交叉熵:

$$\mathcal{D}(p(\sigma),q(\sigma))=\int_{\Omega}p(\sigma)\ln\frac{p(\sigma)}{q(\sigma)}\mathrm{d}\sigma \tag{8}$$

交叉熵用来评估两个概率分布的相似程度, 交叉熵的值越小, 表示 $p(\sigma)$和 $q(\sigma)$越相似, $\mathcal{D}(p(\sigma),q(\sigma))$=0 当且仅当 $p(\sigma)$=$q(\sigma)$.

根据定义 7, 下面给出在 SHS 路径空间上的交叉熵优化模型的构造. 假设 SHS 路径σ的真实分布 $f(\sigma,\boldsymbol{u})$, $\boldsymbol{u}\in\boldsymbol{\Theta}$来自于参数化分布族$\{f(\sigma,\boldsymbol{\Theta})\}$中的一个分布, 交叉熵优化方法是在参数化分布族中选择一个分布 $f(\sigma,\boldsymbol{\lambda})$,

$\boldsymbol{\lambda}\in\Theta$与最优分布 $g^*(\sigma)$交叉熵最小. 该优化问题可描述为

$$\min_{\boldsymbol{\lambda}} \mathcal{D}(g^*(\sigma), f(\sigma,\boldsymbol{\lambda})) = \min_{\boldsymbol{\lambda}} \int_\Omega g^*(\sigma)\ln\frac{g^*(\sigma)}{f(\sigma,\boldsymbol{\lambda})}\mathrm{d}\sigma = \min_{\boldsymbol{\lambda}} \int_\Omega g^*(\sigma)\ln g^*(\sigma)\mathrm{d}\sigma - \int_\Omega g^*(\sigma)\ln f(\sigma,\boldsymbol{\lambda})\mathrm{d}\sigma \tag{9}$$

公式(9)第 1 项与$\boldsymbol{\lambda}$无关, 交叉熵最小化等价于第 2 项最大化. 因此, 公式(9)的最小化问题等价于公式(10)的最大化问题:

$$\begin{aligned}\min_{\boldsymbol{\lambda}} \mathcal{D}(g^*(\sigma), f(\sigma,\boldsymbol{\lambda})) &= \max_{\boldsymbol{\lambda}} \int_\Omega g^*(\sigma)\ln f(\sigma,\boldsymbol{\lambda})\mathrm{d}\sigma \\ &= \max_{\boldsymbol{\lambda}} \int_\Omega I(\sigma) f(\sigma,\boldsymbol{u})\ln f(\sigma,\boldsymbol{\lambda})\mathrm{d}\sigma \\ &= \max_{\boldsymbol{\lambda}} E_u[I(\sigma)\ln f(\sigma,\boldsymbol{\lambda})]\end{aligned} \tag{10}$$

求解公式(10)的优化问题, 需要从真实分布 $f(\sigma,\boldsymbol{u})$中进行采样. 然而在稀有属性情况下, 从 $f(\sigma,\boldsymbol{u})$采样时, $I(\sigma)$的值几乎都等于 0, 因此很难从 $f(\sigma,\boldsymbol{u})$采样到满足稀有属性的路径. 通过再次使用重要性采样方法从分布$f(\sigma,\boldsymbol{w})$进行采样, 参数 $\boldsymbol{w}$ 的选择要能够增大满足稀有属性路径出现的概率, 也就是增大 $I(\sigma)$=1 的概率. 因此, 公式(10)优化问题可重新表述为

$$\begin{aligned}\max_{\boldsymbol{\lambda}} \int_\Omega I(\sigma) f(\sigma,\boldsymbol{u})\ln f(\sigma,\boldsymbol{\lambda})\mathrm{d}\sigma &= \max_{\boldsymbol{\lambda}} \int_\Omega I(\sigma)\frac{f(\sigma,\boldsymbol{u})}{f(\sigma,w)} f(\sigma,\boldsymbol{w})\ln f(\sigma,\boldsymbol{\lambda})\mathrm{d}\sigma \\ &= \max_{\boldsymbol{\lambda}} \int_\Omega I(\sigma)W(\sigma,\boldsymbol{u},\boldsymbol{w}) f(\sigma,\boldsymbol{w})\ln f(\sigma,\boldsymbol{\lambda})\mathrm{d}\sigma \\ &= \max_{\boldsymbol{\lambda}} E_w[I(\sigma)W(\sigma,\boldsymbol{u},\boldsymbol{w})\ln f(\sigma,\boldsymbol{\lambda})]\end{aligned} \tag{11}$$

其中, 似然比函数 $W(\sigma,\boldsymbol{u},\boldsymbol{w}) = \dfrac{f(\sigma,\boldsymbol{u})}{f(\sigma,\boldsymbol{w})}$. 公式(11)优化问题的最优解$\boldsymbol{\lambda}^*$可以通过路径样本来估计, 将样本均值代替期望, 可得到交叉熵优化模型:

$$\boldsymbol{\lambda}^* = \arg\max_{\boldsymbol{\lambda}} \frac{1}{N}\sum_{i=1}^{N} I(\sigma_i)W(\sigma_i,\boldsymbol{u},\boldsymbol{w})\ln f(\sigma_i,\boldsymbol{\lambda}) \tag{12}$$

其中, $\sigma_1,\sigma_2,\ldots,\sigma_N$ 是来自于分布 $f(\sigma,\boldsymbol{w})$的样本.

