ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.18, No.4, April 2007, pp.1068−1076
DOI: 10.1360/jos181068

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

一般阶段任务系统的任务可靠性分析*

莫毓昌+, 杨孝宗, 崔 刚, 刘宏伟

(哈尔滨工业大学 计算机科学与技术系,黑龙江 哈尔滨 150001)

Mission Reliability Analysis of Generalized Phased Mission Systems

MO Yu-Chang+, YANG Xiao-Zong, CUI Gang, LIU Hong-Wei

(School of Computer Science and Technology, Harbin Institute of Technology, Harbin 150001, China)

+ Corresponding author: Phn: +86-451-86413555, Fax: +86-451-86414093, E-mail: myc@ftcl.hit.edu.cn

Mo YC, Yang XZ, Cui G, Liu HW. Mission reliability analysis of generalized phased mission systems. *Journal of Software*, 2007,18(4):1068−1076. http://www.jos.org.cn/1000-9825/18/1068.htm

Abstract: To attack the weak points of the state-of-the-art, this paper shows how to analyze mission reliability of the generalized PMS with random phases duration and Markov regenerative intraphase processes. These generalized PMS are modeled under a simple and practical 5-tuple analysis model. This paper proves that the underlying intraphase processes are Markov regenerative processes and shows how to compute the conditional transient occupation probability matrix for each phase. Then it shows how to use these matrices to compute mission reliability of the generalized PMS. Using Laplace transformation can simplify the whole analysis process. Equipped with the analysis model, reliability of the generalized PMS can be efficiently analyzed.

Key words: phased mission systems (PMS); reliability analysis; homogeneous Markov pocess; Markov regenerative process; Laplace transformation

摘 要: 研究一般 PMS 的任务可靠性分析.首先给出一个五元组分析模型,该模型能够有效描述阶段持续时间是随机分布的、阶段内行为特性符合马尔可夫再生过程的一般 PMS;为了降低计算复杂度,分析模型的求解过程由两个步骤组成,首先利用马尔可夫再生过程理论,给出一般 PMS 的阶段内随机过程分析公式和简化计算方法;然后给出一般 PMS 任务可靠性分析公式和简化计算方法.应用该分析模型和求解方法,可以有效地对一般 PMS 进行可靠性分析.

关键词: 阶段任务系统;可靠性分析;齐次马尔可夫过程;马尔可夫再生过程; Laplace 变换
中图法分类号: TP316 文献标识码: A

阶段任务系统(phased mission systems,简称 PMS)是一类应用非常广泛的系统.PMS 通过按序执行一系列作业(task),从而完成预定的系统任务(mission),由此,PMS 的整个操作生命周期是由非交叉的阶段(phase)序列构成.通常在一个特定的阶段中,系统经受的环境压力和执行的阶段作业是与其他阶段不同的,因此,系统的可靠性参数(包括维修率和失效率等)和可靠性需求对于不同的阶段是不同的.为了完成预定的任务,PMS 就需要不断改变自身配置以与正在执行的阶段的性能和可靠性要求进行匹配,如果匹配不成功,整个系统就失效,后续的

* Supported by the National Natural Science Foundation of China under Grant No.60503015 (国家自然科学基金)
Received 2005-10-24; Accepted 2006-05-16

阶段就不能执行,从而任务就不能完成.

对 PMS 的任务可靠性分析就是计算在预定时间内系统执行完毕所有的阶段作业完成阶段任务的概率.由于PMS经常被配置到关键应用(critical application)中,特别是航天和军用装备领域,其任务可靠性分析就成为一个重要的问题;同时,由于 PMS 在运行过程中配置和可靠性参数都不断发生变化,这种变化使得 PMS 的任务可靠性分析很困难.

分析 PMS 的任务可靠性的方法可以分成两类:基于状态空间的动态分析方法[1−9]和基于组合模型的静态分析方法[10,11].为了获得实用、可行的任务可靠性分析方法,人们通常对实际 PMS 进行各种假定,比如在静态分析中,人们通常假定目标 PMS 中各个部件的失效行为是相互独立且不可维修的.对于实际存在的大量阶段内部件失效行为相互依赖的可维修 PMS,静态分析方法都不能够很好地加以处理,所以,该类分析方法只被用于处理简单的 PMS 或者对复杂 PMS 进行初步分析,而对复杂的 PMS 进行可信度较高的分析都是基于状态空间的动态分析方法.在动态分析方法中,人们通常假定目标 PMS 的阶段持续时间是确定的,阶段内行为是符合齐次马尔可夫过程特性的.这些假定可以极大地简化目标 PMS 的任务可靠性分析.但是,对于实际存在的大量不满足上述假定的更一般的 PMS,即具有随机分布的阶段持续时间和非指数分布的活动的 PMS,已有的方法都无能为力.

本文采用基于状态空间的动态分析方法来对一般 PMS 进行任务可靠性分析.这类 PMS 的阶段持续时间是随机分布的而不是确定的,阶段内行为符合马尔可夫再生过程(Markov regenerative process,简称 MRP)而不是齐次马尔可夫过程,从而允许各个阶段内各种活动所消耗的时间可以满足指数分布、确定分布或者更一般的分布.本文的主要贡献有如下几点:(1) 定义了一个五元组分析模型,该模型能够有效地描述阶段持续时间是随机分布的,阶段内行为特性符合马尔可夫再生过程的一般 PMS;(2) 证明了该分析模型所刻画的 PMS 阶段内随机过程是 MRP,并且讨论了其有效求解的方法;(3) 推导了一般 PMS 任务可靠性分析公式,并利用 Laplace 变换给出了任务可靠性的简化计算方法.

