文章编号: 1000-6788(2012)10-2323-09 中图分类号: V554 文献标志码: A

基于 Markov 链互模拟的航天器发射任务可靠度模型

董学军 [1,2], 武小悦 [1], 陈英武 [1]

(1. 国防科学技术大学 信息系统与管理学院, 长沙 410073; 2. 酒泉卫星发射中心, 酒泉 732750)

摘 要 状态空间复杂、多过程并发执行和子过程反复迭代的特点, 使航天器发射工程实施全过程的任务可靠性评估难以量化. 通过构建多个并发执行的时间连续的 Markov 链对航天器发射工程状态转移约束关系进行描述, 采用互模拟时间等价关系简化航天器发射工程实施过程的状态空间, 利用连续时间 Markov 链的概率转移特性进行建模与分析, 得到了全系统、全过程的航天器发射任务可靠度模型. 数值验证表明该模型可用于航天器发射任务工期推演、可靠度评估以及薄弱环节分析.

关键词 航天器发射; 互模拟; Markov 链; 任务可靠度; 状态转移概率

Mission reliability model of spacecraft launch based on bisimulation of continuous-time Markov processes

DONG Xue-jun[1,2], WU Xiao-yue[1], CHEN Ying-wu[1]

(1. College of Information System and Management, National University of Defense Technology, Changsha 410073, China; 2. Jiuquan Satellite Launch Center, Jiuquan 732750, China)

Abstract Characteristics of complex state space, multi-process concurrent execution and sub-processes iterative make mission reliability assessment for the whole process of spacecraft launch engineering implementation is difficult to quantify. Multiple concurrently executing continuous time Markov chain is constructed to describe state transition constraint relations of spacecraft launch engineering. The state space of the whole process of spacecraft launch engineering implementation is simplified by bisimulation equivalence relation. The model of mission reliability for spacecraft launch engineering is builded by continuous time Markov chain transfer probability characteristics. In this paper, the example applied results shows that the model is a feasible for decision-making demonstration of spacecraft launch project, evaluation of mission reliability and analysis of weak link.

Keywords spacecraft launch; bisimulation; Markov chains; mission reliability; the state transition probabilities

1 引言

航天器发射工程是以航天器和运载器为对象, 综合运用测试、测控和发射技术, 按照预定的程序和规范, 将航天器准确送入预定轨道的过程. 航天器发射任务可靠度是指航天器发射系统在规定条件下、规定时间内达到预期目的的概率. 由于航天器发射具有高新技术多、系统集成复杂、投入经费大和影响范围广等特点, 任务可靠性评估一直是航天器发射任务决策的重点. 基于规模大、复杂度高、不确定因素多等原因, 传统的任务可靠度评价主要集中在航天产品可靠性、地面发射控制和测量控制设备可靠性等关键系统和重点环节. 航天器发射工程实践数据显示, 因组织不当曾造成多次任务发射失败、终止或工期严重延误, 单纯从产品、设备和环境等方面进行可靠性评估不仅不能全面、客观地反映航天器发射任务可靠度, 也不能满足航天器发射任务决策和组织流程改进等方面的需求. 因此, 从全系统、全过程的角度考察航天器发射任务可靠度具有重

收稿日期: 2011-04-18
资助项目: 国家自然科学基金 (70971131, 71071156)
作者简介: 董学军 (1969–), 男, 博士研究生, 高级工程师, 研究方向: 装备采办与项目管理, E-mail: df_dongxuejun@163.com; 武小悦 (1963–), 男, 博士, 教授, 博士生导师, 研究方向: 系统可靠性分析, E-mail: xiaoyuewucn@yahoo.com; 陈英武 (1965–), 男, 博士, 教授, 博士生导师, 研究方向: 系统规划与管理决策, E-mail: ywchen@nudt.edu.cn.

大现实意义.

航天器发射工程是多阶段任务系统 (multiple phased systems, MPS). 20 世纪 70 年代以来, 国内外学者已对 MPS 进行了大量研究, 已有的方法可分为组合建模、状态空间建模和其他方法. 当前组合建模类方法研究的热点主要集中在具有不完全故障覆盖 (imperfect fault coverage, IPC) 网 [1]、组合阶段需求 (combinatorial phase requirement, CPR)[2]、多故障模式 (multimode failure)[3−4] 和共因失效 (Common-cause failure, CCF)[5] 等复杂情况的 MPS 可靠性建模分析上, 使用的主要方法是二元决策图 (Binary Decision Diagram, BDD) 技术. 组合建模具有计算效率高的优点, 但其本质上是一种静态逻辑代数分析法, 难以描述系统的动态行为. 状态空间建模法通常使用连续时间 Markov 链 (continuous time Markov chain, CTMC) 描述 MPS 的状态变化情况, 能较好地描述每个阶段内各部件之间的统计相依性以及部件跨阶段的统计相依性. Kim 等 [6] 对 MPS 的三种情况建模进行了分析, Alam 等 [7] 提出了一种通过拼接阶段 CTMC 模型结果来求解 MPS 可靠性的方法, Murphy 等 [8] 指出该方法由于没有正确考虑阶段间单元的状态影响而存在错误. Mura 和 Bondavalli[9] 将 Petri 网模型与 CTMC 模型相结合提出 MPS 的多层次仿真建模的方法, Mo 等 [10] 针对阶段内任务时间为一般分布的情况使用 Markov 再生过程对 MPS 进行了研究, 李岩等 [11] 将 MPS 的状态在阶段间的变化情况划分为 6 种情况以减少状态数. 状态空间法可以描述系统的动态行为, 但其没有考虑多过程并发执行的情况, 同时, 对于大规模问题存在状态爆炸问题. 为充分利用组合建模与状态空间建模的优点, 一些学者还提出了将两类方法相结合进行 MPS 可靠性建模的方法, 如将 MPS 划分为静态模块与动态模块分别进行处理 [12] 的方法和底层使用 CTMC 模型, 上层使用 BDD 模型的两层建模法 [13] 等.