3.3 一个简单的示例

本节通过一个简单的车距保持系统[1]来说明本文方法是如何工作的. 两辆车 Car1 和 Car2 在高速公路上从左向右移动, Car2 行驶在 Car1 前面, 如图 1 所示. 由于车辆在行驶的过程中受路况、风速和人的操纵等随机因素的影响, 两辆车的运动都具有随机性. 为了便于分析, 将所有的随机性都放到 Car1 的运动中, 同时不考虑可能发生的紧急制动, 那么 Car2 的运动建模为恒定速度 v_2; Car1 的运动由图 2 所示的 SHS 表示, 该 SHS 由追逐、保持和制动这 3 个控制模式组成, 分别用 s_0、s_1、s_2 表示, s_0 为初始状态. 图 2 中的Δx 为两辆车之间的距离, $d_0>d_1>d_2>d_3>0$ 是 4 个阈值.

在 s_0 状态, $\Delta x>d_2$, Car1 以速度 $v_1(v_1>v_2)$试图追上 Car2. 由于受随机扰动的影响, Car1 的运动由 $\mathrm{d}x_1(t)=v_1\mathrm{d}t+\mathrm{d}B_t$ 控制. 在 s_1 状态, $d_3<\Delta x<d_1$, Car1 试图以速度 $v2$ 运动, 但在随机扰动下, Car1 的运动由 $\mathrm{d}x_1(t)=v_2\mathrm{d}t+\mathrm{d}B_t$ 控制. 在 s_2 状态, $\Delta x<d_3$, Car1 将按照规定的程序进行制动, Car1 的运动由 $\mathrm{d}^2x_1(t)=-a_1\mathrm{d}t^2$ 控制, 这里忽略了制动过程中的噪音.

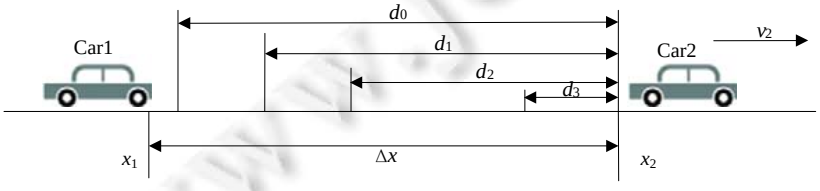

图 1 车辆距离保持系统

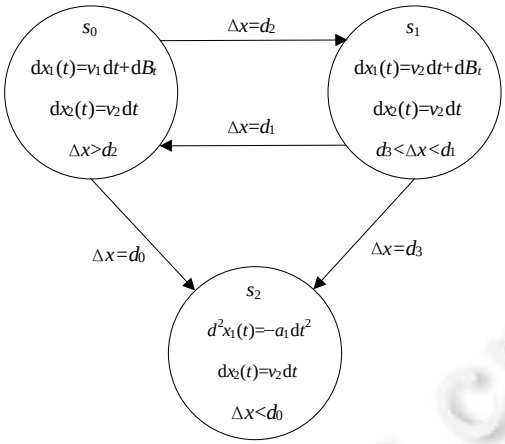

图 2　车距保持系统的随机混成系统

由于本例的 SDE 比较简单, 因此根据每个控制模式的 SDE、不变式集以及每条边的卫式条件, 可以计算出对应的 CTMC 的迁移概率矩阵 $\boldsymbol{P}$ 以及每个控制模式的期望停留时间 $E[T]$:

$$\boldsymbol{P}=\begin{pmatrix}0 & 1 & 0\\ \dfrac{d_2-d_3}{d_1-d_3} & 0 & \dfrac{d_1-d_2}{d_1-d_3}\\ 1 & 0 & 0\end{pmatrix},\ E[T]=\begin{pmatrix}\dfrac{d_0-d_2}{v_1-v_2}\\ \dfrac{d_1-d_2}{d_2-d_3}\\ \sqrt{\dfrac{2(d_0-d_3)}{a_1}}\end{pmatrix}.$$

根据迁移概率矩阵 $\boldsymbol{P}$ 以及期望停留时间 $E[T]$, 计算出迁移率矩阵:

$$\boldsymbol{\lambda}=\begin{pmatrix}0 & \dfrac{v_1-v_2}{d_0-d_2} & 0\\ \dfrac{(d_2-d_3)^2}{(d_1-d_3)(d_1-d_2)} & 0 & \dfrac{d_2-d_3}{d_1-d_3}\\ \sqrt{\dfrac{a_1}{2(d_0-d_3)}} & 0 & 0\end{pmatrix}.$$

假设在[0,10s]内, 针对该 SHS 采样一条执行路径σ=(s_0,2),(s_1,3),(s_0,1),(s_1,2),(s_2,2),(s_0). 根据引理 1, $f(\sigma,\boldsymbol{\lambda})=(\sigma,\boldsymbol{\lambda})=\lambda_{01}^2e^{-3\lambda_0}\lambda_{10}e^{-3\lambda_1}\lambda_{12}e^{-2\lambda_1}\lambda_{20}e^{-2\lambda_2}$, 将迁移率矩阵$\boldsymbol{\lambda}$中的相关分量带入, 即可计算出 $f(\sigma,\boldsymbol{\lambda})$的值.