本文第 1 节分析相关工作,并与我们的工作进行比较.第 2 节给出一个应用实例.第 3 节定义一个五元组分析模型.第 4 节给出 PMS 阶段内随机过程分析方法和任务可靠性分析方法.第 5 节针对不同的实际 PMS 讨论分析模型的应用.最后是总结及下一步工作展望.

1 相关工作

基于状态空间的分析模型能够完整、准确地表述可维修 PMS 的动态行为和系统部件在 PMS 运行过程中的各种依赖关系,所以,对于利用这类分析模型分析复杂 PMS 的任务可靠性得到了广泛的研究.通常,为了获得实用、可行的任务可靠性分析方法,人们对目标 PMS 的阶段持续时间和阶段内行为进行一些假定.

比如在阶段持续时间方面,文献[1–5]分析的目标 PMS 的阶段持续时间是确定的.显然,分析确定阶段持续时间 PMS 比分析随机阶段持续时间 PMS 要简单,而且确实存在确定阶段持续时间 PMS,比如航天器 PMS 的各个阶段(如发射、升空、巡航、着陆)的持续时间都是预先设计好的.但是,现实中还存在大量的 PMS,这些系统的阶段持续时间不是预先设计好的,阶段执行是由某些不可预测的事件触发的,阶段的开始时间和结束时间是未知的,所以,对于这些 PMS 的阶段持续时间,实际上是随机分布的.指数分布由于长尾性(long tail)一般不用于刻画阶段持续时间分布.对于一般的随机阶段持续时间分布,文献[6,7]并没有给出 PMS 任务可靠性分析公式,而是利用近似方法或者数值分析方法直接计算可靠性结果.文献[8]在阶段内随机过程是齐次马尔可夫过程的条件下推导了阶段持续时间分布为一般分布的 PMS 任务可靠性分析公式.

在阶段内行为方面,文献[1–6,8]的研究工作都假定阶段内随机过程是齐次马尔可夫过程,即各个阶段内所有活动所消耗的时间都必须满足指数分布.由于对齐次马尔可夫过程存在成熟而有效的数学分析方法,所以,这种假定可以极大地简化 PMS 的任务可靠性分析.然而大部分实际的 PMS 系统都存在非指数分布的活动,一个典型的例子就是维修活动.为了允许阶段内随机过程是更一般的随机过程,文献[7]允许各个阶段内活动所消耗的时间指数分布具有全局时间依赖的参数,从而为整个 PMS 构造了一个连续参数的非齐次马尔可夫过程.但是该

方法的计算代价太大,只能用于极其简单的 PMS.

在已有的研究工作中,只有文献[9]与我们的工作最接近,同时考虑了阶段内随机过程是一般的随机过程和阶段持续时间是随机分布的两种情况.文献[9]利用马尔可夫再生随机 Petri 网(Markov regenerative stochastic petri nets,简称 MRSPN)刻画一般 PMS 的动态行为,通过 PMS 的阶段结构找出各个再生点,再利用这些再生点构造一个巨大的 MRP 描述 PMS 整个生命周期中的行为,通过求解该 MRP 对 PMS 的任务可靠性进行分析.这种方法存在两大问题:1) 没有很好地考虑如何缓解在建模过程中产生的状态爆炸问题;2) 由于 MRP 特有的第二类 Volerra 积分形式 $V(t)=E(t)+\mathrm{d}K*V(t)$求解很困难,广泛应用 MRP 会导致严重的模型求解问题,使得模型只能应用于简单 PMS.与他们的工作比较,我们的分析工作不是基于复杂的 MRSPN,而是基于一个简单的五元组分析模型.在设计该分析模型的过程中,我们采用了状态空间压缩编码和分支矩阵方法,能够更好地缓解状态爆炸问题.同时,在模型求解过程中,只在阶段内过程分析中采用了 MRP 方法并采用 Laplace 变换简化计算,对于任务可靠性分析推导了更为简单的卷积分公式,并进一步利用 Laplace 变换简化计算,从而使得我们的分析模型和分析方法更为有效、实用.

2 实例系统

我们考虑一个 PMS,见表 1,它有 4 个阶段,各个阶段的持续时间是随机分布的.该 PMS 配备有 4 个相同的相互冗余的处理器.对应每个给定的阶段 PMS 有运行配置,*cfg* 是指活动处理器的个数,不用的处理器可以作为冷备份.所有活动处理器都可能会出现故障,而处于冷备份的处理器不会出现故障,活动处理器失效行为是独立的并且失效分布函数是指数分布(λ=0.001).虽然在不同的阶段内处理器的失效率可能是不同的,但是在一个指定的阶段内其失效率是固定不变的.当一个活动处理器失效之后,备份处理器就被激活以代替失效的处理器,使得系统配置保持运行配置.接替行为所需的时间是可以忽略的,并且总是成功.失效处理器在确定时间 τ=1h 内被修复,修复后的处理器可以根据实际情况被激活或者成为冷备份.如果失效的处理器过多,使得 PMS 不能够获得运行配置,则 PMS 失效.

Table 1 Parameters of the example PMS

表 **1** PMS 实例的参数

Phase	Distribution	Parameter value	Mean value	Running configuration	Failure rate
1	Deterministic with value *d*	100	100	*cfg*=3	2λ
2	Negative exponential with rate λ2	0.000 5	200	*cfg*=2	λ
3	2-stage Erlang with rate λ3	0.025	40	*cfg*=3	5λ
4	Uniform within time window [*a*,*b*]	*a*=5,*b*=10	7.5	*cfg*=3	2λ

3 分析模型

在本文中,我们研究的是阶段持续时间是随机分布的并且阶段内行为(具体指的是失效行为和修复行为)允许是一般随机分布的一般 PMS.本节利用一个五元组分析模型来有效地刻画这类 PMS.