航天器发射工程组织过程表现为在统一的任务流程下, 相互衔接而又各自相对独立的活动集合. 当把每项活动看作一个状态时, 一组相互衔接的活动就构成一个 CTMC, 使用多个并发执行的 CTMC 可以完整地描述航天器发射工程的全过程. CTMC 是一个用于系统性能分析的数学模型 [14], 利用 CTMC 的研究成果 [15] 可以建立任何一个独立的 CTMC 任务可靠性解析模型, 但由于航天器发射工程实施中存在多个 CTMC 并发执行的情况, 必须考虑多个并发 CTMC 的集结问题. 在并发系统理论中, 人们对广泛使用的 Markov 链模型定义了相关的等价关系, 用来对状态空间进行聚类, 达到压缩状态空间的目的. Van Glabbeek 成功建立了线性和分支时间的等价谱系 [16], 指出互模拟具有比其它等价关系更强的区分能力. 互模拟等价关系 (bisimulation equivalence relations, BER) 是一种定义在状态空间等价和状态空间约简上的等价语义, 它在进程代数和模型检测 [17] 理论中具有重要意义. Baier 等 [18] 将 BER 引入 CTMC 中, 为相应系统状态空间简化提供了重要手段. 本文利用 CTMC 上的 BER, 研究将多个并发和顺序执行的 CTMC 集结成一个 CTMC 的方法, 以达到使用 CTMC 模型考察航天器发射工程全系统、全过程任务可靠性的目的.

2 任务描述及定义

2.1 工程过程简介

本文只考察单次按计划下达的航天器发射工程的任务可靠性, 且工程启动时间确定, 工期明确. 航天器发射一般按照任务准备、单机测试、分系统测试、联合检查和任务发射的流程组织, 并依据物流的实际需要在相应时间节点处安排吊装、对接、转运和加注等活动. 地面测量、发射、控制和通信系统的活动, 按照航天器和运载器测试发射过程时间节点要求随时参与相关工作. 通常依据不同时段工作特点, 航天器发射任务被划分成很多个子过程. 子过程是一组相互关联的活动, 由输入、输出和明确的工作范围, 全部子过程构成一个有限集, 每个子过程的输出要求是由有限标准组成的集合, 决策者依据过程输出与标准集的吻合程度决定是否转入下一子过程、或转入已实施过的某子过程、或终止任务发射.

表 1 是按照航天器发射工程工艺流程关系和工程里程碑进行归纳、筛选后的主要子过程列表, 图 1 是按照某航天发射中心基础设施、工作环境和工作关系约束, 使用表 1 中的子过程项目, 抽象形成的航天器发射工程任务过程简图 (实际的任务过程要复杂得多). 图中节点代表子过程, 节点编号与表 1 中的编号保持一致.

2.2 模型定义

将子过程看成 CTMC 中的状态, 即子过程与状态等价, 则航天器发射任务组织实施过程是多个随时间连续变化于离散状态空间的马尔科夫链.

定义 1 用 $i, i = 1, 2, \cdots, n$ 表示任务状态, 将任务开始时刻记为 $t_0 = 0, t_i$ 表示任务处于状态 i 的时刻,

有 $t_n > t_{n-1} > \cdots > t_1 > t_0 = 0$, 则任务过程可表示为一个 CTMC 的三元组 (S, R, D), 其中 S 是状态空间 $\{1, 2, \cdots, n\}$ 的集合 (n 是有限正整数), R 是 $S \times S$ 的转移率矩阵, D 是初始分布或初始态.

表 1 航天器发射工程主要子过程列表

编号	子过程 (状态)	编号	子过程 (状态)	编号	子过程 (状态)	编号	子过程 (状态)
1	航天器进场	2	航天器单元分系统检测	3	航天器总装及检漏	4	航天器电测匹配总检查
5	航天器模飞	6	航天器与应用系统总装联试	7	航天器扣罩、转运	8	运载器进场
9	运载器吊装对接单元测试	10	运载器分系统测试	11	运载器匹配测试	12	运载器总检查
13	线电路调整、装备转场	14	测控通信系统联调联试	15	飞控模式演练	16	联合检查
17	航天器加注、运载器复测	18	对接及转运	19	运载器加注及发射	20	任务成功
21	任务失败	22	任务终止				