接下来解释公式(12)中各参数和函数的物理意义. 参数 $\boldsymbol{u}$ 是 CTMC 真实的迁移率矩阵, 参数 $\boldsymbol{w}$ 是初始参数, $\boldsymbol{w}$ 的选择要能够增大满足稀有属性路径出现的概率, 因此, 参数 $\boldsymbol{u}$ 和 $\boldsymbol{w}$ 是已知的, 即公式(12)中路径样本的似然比 $W(\sigma,\boldsymbol{u},\boldsymbol{w})=\dfrac{f(\sigma,\boldsymbol{u})}{f(\sigma,\boldsymbol{w})}$ 是可计算的. $I(\sigma_i)$表示 BLTL 模型检测器的输出, 如果$\sigma_i\vDash\varphi$, 则为 1; 否则为 0. $f(\sigma_i,\boldsymbol{\lambda})$是待优化的函数, 其中, $\boldsymbol{\lambda}$是优化变量.

4　安全性验证算法

根据引理 1 的参数化分布函数族 $f(\sigma,\boldsymbol{\lambda})$, 定理 1 给出了交叉熵优化模型(12)的优化解.

定理 1. 公式(12)交叉熵优化模型的最优解:

$$\lambda_{lm}=\frac{\sum_{i=1}^{N}I(\sigma_i)W(\sigma_i,\boldsymbol{u},\boldsymbol{w})c_{lm}^{(i)}}{\sum_{i=1}^{N}I(\sigma_i)W(\sigma_i,\boldsymbol{u},\boldsymbol{w})\tau_l^{(i)}} \tag{13}$$

其中, σ_i ($1\leqslant i\leqslant N$)是来自于分布 $f(\cdot,\boldsymbol{w})$的样本路径, $f(\sigma_i,\boldsymbol{u})$表示 SHS 路径真实概率分布, 似然比:

$$W(\sigma_i,\boldsymbol{u},\boldsymbol{w})=\prod_{l,m\in S}\left(\frac{u_{lm}}{w_{lm}}\right)^{c_{lm}^{(i)}}\prod_{l\in S}\mathrm{e}^{(w_l-u_l)\tau_l^{(i)}}.$$

证明: 由公式(2)和公式(12)可得:

$$\max_{\boldsymbol{\lambda}}\frac{1}{N}\sum_{i=1}^{N}I(\sigma_i)W(\sigma_i,\boldsymbol{u},\boldsymbol{w})\ln f(\sigma_i,\boldsymbol{\lambda})=\max_{\boldsymbol{\lambda}}\frac{1}{N}\sum_{i=1}^{N}I(\sigma_i)W(\sigma_i,\boldsymbol{u},\boldsymbol{w})\left(\ln\iota_{init}(s_0)+\sum_{l,m\in S}c_{lm}^{(i)}\ln\lambda_{lm}+\sum_{l\in S}-\lambda_l\tau_l^{(i)}\right).$$

$\ln f(\sigma_i,\boldsymbol{\lambda})$是凸函数且对$\boldsymbol{\lambda}$可微, 将上式对$\lambda_{lm}$求偏导并令其等于 0 可得:

$$\sum_{i=1}^{N}I(\sigma_i)W(\sigma_i,\boldsymbol{u},\boldsymbol{w})\left(\frac{c_{lm}^{(i)}}{\lambda_{lm}}-\tau_l^{(i)}\right)=0\Rightarrow\frac{1}{\lambda_{lm}}\sum_{i=1}^{N}I(\sigma_i)W(\sigma_i,\boldsymbol{u},\boldsymbol{w})c_{lm}^{(i)}=\sum_{i=1}^{N}I(\sigma_i)W(\sigma_i,\boldsymbol{u},\boldsymbol{w})\tau_l^{(i)}$$

$$\Rightarrow\lambda_{lm}=\frac{\sum_{i=1}^{N}I(\sigma_i)W(\sigma_i,\boldsymbol{u},\boldsymbol{w})c_{lm}^{(i)}}{\sum_{i=1}^{N}I(\sigma_i)W(\sigma_i,\boldsymbol{u},\boldsymbol{w})\tau_l^{(i)}}.$$

由公式(13)可知, 最优解的估计值依赖初始分布 $f(\sigma,\boldsymbol{w})$. 然而一般情况下, $f(\sigma,\boldsymbol{w})$分布是远离最优分布的, 即使该分布产生 100%满足稀有属性的路径样本, 但样本仅集中在满足稀有属性的小部分路径上. 这种分布将具有较低的样本方差, 给人以高信度的错误印象, 会严重低估真实概率.

为了降低初始分布 $f(\sigma,\boldsymbol{w})$对所求的最优重要性采样分布参数的影响, 本文使用平滑策略在路径空间中迭代学习求解. 通过迭代, 算法能够探索更广的路径空间, 从而可以获得更好的近似最优解. 令初始分布参数$\boldsymbol{w}=\boldsymbol{\lambda}^{(0)}$, 由公式(13)得到公式(14)的迭代公式:

$$\lambda_{lm}^{(n+1)}=\frac{\sum_{i=1}^{N}I(\sigma_i)W(\sigma_i,\boldsymbol{u},\boldsymbol{\lambda}^{(n)})c_{lm}^{(i)}}{\sum_{i=1}^{N}I(\sigma_i)W(\sigma_i,\boldsymbol{u},\boldsymbol{\lambda}^{(n)})\tau_l^{(i)}} \tag{14}$$