通常设计一个模型需要在表达能力和可求解性两者之间进行权衡,我们需要扩充模型允许阶段持续时间是随机的并且阶段内行为是一般随机分布的,同时,为了保证模型能够被有效地求解,我们需要对系统的行为进行一定的约束,即模型假设.另外,基于状态空间的分析模型中一个不可回避的问题就是状态空间爆炸,在设计模型的过程中必须要采用有效的措施来延缓状态爆炸.

3.1 模型假设

每个模型都有其适用范围,明确地给出模型假设有利于模型的研究和比较.比如文献[1–8]或者假设目标 PMS 的阶段持续时间是确定的;或者假设阶段内随机过程是齐次马尔可夫过程.与他们的分析模型相比,我们的分析模型对一般 PMS 的行为采用了更弱的模型假设.

假设 **1**. 对于任意 $s_1,s_2,s_3,s_4\in S,t_1>t_2>t_3\geq 0,prob\{T(s_1,s_2,t_1)|E(s_1,t_2)\wedge S(s_3,t_3)\}=prob\{T(s_1,s_2,t_1)|E(s_1,t_2)\wedge S(s_4,t_3)\}$. 其中,谓词 $T(s_1,s_2,t_1)$表示 PMS 在时刻 t_1 发生从 s_1 至 s_2 的配置转换,谓词 $E(s_1,t_2)$表示 PMS 在时刻 t_2 进入配置 s_1,

谓词 $S(s_3,t_3)$和 $S(s_4,t_3)$表示 PMS 在时刻 t_3 处于配置 s_3/s_4.

假设 1 要求,阶段 i 内 PMS 在进入配置 s 之后的行为与它在进入 s 之前的行为无关.

假设 **2**. 对于任意 $s_1,s_2\in S,t_1,t_2,t\geq 0,prob\{T(s_1,s_2,t_1+t)|E(s_1,t_1)\}=prob\{T(s_1,s_2,t_2+t)|E(s_1,t_2)\}$.其中,谓词 $T(s_1,s_2,t_1+t)$和 $T(s_1,s_2,t_2+t)$表示 PMS 在时刻 t_1+t/t_2+t 发生从 s_1 至 s_2 的配置转换,谓词 $E(s_1,t_1)$和 $E(s_1,t_2)$表示 PMS 在时刻 t_2/t_1 进入配置 s_1.

假设 2 要求,阶段 i 内 PMS 在进入配置 s 之后的行为与它在进入 s 的时刻无关.

假设 **3**. 阶段转换是满足记忆丢失(memory loss)的.

假设 3 要求在前一阶段结束之前,各个未完成转换所消耗的时间或所完成的工作量在新的阶段开始后就全部不计.比如在阶段 i 结束之前 PMS 进入操作配置 s,然后,PMS 启动一项维修活动,试图从 s 转换到另一操作配置 s',但在该维修活动完成之前,阶段 i 结束 PMS 以配置 s 进入新的阶段 i+1,此时,PMS 在阶段 i 内完成的部分维修活动将全部丢弃.

3.2 模型描述

定义 **1**. 一个 PMS 等价于一个 5 元组 $M=\{S,n,C,TPM,F\}$,其中:

- S 是 PMS 的配置空间

所谓的系统配置是系统所有基本部件状态的组合,基本部件是不可细分的简单部件,其状态是二元的或者是正常/可运行或者是失效/不可运行.利用组合编码可以用二进制数来表达配置.PMS 的配置空间 S 包含 PMS 所有可能的配置.比如某个 PMS 有 4 个部件 A,B,C 和 D.该 PMS 的配置空间就包含 16 种可能的配置〈0000〉,〈0001〉,…,〈1111〉.配置〈0000〉表示系统的所有部件都正常,而配置〈1111〉表示系统的所有部件都失效.配置〈0000〉至配置〈1000〉的转换表示部件 A 发生故障;而配置〈1000〉至配置〈0000〉的转换表示部件 A 被修复了.根据上述的编码获得的配置空间是组合爆炸的,即如果 PMS 有 Q 个部件,那么模型的配置空间为 $2^{|Q|}$.

通常在高可靠的 PMS 系统中,一个逻辑部件是由很多同构的冗余物理部件构成,这些同构的物理部件相互进行备份,当某个部件失效之后由其他正常部件代替其执行任务,只有当失效的物理部件数目达到阈值之后逻辑部件才失效.比如,一个可维修的 PMS 是由 2 个同构冗余 A 部件和 3 个同构冗余 B 部件组成,它的配置空间是{(2,3),(2,2),(2,1),(2,0),(1,3),(1,2),(1,1),(1,0),(0,3),(0,2),(0,1),(0,0)}.配置(i,*)至配置(i–1,*)的转换表示一个 A 部件失效,而配置(i–1,*)至配置(i,*)的转换表示一个失效的 A 部件被修复.由于失效事件和修复事件在 PMS 的整个生命周期中都随机出现,所以 PMS 的配置在整个运行过程中不断地发生变换.

根据上述压缩编码方法,我们可以得到如下性质:

性质 **1**. 分析模型的配置空间不是随着冗余部件的增加呈指数增长,而呈线性增加.

显然,当一个 PMS 越复杂,冗余的部件越多,配置空间的精简程度也越大.