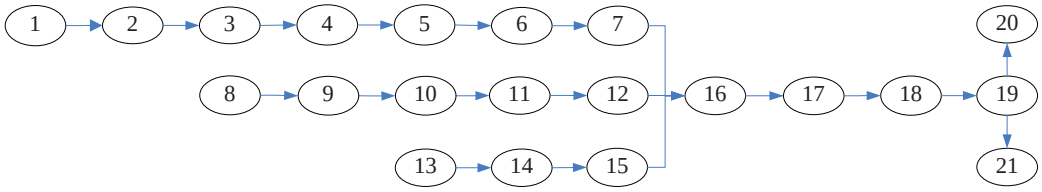

图 1 航天器发射工程过程简图

定义 2　将航天器发射任务过程看作连续时间的随机过程 $X(t), t \geq 0$, 如果 $X(t) = i$, 那么称该过程在 t 时刻处于状态 i. 以 $P_{ij}(\Delta t)$ 表示任务处于状态 i 在经过时间 Δt 后处于状态 j 的概率, 由 CTMC 的性质知, 对一切 $\Delta t \geq 0$ 和非负整数 $i, j, x(u), 0 \leq u < t$ 有

$$\begin{aligned} P_{ij}(\Delta t) &= P\{X(\Delta t + t) = j | X(t) = i, X(u) = x(u), 0 \leq u < t\} \\ &= P\{X(\Delta t + t) = j | X(t) = i\} = 1 - \mathrm{e}^{-\lambda_{ij}\Delta t} \end{aligned} \tag{1}$$

参数 λ_{ij} 称为状态 i 到状态 j 的转移率, 与时间 Δt 无关. i 与 j 不同, 若 i 与 j 相同, 则概率 $P_{ij}(\Delta t)$ 表示任务在 Δt 内仍然停留在状态 i 的概率, 并随时间的增加而减少.

定义 3　用 T_i 表示完成子过程 i 的规定时刻, t_i 为子过程花费的时间, 依据图 1 中的工作流程约束, 则子过程 i 的任务可靠度函数为:

$$R_i(t_i) = \begin{cases} P_{i,16}\left(t_i \leq T_i\right), & i = 7, 12, 15 \\ P_{i,20}\left(t_i \leq T_i\right), & i = 19 \\ P_{i,i+1}\left(t_i \leq T_i\right), & i \neq 7, 12, 15, 19 \end{cases} \tag{2}$$

用 T 表示工程工期, t 为工程花费的时间, i_0 是任务的初始态, 则任务可靠度函数为:

$$R(t) = P_{i_0,20}\left(t \leq T\right) \tag{3}$$

定义 4　令 q_{ij} 为任务处于状态 i 时转移到状态 j 的速率, 即瞬时转移率, v_i 是过程处于状态 i 时的转移速率, 而 P_{ij} 是这个状态转移到状态 j 的概率, 对一切 i, j 有 $q_{ij} = v_i P_{ij}$, 令

$$\lambda_{ij} = \begin{cases} q_{ij}, & i \neq j \\ -v_i, & i = j \end{cases} \tag{4}$$

上式中 λ_{ij} 表示状态 i 到状态 j 的转移率. 定义转移率矩阵

$$M = (\lambda_{ij})_{n \times n}, \quad i, j = 1, 2, \cdots, n \tag{5}$$

其中 $\lambda_{ii} = -\sum_{j \neq i}^{n} \lambda_{ij}$, 即 $\sum_{j=1}^{n} \lambda_{ij} = 0$.

3　模型设计

3.1　任务过程 Markov 模型

图 2 是依据图 1 和表 1 绘制的航天器发射工程状态转移约束关系图.