其中, N 为每次迭代的样本数, $W(\sigma_i,\boldsymbol{u},\boldsymbol{\lambda}^{(n)})=\frac{f(\sigma_i,\boldsymbol{u})}{f(\sigma_i,\boldsymbol{\lambda}^{(n)})}$表示第 n 次迭代中样本σ_i的似然比, σ_i是从分布 $f(\sigma,\boldsymbol{\lambda}^{(n)})$中采样的第 i 个样本路径. 在任意一次模拟运行中, 通常只能看到很少部分的状态转换. 在每次迭代过程中, 有些参数在满足稀有属性的路径中不起作用, 公式(14)会将这些参数值设置为 0, 这些参数在所有后续迭代中都不起作用, 这将导致迭代算法过早收敛无法探测更广泛的参数空间. 为了避免这种情况的发生, 采用平滑策略, 将当前迭代值与前一次迭代参数加权进行平滑, 如公式(15)所示:

$$\lambda_{lm}^{(n+1)}=a\lambda_{lm}^{(n)}+(1-a)\frac{\sum_{i=1}^{N}I(\sigma_i)W(\sigma_i,\boldsymbol{u},\boldsymbol{\lambda}^{(n)})c_{lm}^{(i)}}{\sum_{i=1}^{N}I(\sigma_i)W(\sigma_i,\boldsymbol{u},\boldsymbol{\lambda}^{(n)})\tau_l^{(i)}},\ a\in(0,1) \tag{15}$$

平滑策略降低暂时在迭代中不起作用参数的重要性, 而不是将其设置为 0, 从而保留了重要的尚未起作用的参数. 公式(14)和公式(15)共同保证从满足稀有属性的路径集合中较均匀地采样.

综上所述, 算法 1 给出了交叉熵迭代学习(cross entropy iterative learning, CEIL)算法描述. CEIL 算法通过对 SHS 迭代采样, 在其路径空间上的参数化分布族中迭代学习出待验证属性的最优重要性采样分布的参数.

算法 1. 交叉熵迭代学习算法.

输入: 每次迭代样本数 N, SHS 路径分布的真实参数 u, 初始参数$\boldsymbol{\lambda}^{(0)}$, 最大迭代次数 $n_{\max}$;

输出: 最优参数$\boldsymbol{\lambda}^*$.

1: n=0;
2: **repeat**
3: A=0, B=0, i=1;
4: **while** $i \leqslant N$ **do**
5: generate a path σ_i according to the pdf $f(\cdot,\boldsymbol{\lambda}^{(n)})$;
6: **if** $\sigma_i \models \varphi$ **then**
7: $W_i = \prod_{l,m\in S}\left(\frac{u_{lm}}{\lambda_{lm}^{(n)}}\right)^{c_{lm}^{(i)}} \prod_{l\in S} \mathrm{e}^{\left(\lambda_l^{(n)}-u_l\right)\tau_l^{(i)}}$;
8: $A = A + W_i c_{lm}^{(i)}$;
9: $B = B + W_i \tau_l^{(i)}$;
10: **end if**
11: i++;
12: **end while**
13: $\lambda_{lm}^{(n+1)} = a\lambda_{lm}^{(n)} + (1-a)\frac{A}{B}$;
14: $\lambda_{lm}^{(n+1)} = \lambda_{lm}^{(n+1)} \Big/ \sum_{m\in S} \lambda_{lm}^{(n+1)}$;
15: n++;
16: **until** $n \geqslant n_{\max}$;
17: **return** $\boldsymbol{\lambda}^{(n)}$;

初始分布$f(\cdot,\boldsymbol{\lambda}^{(0)})$的选择要能在第 1 次迭代中产生一些满足稀有属性的路径, 即参数$\boldsymbol{\lambda}^{(0)}$的选择要能增大稀有属性出现的概率. 停止迭代条件可以是两次迭代参数向量之间的距离不大于某一常数或限定最大迭代次数. 例如: 给定一个较小ε>0, 若满足$\|\boldsymbol{\lambda}^{(n)}-\boldsymbol{\lambda}^{(n-1)}\| \leqslant \varepsilon$, 则停止迭代. 为便于比较, 在实验中限定最大迭代次数. 由于参数不受约束, 为了便于判断收敛性, 因此在每次迭代后对它们进行标准化(语句 14). 不考虑样本获取时间和 BLTL 模型检测时间, 算法 1 的时间复杂度为 $O(n_{\max}\times|\boldsymbol{\lambda}|\times N)$. 由于优化的目标函数是凸的, 因此存在唯一最优解. 如果算法 1 收敛, 它必然收敛到唯一的最优解附近. 使用最后一次迭代的样本, 通过最优重要性采样分布来估计 SHS 满足稀有属性的概率 $\hat{p}$, 算法 2 描述了稀有属性验证算法的验证过程.

算法 2. 稀有属性验证算法.

输入: 样本数 N_{IS}, SHS 路径分布的真实参数 $\boldsymbol{u}$, 算法 1 计算的最优参数$\boldsymbol{\lambda}^*$;
输出: SHS 满足稀有属性的概率 $\hat{p}$.

1: A=0, i=1;
2: **while** $i \leqslant N_{IS}$ **do**
3: generate a path σ_i according to the pdf $f(\cdot,\boldsymbol{\lambda}^*)$;
4: **if** $\sigma_i \models \varphi$ **then**
5: $W_i = \prod_{l,m\in S}\left(\frac{u_{lm}}{\lambda_{lm}^*}\right)^{c_{lm}^{(i)}} \prod_{l\in S} \mathrm{e}^{(\lambda_l^*-u_l)\tau_l^{(i)}}$;
6: A=A+W_i;
7: **end if**
8: i++;
9: **end while**

10: **return** $\frac{A}{N_{IS}}$;

5 实验及分析

本节通过两组实验来验证 CEIL 方法的有效性.