- n 是阶段的数目

PMS 的每个阶段都把配置空间 S 分割成两个不相交的集合:操作配置集合 O 和失效配置集合 F.比如阶段 $i(n\geq i\geq 1)$把 S 分割成不相交集合 O_i 和 F_i,即 $S=O_i\cup F_i,O_i\cap F_i=\varnothing$,其中,$O_i$ 中的配置是阶段 i 对应的操作配置(在这些配置上,PMS 可以执行阶段 i 的工作),而 F_i 中的配置是阶段 i 对应的失效配置(在这些配置上,PMS 失效不能执行阶段 i 的工作).需要指出的是,一个操作配置中的所有正常部件并不一定都是运行的,根据 PMS 的具体运行说明,允许部分正常部件作为备份,当某些正在运行的正常部件出现故障时用来接替它们.

对于连续两个阶段 i 和 i+1$(n>i\geq 1)$,O_{i+1} 和 O_i 存在 3 种可能的关系:$O_i\subseteq O_{i+1}$ 或者 $O_{i+1}\subseteq O_i$ 或者$(O_{i+1}\cap O_i)\neq\varnothing$/$O_{i+1}/O_i$.$O_i\subseteq O_{i+1}$ 表示当 PMS 在阶段 i 正常结束的条件下可以直接进入阶段 i+1;而后两种可能性表示当 PMS 在阶段 i 正常结束时,必须处于某些配置下才能够进入阶段 i+1,通常意味着某些必要的部件不能够失效,或者如果失效了必须及时修复好.实际上,$(O_{i+1}\cap O_i)=\varnothing$对于实际 PMS 是不可能的.

为了便于后面叙述,约定 $O_0=S$,并定义一个函数族$\{g_0,g_1,\ldots,g_n\}$.函数 $g_i(n\geq i\geq 0)$把集合 O_i 中每个元素和集合$\{1,2,\ldots,|O_i|\}$中的每个元素一一对应起来,即每个 $o\in O_i,g_i(o)=k,k\in\{1,2,\ldots,|O_i|\}$.函数 g_i 的反函数 g_i^{-1} 把集合

$\{1,2,\ldots,|O_i|\}$中的每个元素和集合 O_i 中每个元素一一对应起来,即每个 $k\in\{1,2,\ldots,|O_i|\}$, $g_i^{-1}(k)=o,o\in O_i$.

- $C=\{C_1,C_2,\ldots,C_n\}$是分支矩阵集合

分支矩阵 $C_i(n\geq i\geq 1)$是$|O_{i-1}|\times|O_i|$的,其每一行对应集合 O_{i-1} 中的一个元素,g_{i-1}/g_i 是行/列号和 O_{i-1}/O_i 之间的映射函数;每一行/列对应集合 O_{i-1}/O_i 中的一个元素.矩阵 C_i 中元素取值方法如下所示:

$$[C_i]_{m,n}=\begin{cases}1, & \text{if } o\in O_i\cap O_{i-1}, g_{i-1}(o)=m, g_i(o)=n\\ 0, & \text{otherwise}\end{cases} \tag{1}$$

- $TPM=\{TPM_1,TPM_2,\ldots,TPM_n\}$是阶段内一步转换概率分布矩阵集合

矩阵 TPM_i 中元素$[TPM_i]_{s,s'}$表示在阶段 i 内从配置 s 到配置 s'的一步转换概率分布函数$(s,s'\in S)$.在对 PMS 进行任务可靠性分析的过程中,我们需要把这些阶段概率分布矩阵耦合起来,所以,这些 TPM_i 必须是同阶的,即$|S|\times|S|$的,其每一行/列对应集合 S 中的一个元素.这样使得 TPM_i 矩阵很大,并且包含了很多与本阶段特性无关的信息,使得分析过程难度加大,复杂性也加大.

通过利用分支矩阵 TPM_i 可以只包含$|O_i|\times|O_i|$个有效元素也能够相互耦合.精简后的 TPM_i 其每一行/列对应集合 O_i 中的一个元素,函数 g_i 是映射函数.矩阵 TPM_i 中元素$[TPM_i]_{m,n}=[TPM_i]_{s,s'}$表示在阶段 i 内从配置 $s=g_i^{-1}(m)$到配置 $s'=g_i^{-1}(n)$的一步转换概率分布函数$(s,s'\in O_i)$.由于阶段 i 内 PMS 在进入配置 s 之后的行为可以是任意的,所以,$[TPM_i]_{s,s'}$可以是任意的概率分布函数,包括指数分布、确定分布和其他一般分布.

- $F=\{f_1,f_2,\ldots,f_n\}$是随机阶段持续时间分布的概率密度函数集合

各个阶段内的概率密度函数是相互独立的.

3.3 实例模型

根据上述定义的分析模型,我们可以为本文实例设计相应的分析模型.由于受篇幅所限,我们省略了模型元素 C 和 F,只给出 S 和 TPM.

- 实例模型的 $S=\{(4),(3),(2),(1),(0)\}$

显然,采用了压缩的配置编码的方法,使得模型的配置空间元素从 2^5 缩减为 5.

- 实例模型的 $TPM=\{TPM_1,TPM_2,TPM_3,TPM_4\}$

$TPM_1=[(1-F_1)^3,3(1-F_1)^2F_1;(1-F_1)^3R,(1-F_1)^3(1-R)]$.

$TPM_2=[(1-F_2)^2,2(1-F_2)F_2,F_2^2;(1-F_2)^2R,(1-F_2)^2(1-R),2(1-F_2)F_2(1-R);$

$(1-F_2)^2R^2,(1-F_2)^2R(1-R),(1-F_2)^2(1-R)^2]$.

$TPM_3=[(1-F_3)^3,3(1-F_3)^2F_3;(1-F_3)^3R,(1-F_3)^3(1-R)]$.

$TPM_4=[(1-F_4)^3,3(1-F_4)^2F_4;(1-F_4)^3R,(1-F_4)^3(1-R)]$.