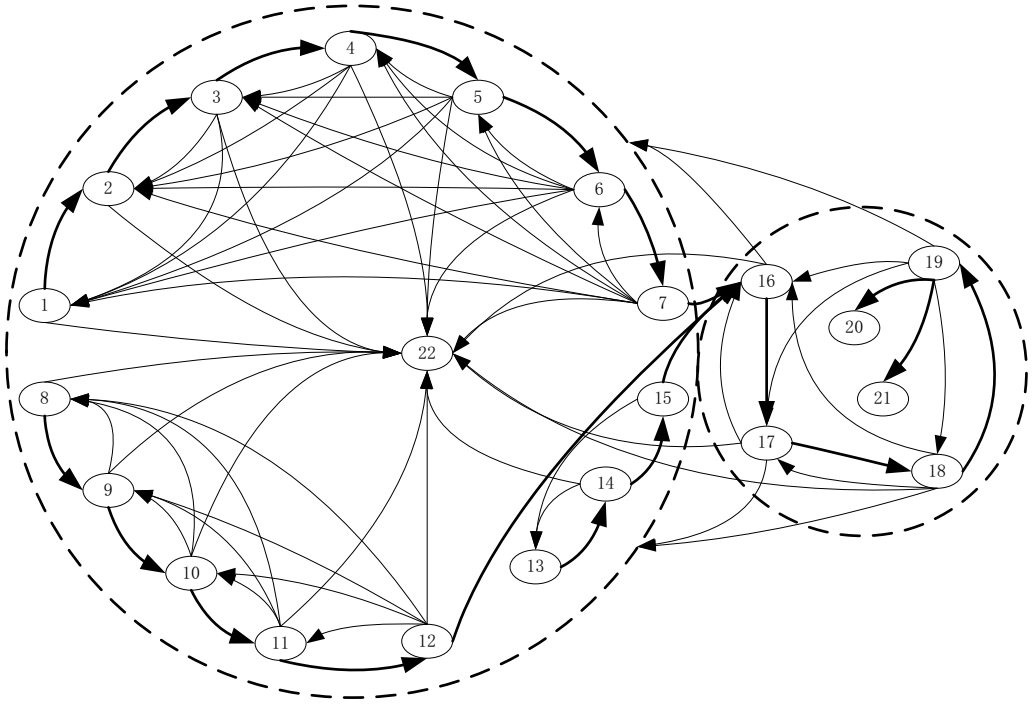

图 2 航天器发射工程状态转换模型

图 2 中使用三个 CTMC $L1$、$L2$、$L3$ 分别表示航天器和应用系统、运载器系统、测控通信系统的部件、单元、分系统、匹配和总检查的状态变化过程, 其中 $S_{L1}=\{1,2,3,4,5,6,7,16,22\}$ 是航天器和应用系统测试装配的任务状态集, $S_{L2}=\{8,9,10,11,12,16,22\}$ 是运载器测试总装的任务状态集, $S_{L3}=\{13,14,15,16,22\}$ 是测控通信系统联试对接演练的状态集, $16,22$ 为吸收态, 其他状态是暂态. 使用 CTMC $L4$ 表示航天器和应用系统、运载器系统、测控通信系统共同组织联合检查、测试、加注、合练和发射的过程, 其中 $S_{L4}=\{16,17,18,19,20,21,22\}$ 是其任务状态集, $20,21$ 和 22 为吸收态, 其他状态是暂态.

由于航天器发射任务组织过程中任一子过程都可能因为航天产品性能、或地面设备原因、或组织失误而导致发射任务终止, 所以存在一个吸收态 22(终止). 任务发射的结果可能是航天器准确入轨并开始正常工作, 也可能是航天器未到达预定轨道、或虽到达预定轨道但不能正常工作, 因此还存在两个吸收态 20(成功) 和 21(失败). 实际工程中, 只有航天器和应用系统、运载器系统、测控通信系统都满足联合检查的条件时, 任务才能进入联合检查阶段. 因此图 2 中状态 $7,12$ 和 15 必须同时转移到状态 16, 即三者中的任一状态转移到 16 必须以其他两个状态转移为条件.

3.2 状态转移率模型

3.2.1 状态转移概率

在 CTMC Lk 中, 状态 i 转移到后继状态 j 的概率 P_{ij} 与航天产品任务可靠度、地面设备任务可靠度和任务组织可靠度直接相关. 航天产品 (包括航天器、应用系统和运载器) 可靠度是指在子过程 i 的任务剖面内, 航天产品满足测试、试验和装配要求的概率. 设航天器可靠度为 a_i, 运载器可靠度为 b_i, 应用系统可靠度为 c_i, 则航天产品可靠度 $r_{sp,i}=a_i\times b_i\times c_i$. 地面设备可靠度 (包括测发、测控通信和关键勤务保障设备) 是指在子过程 i 的任务剖面内, 地面设备完成规定功能的概率. 设测发设备任务可靠度为 d_i, 测控通信设备任务可靠度为 e_i, 关键技术勤务保障设备任务可靠度为 f_i, 则地面设备可靠度 $r_{eq}=d_i\times e_i\times f_i$. 任务组织可靠度是指在现有资源和流程下, 在子过程 i 的任务剖面内组织完成规定任务的概率, 用 $r_{og,i}$ 表示. 航天产品、地面设备和组织任务可靠度的评估都有相应的规范或指导方法, 本文不讨论此类问题. 由于航天产品可靠度、地面设备可靠度和组织任务可靠度相互独立, 因此在规定时间内子过程 i 正常结束的概率 r_i 为

$$r_i=r_{sp,i}\times r_{eq,i}\times r_{og,i} \tag{6}$$

由于子过程 i 的正常结束便意味着任务正常进入到后继子过程 j, 因此在规定时间内, 任务从第 i 个状态转移到后继状态 j 的概率就是子过程 i 正常结束的概率 r_i. 当过程离开状态 i, 以 P_{ij} 进入另一个状态 j

时, 有 $p_{ii}=0, \sum_j p_{ij}=1$. 实际工程中, 子过程 i 的工作范围、活动内容和可用资源是确定的, 其完成时间是可以预期的, 用 Δt_i 表示. 用 T_{i-1} 表示任务离开状态 $i-1$ 进入状态 i 的时刻, $P_{i,22}$ 表示任务自状态 i 转入终止态 22 的概率, $P_{19,21}$ 表示任务自状态 19 转入失败态的概率 21, 其中 $P_{i,21}, P_{i,22}$ 可通过数据统计或专家估算获得. 考察以下情况:

(a) 当 $i=1,8,13$, 即 i 为 CTMC $L1$、$L2$ 或 $L3$ 中的第一个状态时, 工程离开状态 i 时只能进入后继状态 $i+1$ 或终止态 22, 有

$$P_{ij}=\frac{r_i}{r_i+P_{i,22}},\quad j=i+1 \tag{7}$$

(b) 当 $i=2,3,4,5,6,7,9,10,11,12,14,15,16,17,18$, 即 i 不是 CTMC $L1$、$L2$ 和 $L3$ 中的第一个状态, 也不是 CTMC $L4$ 的最后一个暂态时, 工程离开状态 i 时只能转入其后继状态 k, 或其之前的某个状态, 或终止态 22. 设在状态 i 之前共有 n 个状态, 有

$$P_{ij}=\begin{cases} r_i, & j=k \\ \dfrac{1-r_i-P_{i,22}}{n}, & j<i \end{cases} \tag{8}$$

(c) 当 $i=19$ 即 i 是 CTMC $L4$ 中的最后一个暂态时, 工程离开状态 i 时只能转入成功态 20, 或失败态 21, 或 i 之前的某个状态. 设 i 之前共有 n 个状态, 有

$$P_{ij}=\begin{cases} r_i, & j=20 \\ \dfrac{1-P_{i,20}-P_{i,21}}{n}, & j<i \end{cases} \tag{9}$$