- 第 1 个案列是可修构件系统(repairable component system, RCS)[18], 采用 CTMC 进行建模, 可通过 PRISM 工具获得精确的计算结果. 实验中, 将 CEIL 方法的估计结果分别与 SMC 主流方法——BIET 方法估计结果以及 PRISM 计算结果进行比较;
- 第 2 个案列是汽车燃油容错控制系统(fault-tolerant fuel control system, FFCS, http://ww2.mathworks.cn/help/simulink/examples/modeling-a-fault-tolerant-fuel-control-system.html?lang=en), FFCS 来自 MATLAB 的 Stateflow/Simulink 混成系统建模案例, 通过故障注入的方式引入随机性, 并在 MATLAB 中仿真获取系统执行路径, 采用 Plasma-Lab[31]工具中的 BLTL 模型检测器实现对路径的检测. 实验中, 通过 CEIL 方法验证 FFCS 稀有属性, 并与启发式重要性采样(heuristic importance sampling, HIS)方法[17]进行比较.

5.1 实验结果有效性度量

在非稀有属性验证情况下, 采用置信区间来评估各类方法估计的精度; 在稀有属性验证情况下, 采用相对误差评估估计的精度:

$$RE(\hat{p})=\frac{\sqrt{Var[\hat{p}]}}{E[\hat{p}]}\approx\sqrt{\frac{1}{Np}} \tag{16}$$

其中, $E[\hat{p}]$用当前估计值 $\hat{p}$ 代替, $Var[\hat{p}]=\frac{1}{N-1}\sum_{i=1}^{N}(I(\sigma_i)W(\sigma_i,\boldsymbol{u},\boldsymbol{\lambda}^*)-\hat{p})^2$.

偏度(skewness)是统计数据分布偏斜方向和程度的度量, 表征概率分布密度曲线相对于平均值不对称程度的特征数. 偏度是样本的三阶标准化矩, 正态分布的偏度为 0, 其估计量均匀分布在均值周围:

$$Skew(\hat{p})=\frac{N\sum_{i=1}^{N}\left(\hat{p}_i-\sum_{j=1}^{N}\hat{p}_j\right)^3}{(N-1)(N-2)(Var[\hat{p}])^{3/2}} \tag{17}$$

5.2 RCS属性验证

RCS 包括 6 种类型的子系统, 每种类型的子系统分别包含(5,4,6,3,7,5)个相同的组件, 每个组件独立失效. 子系统组件故障率分别为($2.5\varepsilon,\varepsilon,5\varepsilon,3\varepsilon,\varepsilon,5\varepsilon$), ε=0.01, 修复率为(1.0,1.5,1.0,2.0,1.0,1.5), 这两组参数对应算法 1 中的路径分布的真实参数 $\boldsymbol{u}$. 系统被建模为 CTMC, 具有 40 320 个状态的中等大的状态空间, 可以使用概率模型检测方法给出精确结果. 待优化的系统参数 λ_i (i=1,…,12)共 12 个, 其中, 奇数下标表示失效率, 偶数下标表示修复率. 系统的初始状态是没有任何组件失效, 当一种类型的组件全部失效时系统失效. 待验证的 RCS 属性是“在没有任何组件失效的初始条件下, 系统在 1 000 s 内失效的概率”. 令 $fail_i$ (i=1,…,6)表示第 i 个子系统组件的失效个数, $init$ 表示系统初始状态没有组件失效, $init=(fail_1=0\wedge fail_2=0\wedge fail_3=0\wedge fail_4=0\wedge fail_5=0\wedge fail_6=0)$, failure 表示系统失效 $failure=(fail_1=5\wedge fail_2=4\wedge fail_3=6\wedge fail_4=3\wedge fail_5=7\wedge fail_6=5)$. 则该属性可用 BLTL 公式描述为

$$\Pr(\bigcirc(\neg init\bigcup^{1000} failure)).$$

在无任何先验信息的情况下, 假设所有状态的初始转换率 λ_i=0.1 (i=1,…,12), 对应算法 1 中的初始参数 $\boldsymbol{\lambda}^{(0)}$. 算法 1 每次迭代的路径样本数 $N=10^3$, 最大迭代次数 $n_{\max}$=15, 平滑因子 α=0.2. 算法 1 最后一次迭代路径样本用作算法 2 的输入, 即 $N_{IS}=10^3$, 因此共需要 1.5×10^4 个路径样本. 图 3 给出了 CEIL 方法在 15 次迭代过程中参数变化的趋势: 迭代开始时, 观察到参数快速趋向收敛; 当参数接近其最优值时, 它会减慢到随机波动. 在第 10 次迭代时, 参数已经开始收敛到稳定值. 从参数收敛趋势可以看出: 随着迭代次数的增加, 失效率参

数值都有所上升，意味着采样到满足稀有属性的路径比例在逐渐增大. 修复率参数值下降，意味着算法很少做修复转换，因为算法只对系统失效路径感兴趣. 当修复率参数值都不为0时，表明算法试图考虑所有失效路径的点，也意味着算法能够较均匀地采样到满足验证属性的路径.