其中,F_1,F_2,F_3 和 F_4 是参数分别为 $2\lambda,\lambda,5\lambda,2\lambda$的负指数分布,$R$ 是参数为 10 的确定分布.

由于采用了分支矩阵,使得各个 TPM_i 的复杂度并不是固定为$|S|\times|S|$,而是可以随着实际阶段配置的要求进行压缩.

4 模型求解

求解分析模型的任务可靠性就是计算 t 时间内系统完成任务的概率.整个求解过程可以分成两步:

- 阶段内随机过程分析

阶段内随机过程分析的目标是计算阶段 i 内的条件瞬时占有概率矩阵 $V_i(t)$,$V_i(t)$是$|O_i|\times|O_i|$的,其每一行/列对应集合 O_i 中的一个元素,函数 g_i 是映射函数.$V_i(t)$中元素$[V_i(t)]_{m,n}=[V_i(t)]_{s,s'}$是当阶段 i 开始时 PMS 处于 $s=g_i^{-1}(m)$,时间 t 后(t 是在阶段 i 结束之前)PMS 处于 $s'=g_i^{-1}(n)(s,s'\in O_i)$的概率.

- 任务可靠性分析

任务可靠性分析的目标是根据获得的 $V_i(t)$求解 $R(t)$,$R(t)$就是 t 时间内系统完成任务的概率.

4.1 阶段内随机过程分析

性质 **2**. 分析模型所刻画的 PMS 阶段内随机过程是 MRP.

首先简单介绍 MRP 理论.一个随机过程$\{Z(t),t\geq 0\}$如果在时刻 T 满足马尔可夫属性,那么对于任意 $0<t_1<t_2<\ldots<t_k$ 和 $x_1,x_2,\ldots,x_k$,

$$\begin{aligned} &prob\{Z(T+t_1)\leq x_1,Z(T+t_2)\leq x_2,\ldots,Z(T+t_k)\leq x_k \mid Z(T),Z(t),0\leq t<T\}\\ &=prob\{Z(T+t_1)\leq x_1,Z(T+t_2)\leq x_2,\ldots,Z(T+t_k)\leq x_k \mid Z(T)\} \end{aligned} \tag{2}$$

如果一个随机过程$\{Z(t),t\geq 0\}$并不是在整个定义的时间区间内都具有马尔可夫属性,只是在一系列嵌入的时间点$(T_0=0,T_1,\ldots,T_n,\ldots)$上 $Z(t)$才满足马尔可夫属性,那么,该随机过程被称为马尔可夫再生随机过程(MRP).这些嵌入的时间点称为再生时间点.

记$\{X(t),t\geq 0\}$为描述阶段 $i(n\geq i\geq 1)$内系统配置演变的随机过程.$X(t)$在一系列嵌入的时间点$(T_0=0,T_1,\ldots,T_n,\ldots)$上发生配置变化,即在这些时间点上 PMS 发生配置转换.通过分析模型假设 1 和假设 2 可知,阶段 i 内 PMS 在进入配置 s 之后的行为与它在进入 s 之前的行为无关,所以在这些时间点上,$X(t)$是满足马尔可夫属性的.但是由于允许一步转换概率分布可以是一般的非指数的概率分布,所以 $X(t)$并不是在所有的时间点都具有马尔可夫属性.由此可知,阶段 i 内配置演变的随机过程$\{X(t),t\geq 0\}$是 MRP,而且可以证明序列$\{(X(T_i),T_i)\}(i\geq 0)$是马尔可夫更新序列(Markov renewal sequence).

下面我们介绍如何求解 $V_i(t)$.

$$\left[V_i(t)\right]_{s,s'}=prob\{X(t)=s'\,|\,X(0)=s\}=prob\{X(t)=s',T_1>t\mid X(0)=s\}+prob\{X(t)=s',T_1\leq t\mid X(0)=s\} \tag{3}$$

其中,

$$prob\{X(t)=s',T_1\leq t\mid X(0)=s\}=\sum_{k\in O_i}\int_0^t\left[V_i(t-x)\right]_{k,s'}\mathrm{d}prob\{X(T_1)=k,T_1\leq x\mid X(0)=s\} \tag{4}$$

记 $\left[K_i(t)\right]_{s,s'}=prob\{X(T_1)=k,T_1\leq t\mid X(0)=s\}$,而 $\left[E_i(t)\right]_{s,s'}=prob\{X(t)=s',T_1>t\mid X(0)=s\}$,则,

$$\left[V_i(t)\right]_{s,s'}=\left[E_i(t)\right]_{s,s'}+\sum_{k\in O_i}\int_0^t\left[V_i(t-x)\right]_{k,s'}\mathrm{d}\left[K_i(x)\right]_{s,k} \tag{5}$$

以矩阵方式重写

$$V_i(t)=E_i(t)+\mathrm{d}K_i*V_i(t) \tag{6}$$

通常,称矩阵 K_i 为全局核心(global kernel)矩阵,刻画了阶段 i 内 MRP 过程在紧接着下一个再生时间点之后的行为,而称矩阵 E_i 为局部核心(local kernel)矩阵,刻画了阶段 i 内 MRP 过程在两个再生时间点之间的行为.