3.2.2 状态逗留概率

令 Δt_i 为考察工程状态 i 的时间间隔, 也是完成子过程 i 所需的时间. 用 T_i^* 表示状态 i 的开始时刻, P_{ii} 表示工程仍逗留在状态 i(暂态) 的概率. 依据航天器发射工程子过程的特点, 设在任意观察时刻 $T_i^*+m\Delta t_i$, 状态 i 转移到其之前各状态的概率和仍逗留在状态 i 的概率相同, 设状态 i 之前共有 $n-1$ 个状态, 在 $T_i^*+\Delta t_i$ 时刻, 有

$$P_{ii}\left(T_i^*+\Delta t_i\right)=\begin{cases} \dfrac{1-r_i-P_{i,22}}{n}, & i\neq 19 \\ \dfrac{1-r_i-P_{i,20}-P_{i,21}}{n}, & i=19 \end{cases} \tag{10}$$

在观察 (工程实际中决定是否转入下一子过程) 时刻工程仍逗留在状态 i, 意味着需重新组织实施子过程 i, 因此, 在 $T_i^*+2\Delta t_i$ 时刻, 有

$$P_{ii}\left(T_i^*+\Delta t_i\right)=\begin{cases} \left(\dfrac{1-r_i-P_{i,22}}{n}\right)^2, & i\neq 19 \\ \left(\dfrac{1-r_i-P_{i,20}-P_{i,21}}{n}\right)^2, & i=19 \end{cases} \tag{11}$$

在 $T_i^*+m\Delta t_i$ (m 为正整数) 时刻, 有

$$P_{ii}\left(T_i^*+\Delta t_i\right)=\begin{cases} \left(\dfrac{1-r_i-P_{i,22}}{n}\right)^m, & i\neq 19 \\ \left(\dfrac{1-r_i-P_{i,20}-P_{i,21}}{n}\right)^m, & i=19 \end{cases} \tag{12}$$

3.2.3 状态转移率

当 $i\neq 19$ 时, 任务逗留在状态 i 的时间 Δt_i 的数学期望为

$$\begin{aligned}\Delta t_i^* &= \Delta t_i+\Delta t_i\frac{1-r_i-P_{i,22}}{n}+\Delta t_i\left(\frac{1-r_i-P_{i,22}}{n}\right)^2+\cdots+\Delta t_i\left(\frac{1-r_i-P_{i,22}}{n}\right)^m+\cdots \\ &= \frac{n\Delta t_i}{n-1+r_i+P_{i,22}}\end{aligned} \tag{13}$$

同理得 $i=19$ 时, 任务逗留在状态 i 的时间的数学期望 Δt_i^* 为

$$\Delta t_i^*=E\left(t_i\right)=\frac{n\Delta t_i}{n-1+r_i+P_{i,20}+P_{i,21}} \tag{14}$$

所以, 工程离开状态 i 的速度的数学期望 v_i^* 为

$$v_i^* = E(v_i) = \begin{cases} \dfrac{n\Delta t_i}{n-1+r_i+P_{i,22}}, & i \neq 19 \\ \dfrac{n\Delta t_i}{n-1+r_i+P_{i,20}+P_{i,21}}, & i = 19 \end{cases} \tag{15}$$

由式 (4) 得状态转移率 $\lambda_{i,j}$ 为

$$\lambda_{i,j} = \begin{cases} v_i^* P_{i,j}, & i \neq j \\ -v_i^*, & i = j \end{cases} \tag{16}$$

3.3 互模拟等价关系模型

依据任务过程 Markov 模型, $L1$、$L2$ 和 $L3$ 是并发的, 并在同一时刻转移到 $L4$ 的状态 16. 不考虑 $L1$、$L2$ 和 $L3$ 的内部状态及其转移特性, 只考察它们外部可见的开始时间、转移速度和转移到状态 16 和 22 的转移概率. 假设存在一个等价类 C, 使得任务子过程 $L123$ 的外部特性与 $L1$、$L2$ 和 $L3$ 并发执行时表现的外部特性相同, 我们称 $L123$ 与 $L1$、$L2$ 和 $L3$ 并发执行存在互模拟等价关系. 令 T_0 为任务开始时间, V 为任务离开 $L1$、$L2$ 和 $L3$ 并发执行状态的速度, P 为任务转移至状态 16 和 22 的概率. 定义 $L1$、$L2$ 和 $L3$ 并发执行的状态集为 S, 即 S 是由 $L1$、$L2$ 和 $L3$ 中所有暂态组成的集合, $S = \{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\}$, $P_{j,22}$ 是 S 集中任一状态 j 转移至吸收态 22 的概率. 从外部观察, S 转移到吸收态 22 的概率 $P_{S,22}$ 是所有 $P_{j,22}$ 共同作用的结果.

$$P_{S,22} \approx 1 - \prod_{j \in S} (1 - P_{j,22}) \tag{17}$$

由公式 (14) 计算任一子过程 i 花费时间的数学期望, 得

$L1$ 花费时间的期望是 $\Delta t_{L1}^* = \Delta t_1^* + \Delta t_2^* + \Delta t_3^* + \Delta t_4^* + \Delta t_5^* + \Delta t_6^* + \Delta t_7^*$;

$L2$ 花费时间的期望是 $\Delta t_{L2}^* = \Delta t_8^* + \Delta t_9^* + \Delta t_{10}^* + \Delta t_{11}^* + \Delta t_{12}^*$;

$L3$ 花费时间的期望是 $\Delta t_{L3}^* = \Delta t_{13}^* + \Delta t_{14}^* + \Delta t_{15}^*$;

任务在状态集 S 的逗留时间 Δt_S 的数学期望是 $\Delta t_S^* = \max(\Delta t_{L1}^*, \Delta t_{L2}^*, \Delta t_{L3}^*)$.