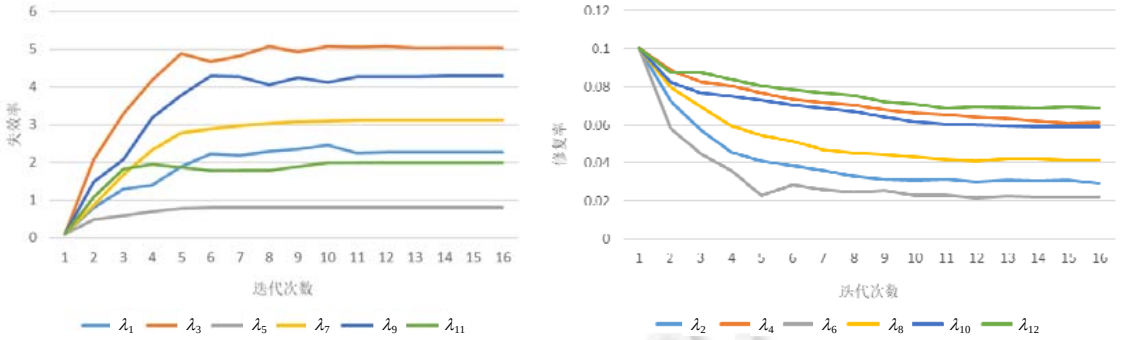

图 3　在 15 次迭代中参数收敛情况

下面给出 CEIL 方法与 BIET 方法[11]的统计性能比较. BIET 方法的精度$\varepsilon=10^{-4}$，置信系数 $1-a=0.95$，先验分布是(0,1)上的均匀分布. CEIL 方法每次迭代的路径样本数 $N=10^3$，最大迭代次数 $n_{\max}=15$，平滑因子$\alpha=0.2$. 在上述参数设置下，使用 CEIL 方法与 BIET 方法分别进行了 100 次实验，计算两种方法的经验均值、偏度、方差、覆盖率和平均每次样本数量等统计指标，见表 1.

使用 PRISM 工具计算属性被满足的概率是 3.286×10^{-5}.

表 1　CEIL 和 BIET 方法的统计性能比较

算法	均值	偏度	方差	半区间宽度	区间覆盖(%)	每次样本数量
CEIL	3.294×10^{-5}	−0.082	9.351×10^{-7}	1.816×10^{-5}	100	1.5×10^{4}
BIET	3.279×10^{-5}	0.076	2.457×10^{-7}	10^{-4}	100	3.158×10^{4}

从表 1 可知: 对于非稀有属性验证, CEIL 方法的计算精度非常接近 BIET 方法，但 BIET 达到指定的精度和置信水平所需的样本数量是 CEIL 方法的 2 倍. 因此, CEIL 方法的计算效率要优于 BIET 方法.

5.3 FFCS稀有属性验证

FFCS 由传感子系统、燃油流量控制器、空燃比计算器和传感器故障检测器组成. 传感子系统由油门角度传感器、发动机速度传感器、废气氧气传感器(EGO)和进气歧管绝对压力传感器(MAP)这 4 个传感器组成. FFCS 检测到单个传感器故障时具有高度稳定性，控制系统会动态地调节参数以防止工作中断. 如果两个以上的传感器发生故障，系统无法可靠地控制空燃比，则发动机关闭. 系统的 Stateflow 控制逻辑共有 24 个位置，分组在 6 个并行状态中，系统的 Simulink 部分由几个非线性方程和带切换条件的线性微分方程组成.

系统随机性是通过在 EGO、速度和 MAP 传感器中引入随机故障而获得的. 通过 3 个具有不同到达率的独立泊松过程对故障进行建模. 当发生故障时，它以 1 s 的固定服务时间修复(即传感器保持故障状态 1 s，然后，它恢复正常操作). 为了保证安全属性是一个否定稀有属性，将 3 个传感器的故障率都设定为 0.001，对应算法 1 中的路径分布的真实参数 $\boldsymbol{u}$. 对油门提供周期性三角形输入，并且标称速度保持不变，这确保了一旦设置了 3 个故障率，对于任何给定的时序逻辑属性φ, 模型满足φ的概率不会改变. FFCS 待验证的安全系统属性是“在 100 s 内，不会发生燃油流量等于 0 达到 1 s”. 在实际系统中，这个属性是非常重要的，因为燃油流量等于 0 达到 1 s，发动机将停止，这可能引发严重的安全事故. 该安全属性用 BLTL 公式表示为

$$\Pr(\neg\Diamond^{100}\Box^{1}(FuelFlowRate=0)).$$

在上述参数设置下，该安全属性的否定是一个稀有属性，BIET 方法在有限的时间内几乎采样不到满足该稀有属性的路径而变得不可行. 为了评估 CEIL 方法对稀有属性验证的性能，将 3 个传感器的初始故障率都设

定为 0.1, 对应算法 1 中的初始参数$\boldsymbol{\lambda}^{(0)}$. 对算法 1 进行 25 次迭代, 每次迭代样本数 N=104, 平滑因子α=0.2, 共需要 2.5×10^5 个样本. 图 4 绘出了 CEIL 在迭代过程中估计值的变化情况, 从第 17 次迭代开始, 估计值逐渐收敛. 图 5 绘出了 CEIL 方法迭代过程中相对误差的变化情况, 从第 19 次迭代开始, 相对误差逐渐收敛. 最终, FFCS 违背安全属性的概率估计值为 2.328×10^{-11}, 相对误差为 0.01.

图 4 CEIL 在迭代过程中估计值的收敛性

图 5 CEIL 在迭代过程中相对误差的变化

为了验证 CEIL 方法的统计性能, 在上述参数下进行了 100 次实验, 每次实验使用 2.5×10^5 个样本. 在相同样本数量下, 与 HIS 方法性能相比, 表 2 给出了均值、偏度、标准方差(似然比标准方差)、相对误差和每次实验的样本数量等统计指标. 从表 2 中可以看出: 在相同样本数量下, 与 HIS 方法相比, CEIL 方法的估计值更好地分布在均值附近, 似然比标准方差和相对误差减少超过 10 倍以上. 虽然真实概率未知, 但似然比标准方差、偏度性以及相对误差等统计指标很好地说明了真实概率与均值是非常接近的.