由于阶段 i 内配置演变的随机过程$\{X(t),t\geq 0\}$是 MRP,并且 $X(t)$的所有配置发生变化的时刻都是再生时间点,所以在两个再生时间点之间 $X(t)$是不发生变化的.由此可以得到下面的计算方法:

$$\left[E_i(t)\right]_{s,s'}=prob\{X(t)=s',T_1>t\mid X(0)=s\}=\begin{cases}0, & \text{if } s\neq s'\\ [TPM_i]_{s,s'}, & \text{if } s=s'\end{cases} \tag{7}$$

由于对 $X(t)$所有配置发生变化的时刻都是再生时间点,所以,只有配置发生变化才能到达下一个再生时间点.由此得到下面的计算方法:

$$\left[K_i(t)\right]_{s,s'}=prob\{X(T_1)=k,T_1\leq t\mid X(0)=s\}=\begin{cases}0, & \text{if } s=s'\\ [TPM_i]_{s,s'}, & \text{if } s\neq s'\end{cases} \tag{8}$$

显然,直接对矩阵积分等式(6)求解来计算 $V_i(t)$,计算量代价太大,除非是极其简单的 PMS,否则,该方法不能采用[12,13].我们可以利用 Laplace 变换按照以下步骤简化 $V_i(t)$的求解:

(1) 根据 TPM_i,利用式(7)和式(8),计算矩阵 $K_i(t),E_i(t)$.

(2) 利用 Laplace 变换计算 $LTK_i(s)=\int_0^\infty \mathrm{e}^{-st}\mathrm{d}K_i(t)$, $LTE_i(s)=\int_0^\infty \mathrm{e}^{-st}E_i(t)\mathrm{d}t$.

(3) 解线性方程系统:$[\boldsymbol{I}-LTK_i(s)]LTV_i(s)=LTE_i(s)$,求得 $LTV_i(s)$.

(4) 对 $LTV_i(s)$求逆得 $V_i(t)$.

步骤(1)可以直接实现.步骤(2)的计算复杂性与矩阵 K_i 及 E_i 中元素的复杂性有关,对于简单的元素,可以通

过查找 Laplace 变换表直接计算;对于复杂的函数,可以利用数学软件(如 Matlab)编程实现.步骤(3)可以直接利用数学软件实现矩阵除.对于步骤(4),如果获得的 $LTV_i(s)$中的元素较为简单,可以通过查找逆 Laplace 变换表直接计算 $V_i(t)$;如果 $LTV_i(s)$中的元素复杂,不能直接计算,可以利用 Laplace 数值逆求解算法[14,15]对 $LTV_i(s)$求数值逆,并对结果进行拟合得到 $V_i(t)$.

4.2 求解任务可靠度

记$\{X(t),t\geq 0\}$为在 PMS 整个运行过程中系统配置演变的随机过程.定义一个$|O_1|\times|O_n|$的矩阵 $P(t)$,其每一行/列对应集合 O_1/O_n 中的一个元素,函数 g_1/g_n 是映射函数.矩阵 $P(t)$中元素$[P(t)]_{m,n}=[P(t)]_{s,s'}$表示,当 $t=0$ 时 PMS 处于配置 $s=g_1^{-1}(m)(s\in O_1)$,时间 t 后 PMS 执行系统任务完毕停止在配置 $s'=g_n^{-1}(n)(s'\in O_n)$的概率.利用初始配置概率分布为 $\boldsymbol{V}(0)$(行向量),$P(t)$,分支矩阵 C_1,我们可以通过式(8)计算在初始配置概率分布为 $\boldsymbol{V}(0)$时 PMS 的任务可靠度 $R(t)$.

$$R(t)=\boldsymbol{V}(0)C_1P(t)\boldsymbol{I} \tag{9}$$

其中,$\boldsymbol{I}$ 是$|O_n|\times 1$ 的元素全为 1 的列向量.

分析 PMS 的任务可靠度的关键就是计算 $P(t)$.首先我们来看两个特殊 PMS 的 $P(t)$计算.

对于单阶段 PMS,利用 $V_1(t)$和 $f_1(t)$,通过下面的计算公式可以求得矩阵 $P(t)$,$P(t)$中的任意元素.

$$\left[P(t)\right]_{s,s'}=prob\{X(T_1)=s',T_1\leq t\mid X(0)=s\}=\int_0^t\left[V_1(x)\right]_{s,s'}f_1(x)\mathrm{d}x \tag{10}$$

对于两阶段 PMS,利用 $V_1(t)$,$V_2(t)$和 $f_1(t)$,$f_2(t)$,通过下面的计算公式可以求得矩阵 $P(t)$中的任意元素.

$$\left[P(t)\right]_{s,s'}=prob\{X(T_2)=s',T_1+T_2\leq t\mid X(0)=s\}=\sum_{k\in O_2}\int_0^t\int_0^{t-x}\left[V_1(x)\right]_{s,k}\left[V_2(y)\right]_{k,s'}f_1(x)f_2(y)\mathrm{d}y\mathrm{d}x \tag{11}$$

以矩阵方式重写:

$$P(t)=\int_0^t\int_0^{t-x}V_1(x)C_2V_2(y)f_1(x)f_2(y)\mathrm{d}y\mathrm{d}x \tag{12}$$

以此类推,对于 n 阶段系统我们通过下面的计算公式可以求得矩阵 $P(t)$.

$$P(t)=\int_0^t\int_0^{t-x_1}\cdots\int_0^{t-x_1-\cdots-x_{n-1}}V_1(x_1)C_2V_2(x_2)C_3\cdots C_nV_n(x_n)f_1(x_1)f_2(x_2)\cdots f_n(x_n)\mathrm{d}x_n\cdots\mathrm{d}x_2\mathrm{d}x_1 \tag{13}$$

显然,利用式(9)和式(13)分析 PMS 的任务可靠性,计算量太大,只适合分析阶段结构简单的 PMS.下面我们介绍利用 Laplace 变换方法简化任务可靠性计算,从而能够分析复杂 PMS 的任务可靠性.