所以任务离开状态集 S 的速度 v_S 的数学期望是

$$v_S^* = \frac{1}{\max(\Delta t_{L1}^*, \Delta t_{L2}^*, \Delta t_{L3}^*)} \tag{18}$$

定义 $L123$ 在 t_0 时刻开始 (t_0 为 $L1$、$L2$ 和 $L3$ 中初始状态的最早开始时刻), 离开速度为 v_S^*, 转移至状态 16 的概率为 $P_{S,16} = 1 - P_{S,22}$, 转移至吸收态 22 的概率为 $P_{S,22}$, 则从外部看, 存在一个等价类 $C = \{16, 22\}$, 使得 $L123$ 与 $L1$、$L2$ 和 $L3$ 并发执行具有相同的外部性质表现, 即 $L123$ 与 $L1$、$L2$ 和 $L3$ 并发执行互模拟. 图 3 是使用互模拟等价关系对图 2 进行压缩后的状态转换图, 图中 $L123$ 是模拟态.

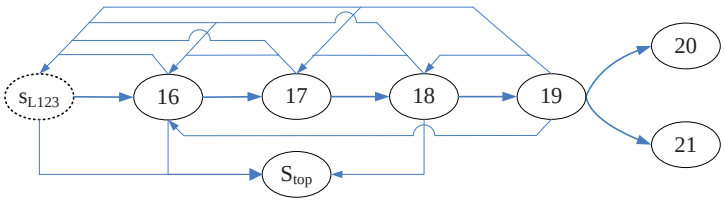

图 3 状态空间压缩后的航天器发射工程状态转换图

从图 3 可以看出, 模拟态 $L123$ 与 CTMC $L4$ 构成一个新的 CTMC EL, 其描述了航天器发射工程的全系统、全过程. 按照定义 3 和定义 4, 根据文献 [15] 给出的结果, 在给定任务开始状态、结束状态和任务工期 T 后, 有任务可靠度

$$R(T) = \mathrm{e}^{MT} \approx \left(I - \frac{MT}{n}\right)^{-n} = \left[\left(I - \frac{MT}{n}\right)^{-1}\right]^n \tag{19}$$

式中 n 为 2 的一个大幂, M 是 CTMC 的转移率矩阵. 通过计算矩阵 $I - \frac{MT}{n}$ 的逆, 并增加这个矩阵到 n 次幂, 就可得到航天器发射任务可靠度的近似值.

4 数值分析

X-51 是一次常规卫星发射任务, 工程实施所需的主要子过程见表 1, 各主要子过程的数据如表 2 所示, 其中航天器可靠度数据是根据航天领域技术现状进行的假定, 地面设备可靠度是对某航天发射中心现有水平的模拟, 组织可靠度是根据国内航天发射任务组织现状, 不失一般性的假定, 子过程完成时间和终止率是依据工程实践统计数据并经折算后的结果. 将航天器经空运首先到达发射场的时刻记为 $t_0 = 0$, 100 个工作时间单位后, 运载器经铁路运输至发射场, 130 个工作时间单位后, 测控通信系统开始进行线电路调整和装备转场.

表 2　X-51 航天器发射工程主要子过程数据表

子过程	航天产品可靠度			地面设备可靠度			组织	完成子过程	终止率	任务计
	a_i	b_i	c_i	d_i	e_i	f_i	可靠度	需要的时间		划时间
1	1	–	1	0.9999	–	0.9999	0.9995	32	6.5×10-4	42
2	0.9990	–	0.9990	0.9995	–	0.9999	0.9995	32	6.5×10-4	42
3	0.9990	–	–	0.9995	–	0.9999	0.9995	28	6.5×10-4	38
4	0.9990	–	0.9990	0.9995	–	0.9999	0.9995	48	6.5×10-4	60
5	0.9990	–	–	0.9995	–	0.9999	0.9995	44	6.5×10-4	55
6	0.9990	–	0.9990	0.9995	–	0.9999	0.9995	24	6.5×10-4	32
7	0.9990	–	–	0.9995	–	0.9999	0.9995	28	6.5×10-4	38
8	–	1	–	0.9999	–	0.9997	0.9995	32	7.0×10-4	42
9	–	0.9980	–	0.9995	–	0.9997	0.9995	32	7.0×10-4	42
10	–	0.9980	–	0.9995	–	0.9997	0.9995	36	7.0×10-4	48
11	–	0.9980	–	0.9995	–	0.9997	0.9995	32	7.0×10-4	42
12	–	0.9980	–	0.9995	–	0.9997	0.9995	24	7.0×10-4	33
13	–	–	–	1	1	–	1	40	0	66
14	–	–	–	0.9999	0.9995	–	0.9995	40	10-5	66
15	–	–	–	0.9995	0.9990	–	1	28	0	45
16	0.9990	0.9990	0.9990	0.9995	0.9995	0.9998	0.9995	36	5.0×10-4	48
17	0.9990	0.9990	0.9990	0.9995	–	0.9998	0.9995	40	5.0×10-4	52
18	0.9990	0.9990	0.9990	0.9995	–	0.9998	0.9995	16	5.0×10-4	22
19	0.9990	0.9990	0.9990	0.9995	0.9995	0.9998	0.9995	24	0	32