表 2 CEIL 和 HIS 方法的统计性能比较

算法	均值	偏度	标准方差	相对误差	每次样本数量
CEIL	2.347×10^{-11}	0.036	2.167×10^{-13}	0.010	2.5×10^5
HIS	2.398×10^{-11}	1.296	2.538×10^{-12}	0.126	2.5×10^5

6 总 结

SMC 已成功地应用于 SHS 安全属性验证并成为最有效的解决方案, 但稀有属性验证是 SMC 面临的挑战性问题. 为了能够从 SHS 中采样到满足稀有属性的样本, 通过 CTMC 构造了 SHS 执行路径的概率空间模型, 给出了随机执行路径的概率测度和参数化概率分布函数族. 构造了交叉熵迭代模型, 通过迭代学习, 在 SHS 路径概率空间中找到近似最优的重要性采样分布, 实现了 SHS 稀有属性样本的高效采样. 实验结果表明: 在非稀有属性验证下, 本文方法只需 BIET 方法一半的样本数量, 其计算精度就非常接近于 BIET 方法. 在稀有属性验证下, 在相同样本数量下, 与启发式的重要性采样方法相比, 本文方法的估计值更好地分布在均值附近, 标准方差和相对误差减少超过一个数量级. 基于本文提出的方法, 结合目前主流 SMC 方法开发一个自适应的 SMC 工具, 将是下一步的研究方向.

References:

[1] Hu JH, Lygeros J, Sastry S. Towards a theory of stochastic hybrid systems. In: Lynch N, Krogh B, eds. Proc. of the Hybrid Systems: Computation and Control. Berlin: Springer, 2000. 160–173. [doi: 10.1007/3-540-46430-1_16]

[2] Wang SL, Zhan NJ, Zhang LJ. A compositional modelling and verification framework for stochastic hybrid systems. Journal Formal Aspects of Computing, 2017, 29(4): 751–775. [doi: 10.1007/s00165-017-0421-7]

[3] Liu Y, Li XD, Ma Y, Wang LZ. Survey for stochastic model checking. Chinese Journal of Computers, 2015, 38(11): 2145–2162 (in Chinese with English abstract). [doi: 10.11897/SP.J.1016.2015.02145]

[4] Baier C, Haverkort BR, Hermanns H, Katoen JP. Model-checking algorithms for continuous-time Markov chains. IEEE Trans. on Software Engineering, 2003, 29(6): 524–541. [doi: 10.1109/TSE.2003.1205180]

[5] Beauquier D. On probabilistic timed automata. Theoretical Computer Science, 2003, 292(1): 65−84. [doi: 10.1016/S0304-3975(01)00215-8]

[6] Agha G, Palmskog K. A survey of statistical model checking. ACM Trans. on Modeling and Computer Simulation, 2018, 28(1): 1−39. [doi: 10.1145/3158668]

[7] Legay A, Viswanathan M. Statistical model checking: Challenges and perspectives. Int'l Journal on Software Tools for Technology Transfer, 2015, 17(4): 369−376. [doi: 10.1007/s10009-015-0384-z]

[8] Larsen KG. Statistical model checking, refinement checking, optimization, … for stochastic hybrid systems. In: Proc. of the Formal Modeling and Analysis of Timed Systems (FORMATS 2012). LNCS 7595, Berlin, Heidelberg: Springer-Verlag, 2012. 7−10.

[9] Clarke EM, Zuliani P. Statistical model checking for cyber-physical systems. In: Bultan T, Hsiung PA, eds. Proc. of the Automated Technology for Verification and Analysis. Berlin: Springer, 2011. 1−12.

[10] Ellen C, Gerwinn S, Fränzle M. Statistical model checking for stochastic hybrid systems involving nondeterminism over continuous domains. Int'l Journal on Software Tools for Technology Transfer, 2015, 17(4): 485−504. [doi: 10.1007/s10009-014-0329-y]

[11] Zuliani P, Platzer A, Clarke EM. Bayesian statistical model checking with application to stateflow/simulink verification. Formal Methods in System Design, 2013, 43(2): 338−367. [doi: 10.1007/s10703-013-0195-3]

[12] Legay A, Sedwards S, Traonouez LM. Rare events for statistical model checking an overview. In: Larsen K, Potapov I, Srba J, eds. Proc. of the Reachability Problems. Cham: Springer, 2016. 23−35. [doi: 10.1007/978-3-319-45994-3_2]

[13] Darío RL, Masegosa AR, Antonio S, Rafael R, Helge L, Nielsen TD, Madsen AL. Scalable importance sampling estimation of Gaussian mixture posteriors in Bayesian networks. Int'l Journal of Approximate Reasoning, 2018, 100: 115−134. [doi: 10.1016/j.ijar.2018.06.004]

[14] Boer PTD, Nicola VF. Adaptive state-dependent importance sampling simulation of Markovian queueing networks. European Trans. on Telecommunications, 2012, 13(4): 303−315. [doi: 10.1002/ett.4460130403]

[15] Reijsbergen D, Boer PT, Scheinhardt W, Haverkort BR. Rare event simulation for highly dependable systems with fast repairs. Performance Evaluation, 2012, 69(7−8): 336−355. [doi: 10.1016/j.peva.2011.11.004]

[16] Barbot B, Haddad S, Picaronny C. Coupling and importance sampling for statistical model checking. In: Flanagan C, König B, eds. Proc. of the 18th Int'l Conf. on Tools and Algorithms for the Construction and Analysis of Systems. Berlin: Springer, 2012. 331−346. [doi: 10.1007/978-3-642-28756-5_23]