首先我们定义一个矩阵族$\{U_1,U_2,\ldots,U_n\}$.矩阵 $U_i(n\geq i\geq 1)$是$|O_i|\times|O_i|$的,其每一行/列对应集合 O_i 中的一个元素,函数 g_i 是映射函数,并且矩阵 $U_i(t)$中元素$[U_i(t)]_{m,n}=[U_i(t)]_{s,s'}$,其中 $s=g_i^{-1}(m)$,$s'=g_i^{-1}(n)(s,s'\in O_i)$的定义如下:

$$\left[U_i(t)\right]_{s,s'}=prob\{X(T_i)=s',T_i\leq t\mid X(T_{i-1})=s\}=\int_0^t\left[V_i(x)\right]_{s',s}f_i(x)\mathrm{d}x=\int_0^t u_i(x)\mathrm{d}x \tag{14}$$

重新推导两阶段 PMS 的 $P(t)$计算方法.

$$\begin{aligned}\left[P(t)\right]_{s,s'}&=prob\{X(T_2)=s',T_1+T_2\leq t\mid X(0)=s\}\\&=\sum_{k\in O_2}\int_0^t prob\{X(T_2)=s',T_2\leq t-x\mid X(T_1)=k\}\mathrm{d}prob\{X(T_1)=k,T_1\leq x\mid X(0)=s\}\end{aligned} \tag{15}$$

用矩阵形式重写公式(15),得

$$P(t)=(U_1C_2)*u_2 \tag{16}$$

依此类推,n 阶段 PMS 的 $P(t)$计算方法:

$$P(t)=((\ldots(((U_1C_2)*u_2)C_3)*u_3\ldots*u_{n-1})C_n)*u_n \tag{17}$$

显然,我们可以利用 Laplace 变换把等式(17)转化为线性方程组进行求解,从而使得 $P(t)$的计算过程得到简化.根据这个思路,我们给出利用 Laplace 变换分析 PMS 任务可靠性的简化方法.

(1) 利用 $V_i(t)$和 $f_i(t)$,$n\geq i\geq 1$,利用公式(14)计算矩阵 $U_1(t)$,$u_i(t)$.

(2) 利用 Laplace 变换计算 $LTU_1(s)=\int_0^\infty \mathrm{e}^{-st}U_1(t)\mathrm{d}t$,$LTu_i(s)=\int_0^\infty \mathrm{e}^{-st}u_i(t)\mathrm{d}t$.

(3) 解线性方程系统:$LTP(s)=LTU_1C_2LTu_2C_3LTu_3\ldots LTu_{n-1}C_nLTu_n$,求得 $LTP(s)$.

(4) 对 $LTP(s)$求逆得 $P(t)$,然后利用公式(9)计算任务可靠度 $R(t)$.

步骤(1)可以直接实现.步骤(2)的计算复杂性与 u_i 的复杂性有关,对于简单的 u_i,可以通过查找 Laplace 变换表直接计算;对于复杂 u_i,可以利用数学软件编程计算.步骤(3)可以直接利用数学软件实现矩阵乘.步骤(4)可以利用 Laplace 数值逆求解算法对 $LTP(s)$求 t 时刻的数值逆,然后直接计算 $R(t)$.

5 模型应用分析

前面我们给出了分析模型及其求解方法,本节讨论分析模型所涉及的 3 个假设与模型的应用之间的关系.

对于很多部件来说,其整个生命周期的失效率特征可以分成 3 个阶段:磨合阶段、稳定阶段和老化阶段.在磨合阶段和老化阶段中部件的失效率很大,而在稳定阶段部件失效率是稳定的.通常,PMS 是从稳定阶段开始配置使用的,许多类型的部件(如电子部件)要经过很长的时间才能达到老化阶段,而 PMS 的工作时间相对来说比较短(如本文的实例 PMS 的平均工作时间是<300h),所以部件在工作时间内的失效行为和修复行为可以看作是稳定的,与其历史无关的.所以假设 1 和假设 2 具有其合理性.应该指出,在一些极其特殊应用下的 PMS(如无人空间探测器)其工作寿命会很长,这些 PMS 的工作后期由于部件进入了老化期,假设 1 和假设 2 将会影响可靠性分析结果的精确性.

假设 3 要求在前一阶段结束之前各个未完成转换所消耗的时间或所完成的工作量在新的阶段开始后就全部不计.如果一般 PMS 的阶段转换确实满足记忆丢失,如 Scheduled Maintenance Systems 就是该类 PMS.另外,如果 PMS 各个阶段内所有活动的时间分布都呈指数分布,则该 PMS 的阶段转换也满足记忆丢失;对于这些 PMS 分析出的结果就是实际结果.如果一般 PMS 包含的所有失效活动都符合指数分布,但是维修活动符合非指数分布(如本文给出的 PMS 实例),并且在阶段转换之后维修活动是继续下去直至完成.那么阶段转换记忆丢失就可能把已经做的部分维修工作忽略,从而使 PMS 的维修行为比实际情况要慢,计算所得的任务可靠度是一种悲观的近似,是一个下限.为了获得这类 PMS 任务可靠度的上限,我们可以对分支转换矩阵 $C=\{C_1,C_2,\ldots,C_n\}$进行定制,通过强制的配置转换,使前一阶段未完成的维修工作提前完成.图 1 给出了本文 PMS 实例任务可靠性的上下限分析,实际的结果应该处于中间所夹的区域内.由于实例中的活动处理器的失效率(0.001/h)很小而失效处理器的修复时间很短(1h),所以上下限比较接近,所夹的区间很小,如果我们提高失效率并延长修复时间,上下限的差距就会被拉大.