第一步, 使用状态转移率模型, 根据表 2 中数据构建 CTMC $L1$、$L2$ 和 $L3$ 的转移率矩阵, 得

$$M_{L1}=\begin{vmatrix} -0.03125 & 0.03123 & 0.00000 & 0.00000 & 0.00000 & 0.00000 & 0.00000 & 0.00000 & 0.00002 \\ 0.00007 & -0.03125 & 0.03115 & 0.00000 & 0.00000 & 0.00000 & 0.00000 & 0.00000 & 0.00002 \\ 0.00002 & 0.00002 & -0.03571 & 0.03564 & 0.00000 & 0.00000 & 0.00000 & 0.00000 & 0.00002 \\ 0.00002 & 0.00002 & 0.00002 & -0.02083 & 0.00000 & 0.00000 & 0.00000 & 0.00000 & 0.00001 \\ 0.00003 & 0.00003 & 0.00003 & 0.00003 & -0.02273 & 0.02258 & 0.00000 & 0.00000 & 0.00001 \\ 0.00006 & 0.00006 & 0.00006 & 0.00006 & 0.00006 & -0.04167 & 0.04135 & 0.00000 & 0.00003 \\ 0.00001 & 0.00001 & 0.00001 & 0.00001 & 0.00001 & 0.00001 & -0.03571 & 0.03564 & 0.00002 \\ 0.00000 & 0.00000 & 0.00000 & 0.00000 & 0.00000 & 0.00000 & 0.00000 & 0.00000 & 0.00000 \\ 0.00000 & 0.00000 & 0.00000 & 0.00000 & 0.00000 & 0.00000 & 0.00000 & 0.00000 & 0.00000 \end{vmatrix}$$

$$M_{L2}=\begin{vmatrix} -0.03125 & 0.03123 & 0.00000 & 0.00000 & 0.00000 & 0.00000 & 0.00002 \\ 0.00007 & -0.03125 & 0.03116 & 0.00000 & 0.00000 & 0.00000 & 0.00002 \\ 0.00003 & 0.00003 & -0.02778 & 0.02769 & 0.00000 & 0.00000 & 0.00002 \\ 0.00002 & 0.00002 & 0.00002 & -0.03125 & 0.03116 & 0.00000 & 0.00002 \\ 0.00002 & 0.00002 & 0.00002 & 0.00002 & -0.04167 & 0.04154 & 0.00003 \\ 0.00000 & 0.00000 & 0.00000 & 0.00000 & 0.00000 & 0.00000 & 0.00000 \\ 0.00000 & 0.00000 & 0.00000 & 0.00000 & 0.00000 & 0.00000 & 0.00000 \end{vmatrix}$$

$$M_{L3}=\begin{vmatrix} -0.02500 & 0.02500 & 0.00000 & 0.00000 & 0.00000 \\ 0.00002 & -0.02500 & 0.02496 & 0.00000 & 0.00002 \\ 0.00011 & 0.00011 & -0.03571 & 0.03550 & 0.00000 \\ 0.00000 & 0.00000 & 0.00000 & 0.00000 & 0.00000 \\ 0.00000 & 0.00000 & 0.00000 & 0.00000 & 0.00000 \end{vmatrix}$$

第二步, 使用互模拟模型构建模拟态 $L123$, 得 CTMC $L1$、$L2$ 和 $L3$ 结束时所用时间的数学期望分别是 257.17, 170.19 和 117.59. 考虑 CTMC $L2$ 和 $L3$ 的开始时间, 得模拟态 $L123$ 的转移率参数为: $\lambda_{L123}\approx 0.00370, \lambda_{L123,16}\approx 0.00367, \lambda_{L123,22}\approx 0.00003$.

第三步, 使用式 (19) 计算 CTMC $L1$、$L2$、$L3$ 和 EL 的任务可靠度, 使用式 (1) 计算 $L123$ 任务可靠度, 得任务可靠度与时间关系见图 4.

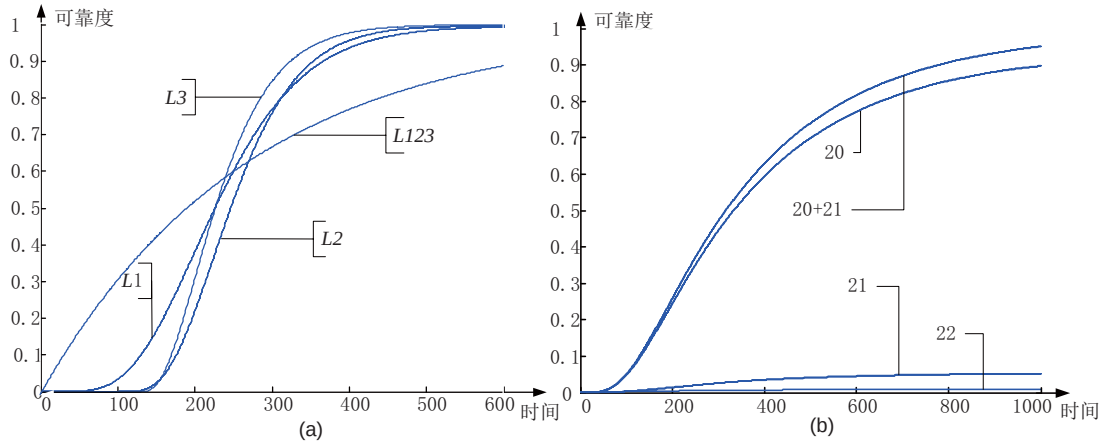

图 4 任务可靠度与时间关系图

图 4(a) 表达了 CTMC $L1$、$L2$、$L3$ 的任务可靠度与计划时间的关系, 并通过模拟态 $L123$ 展现了 CTMC $L1$、$L2$、$L3$ 并发执行转移到状态 16 的任务可靠度与计划时间的关系. 图 4(b) 给出了全系统、全过程的任务可靠度, 图中曲线表示系统从初始态开始执行, 随时间的变化处于状态 $20, 21, 22$ 的概率.