[17] Zuliani P, Baier C, Clarke EM. Rare-event verification for stochastic hybrid systems. In: Proc. of the 15th ACM Int'l Conf. on Hybrid Systems: Computation and Control (HSCC 2012). Beijing: ACM, 2012. 217−226. [doi: 10.1145/2185632.2185665]

[18] Jegourel C, Legay A, Sedwards S. Command-based importance sampling for statistical model checking. Theoretical Computer Science, 2016, 649: 1−24. [doi: 10.1016/j.tcs.2016.08.009]

[19] Kim Y, Kim M, Kim TH. Statistical model checking for safety critical hybrid systems: An empirical evaluation. In: Biere A, Nahir A, Vos T, eds. Proc. of the Hardware and Software: Verification and Testing. Berlin: Springer, 2013. 162−177. [doi: 10.1007/978-3-642-39611-3_18]

[20] Younes HLS, Simmons RG. Statistical probabilistic model checking with a focus on time-bounded properties. Information and Computation, 2006, 204(9): 1368−1409. [doi: 10.1016/j.ic.2006.05.002]

[21] Hérault T, Lassaigne R, Magniette F, Peyronnet S. Approximate probabilistic model checking. In: Steffen B, Levi G, eds. Proc. of the Verification, Model Checking, and Abstract Interpretation. Berlin: Springer, 2004. 73−84. [doi: 10.1007/978-3-540-24622-0_8]

[22] Jiang G, Fu MC. Importance splitting for finite-time rare event simulation. IEEE Trans. on Automatic Control, 2017, 63(6): 1760−1767. [doi: 10.1109/TAC.2017.2758171]

[23] Jegourel C, Legay A, Sedwards S. An effective heuristic for adaptive importance splitting in statistical model checking. In: Margaria T, Steffen B, eds. Proc. of the Leveraging Applications of Formal Methods, Verification and Validation. Specialized Techniques and Applications. Berlin: Springer, 2014. 143−159. [doi: 10.1007/978-3-662-45231-8_11]

[24] Du DH, Cheng B, Liu J. Statistical model checking for rare-event in safety-critical system. Ruan Jian Xue Bao/Journal of Software, 2015, 26(2): 305−320 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4783.htm [doi: 10.13328/j.cnki.jos.004783]

[25] Kumar JA, Ahmadyan SN, Vasudevan S. Efficient statistical model checking of hardware circuits with multiple failure regions. IEEE Trans. on Computer-aided Design of Integrated Circuits and Systems, 2014, 33(6): 945−958. [doi: 10.1109/TCAD.2014.2299957]

[26] Kalajdzic K, Jégourel C, Lukina A, Bartocci E, Legay A, Smolka SA, Grosu R. Feedback control for statistical model checking of cyber-physical systems. In: Margaria T, Steffen B, eds. Proc. of the Leveraging Applications of Formal Methods, Verification and Validation: Foundational Techniques. Cham: Springer, 2016. 46−61. [doi: 10.1007/978-3-319-47166-2_4]

[27] Infantelopez GG, Hermanns H, Katoen JP. Beyond memoryless distributions: Model checking semi-Markov chains. In: Alfaro L, Gilmore S, eds. Proc. of the PAPM-PROBMIV. Berlin: Springer, 2001. 57−70. [doi: 10.1007/3-540-44804-7_4]

[28] Chen T, Han T, Katoen JP, Mereacre A. Model checking of continuous-time Markov chains against timed automata specifications. In: Proc. of the 24th Annual IEEE Symp. on Logic in Computer Science. IEEE Computer Society, 2009. 309−318.

[29] Boer PTD, Kroese DP, Mannor S, Rubinstein RY. A tutorial on the cross-entropy method. Annals of Operations Research, 2005, 134(1): 19−67. [doi: 10.1007/s10479-005-5724-z]

[30] Cérou F, Moral PD, Furon T, Guyader A. Sequential Monte Carlo for rare event estimation. Statistics and Computing, 2012, 22(3): 795−808. [doi: 10.1007/s11222-011-9231-6]

[31] Boyer B, Corre K, Legay A, Sedwards S. PLASMA-Lab: A flexible, distributable statistical model checking library. In: Kaustubh J, Markus S, Marïelle S, Argenio D, Pedro R, eds. Proc. of the Int'l Conf. on Quantitative Evaluation of Systems. Berlin: Springer, 2013. 160−164. [doi: 10.1007/978-3-642-40196-112]

附中文参考文献:

[3] 刘阳, 李宣东, 马艳, 王林章. 随机模型检验研究. 计算机学报, 2015, 38(11): 2145−2162. [doi: 10.11897/SP.J.1016.2015.02145]

[24] 杜德慧, 程贝, 刘静. 面向安全攸关系统中小概率事件的统计模型检测. 软件学报, 2015, 26(2): 305−320. http://www.jos.org.cn/1000-9825/4783.htm [doi: 10.13328/j.cnki.jos.004783]

房丙午(1974－), 男, 博士, 教授, CCF 专业会员, 主要研究领域为系统安全性分析, 安全关键系统, 形式化方法.

谢健(1988－), 男, 博士生, CCF 专业会员, 主要研究领域为系统安全性分析, 安全关键系统, 形式化方法.

黄志球(1965－), 男, 博士, 教授, 博士生导师, CCF 杰出会员, 主要研究领域为系统软件, 智能软件工程, 安全关键系统.