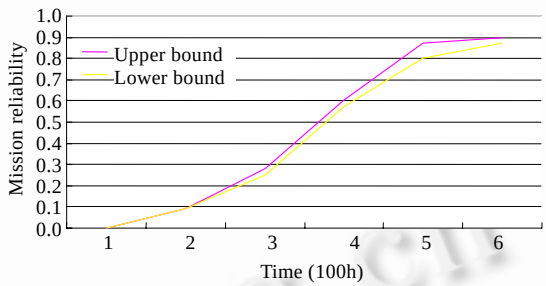

Fig.1 Bounds analysis of reliability of the example PMS

图 1 实例 PMS 系统的任务可靠性上下限分析

6 结束语

本文研究一般 PMS 的任务可靠性分析.首先给出一个五元组分析模型,该模型能够有效地描述阶段持续时间是随机分布的,阶段内行为特性符合马尔可夫再生过程的一般 PMS.为了降低计算复杂度,分析模型的求解过程由两个步骤组成:首先利用马尔可夫再生过程理论,给出一般 PMS 的阶段内随机过程分析公式和简化计算方法;然后给出一般 PMS 任务可靠性分析公式和简化计算方法.应用本文给出的分析模型和求解方法可以有效地对一般 PMS 进行可靠性分析.

根据本文的分析模型构成 PMS 的基本部件的状态是二元的:或者正常或者失效.如实例中的处理器都是经过 Fail-stop 设计的.当 PMS 规模很大时,只考虑基本部件会导致分析模型的配置空间太大而很难进行分析,考虑粗粒度的部件是不可避免的.所以在下一步工作中,需要对分析模型和分析方法进行扩展,使之能够处理具有灰色状态的系统部件.另外,我们需要考虑是否能够进一步弱化模型假设,使得模型的描述能力更强.同时,研究模

型求解算法的新技术,使得模型能够更有效地被求解,扩大分析问题的空间.

致谢 本文的评审专家为本文的完善提出了许多宝贵意见,在此我们深表感谢.

References:

[1] Bondavalli A, Mura I, Nelli M. Analytical modelling and evaluation of phased-mission systems for space applications. In: Paul R, Han JC, eds. Proc. of the IHASE'97. Washington: IEEE Computer Society Press, 1997. 85−91.

[2] Dugan JB. Automated analysis of phased-mission reliability. IEEE Trans. on Reliability, 1991,40(1):45−52.

[3] Mura I, Bondavalli A, Zang X, Trivedi KS. Dependability modelling and evaluation of phased mission systems: A DSPN approach. In: Weinstock CB, Rushby J, eds. Proc. of the DCCA-7. San Jose: IEEE Computer Society Press, 1999. 319−337.

[4] Bondavalli A, Mura I, Chiaradonna S, Filippini R, Poli S, Sandrini F. DEEM: A tool for the dependability modeling and evaluation of multiple phased systems. In: Smith TB, Blough D, Kanoun K, eds. Proc. of the FTCS-30 and DCCA-8. Washington: IEEE Computer Society Press, 2000. 231−236.

[5] Bondavalli A, Chiaradonna S, Di Giandomenico F, Mura I. Dependability modeling and evaluation of multiple-phased systems using DEEM. IEEE Trans. on Reliability, 2004,53(4):509−522.

[6] Somani AK, Ritcey JA, Au SHL. Computationally-Efficent phased-mission reliability analysis for systems with variable configurations. IEEE Trans. on Reliability, 1992,41(4):504−511.

[7] Smotherman M, Zemoudeh K. A non-homogeneous Markov model for phased-mission reliability analysis. IEEE Trans. on Reliability, 1989,38(5):585−590.

[8] Kim K, Park KS. Phased-Mission system reliability under Markov environment. IEEE Trans. on Reliability, 1994,43(2):301−309.

[9] Mura I, Bondavalli A. Markov regenerative stochastic Petri nets to model and evaluate phased mission systems dependability. IEEE Trans. on Computers, 2001,50(12):1337−1351.

[10] Zang X, Sun H, Trivedi KS. A BDD-based algorithm for reliability evaluation of phased mission systems. IEEE Trans. on Reliability, 1999,48(1):50−60.

[11] Xing L, Dugan JB. Comments on PMS BDD generation in 'A BDD-based algorithm for reliability analysis of phased-mission systems'. IEEE Trans. on Reliability, 2004,53(2):169−173.

[12] Choi H, Kulkarni VG, Trivedi KS. Markov regenerative stochastic Petri nets. Performance Evaluation, 1994,20(1-3):335−357.

[13] German R, Logothetis D, Trivedi KS. Transient analysis of Markov regenerative stochastic Petri nets: A comparison of approaches. In: Trivedi KS, ed. Proc. of the 6th Int'l Workshop on Petri Nets and Performance Models. Kyoto: IEEE Computer Society Press, 1995. 103−112.

[14] Abate J, Valko PP. Multi-Precision Laplace transform inversion. Int'l Journal for Numerical Methods in Engineering, 2004,60(5-7): 979−993.

[15] Valko PP. Comparison of sequence accelerators for the Gaver method of numerical Laplace transform inversion. Computers and Mathematics with Applications, 2004,48(3-4):629−636.

莫毓昌(1980－),男,浙江湖州人,博士生,主要研究领域为高可靠计算,可信开发方法.

崔刚(1947－),男,教授,博士生导师,CCF高级会员,主要研究领域为高可靠计算,嵌入式系统设计,汽车电子.

杨孝宗(1939－),男,教授,博士生导师,CCF高级会员,主要研究领域为高可靠计算,移动计算,穿戴机.

刘宏伟(1971－),男,博士,副教授,CCF 高级会员,主要研究领域为高可靠计算,软件可靠性分析.