第四步, 评价任务计划的合理性.

由表 2 知, CTMC $L1$ 的计划工作时间是 307, 计算或查图 4 得其过程可靠度约为 0.80; CTMC $L2$ 的计划工作时间是 207, 计算或查图 4 得其过程可靠度约为 0.79; CTMC $L3$ 的计划工作时间是 177, 计算或查图 4 得其过程可靠度约为 0.86; 任务总计划时间是 461, 计算或查图 4 得其过程可靠度为 0.69.

CTMC $L1$、$L2$、$L3$ 的过程可靠度均在 0.79 以上, 且相差不大; 在计划时间内成功实施发射的可靠度约 0.69, 因此表 2 中给出的 X-51 任务计划可行. 当然, 也可使用本文所给模型对任务计划进行详细讨论或进一步优化.

5 结论

本文以航天器发射工程实践为背景, 针对航天器发射工程任务状态空间有限、多过程并发执行和子过程间反复迭代的特点, 利用连续时间马尔科夫链状态转移率的性质和并发系统中的互模拟技术, 建立了基于多吸收态、多个 CTMC 并发执行和子过程反复迭代的航天器发射任务可靠度模型, 给出了各种状态下任务可靠度的计算方法, 并用数值验证说明了该模型可用于航天器发射任务工期推演、可靠度评估以及薄弱环节分析.

参考文献

[1] Xing L. Reliability evaluation of phased-mission systems with imperfect fault coverage and common-cause failures[J]. IEEE Transactions on Reliability, 2007, 56(1): 58–68.

[2] Xing L. Reliability analysis of phased-mission systems with combinatorial phase requirements[C]. Proceeding of 2001 Annual reliability and Maintainability Symposium, 2001: 344–351.

[3] Tang Z H, Dugan J B. BDD-based reliability analysis of phased-mission systems with multimode failures[J]. IEEE Transactions on Reliability, 2006, 55(2): 350–360.
[4] Zang X Y, Wang D Z, Sun H R, et al. A BDD-based algorithm for analysis of multistate systems with multistate components[J]. IEEE Transactions on Computers, 2003, 52(12): 1608–1618.
[5] Tang Z H, Xu H, Dugan J B. Reliability Analysis of Phased Mission Systems with Common Cause Failure[C]// Proceeding of 2005 Annual Reliability and Maintainability Symposium, New York, USA: IEEE Press, 2005: 313–318.
[6] Kim K, Park K S. Phased-mission system reliability under Markov environment[J]. IEEE Transactions on Reliability, 1994, 43(2): 301–309.
[7] Alam M, Song M, Hester S L, et al. Reliability analysis of phased-mission systems: A practical approach[C]// Proceeding of the Annual Reliability & Maintainability Symposium, New York, USA: IEEE Press, 2006: 551–558.
[8] Murphy K E, Carter C M, Malerich A W. Reliability analysis of phased-mission system: A correct approach [C]// Proceeding of the Annual Reliability & Maintainability Symposium, New York, USA: IEEE Press, 2007: 7–12.
[9] Mura I, Bondavalli A. Hierarchical modeling and evaluation of phased-mission systems[J]. IEEE Transactions on Reliability, 1999, 48(4): 360–368.
[10] Mo Y C, Siewiorek D, Yang X Z. Mission reliability analysis of fault-tolerant multiple-phased systems[J]. Reliability Engineering and System Safety, 2008, 93(7): 1036–1046.
[11] 李岩, 王社伟. 一种新型的多阶段任务系统可靠性分析方法 [J]. 计算机仿真, 2008, 25(1): 100–104.
Li Y, Wang S W. A new reliability analysis method for PMS[J]. Computer Simulation, 2008, 25(1): 100–104.
[12] Yong O, Meshkat L, Dugan J B. Multi-phase reliability analysis for dynamic and static phase[C]// Proceeding of 2002 Anuual Reliability and Maintainability Symposium, IEEE, 2002: 404–410.
[13] Wang D Z, Trivedi K S. Reliability analysis of phased-mission system with independent component repairs[J]. IEEE Transactions on Reliability, 2007, 56(3): 540–550.
[14] 吴尽召, 王永祥, 覃广平. 交互式马尔科夫链 [M]. 北京: 科学出版社, 2007.
Wu J Z, Wang Y X, Tan G P. Interactive Markov Chains[M]. Beijing: Science Press, 2007.
[15] Ross S M. Introduction to Probability Models[M]. 9th ed. Academic Press, 2006.
[16] Van Glabbeek R J. The Linear Time-Branching Time Spectrum[M]. Institute für Informatik, Technische Universität München, 1990.
[17] Clark E M, Long D E, Mcmillan K L. Compositional Model Checking[M]. Boston: MIT Press, 1999.
[18] Baier C, Katoen J P, Hermanns H, et al. Simulation for Continuous-time Markov Chains[M]. Uni Bonn: Technical Report, 2002.