航天资源规划与调度

大型可修航天测控系统可靠性分析方法研究

Reliability Analysis of Repairable Phased-Mission Systems using Modular Methods

吕济民 陈盈果 刘晓路 姚 锋 著

清華大學出版社
北 京

内 容 简 介

本书面向航天测控系统在可靠性评估时面临的结构可变、规模庞大难题，分析探讨了“多阶段任务系统模型”的优缺点及国内外研究成果。此外，本书针对中等规模和大规模系统的可靠性评估问题，分别论述了行为向量方法，基于行为向量与截断算法的混合算法，以及基于行为向量的抽样算法，其中行为向量方法是后两种方法的基础，混合算法适用于部件多但阶段少的系统，抽样算法适用于同时含大量部件和大量阶段的系统，三种方法都适用于部件可修的多阶段任务系统。本书提出的一系列方法有效地解决了一些经典文献中绕不开的计算量爆炸问题。本书的研究成果不仅可应用于我国航天测控通信系统的可靠性评估，也可应用于诸如运输系统、航班部署等真实工程应用的可靠性评估。

本书适合作为管理科学与工程及遥感应用领域相关专业的高年级本科生及研究生教材，也可作为从事大型系统可靠性分析技术研究的科研工作者的参考书。

图书在版编目(CIP)数据

大型可修航天测控系统可靠性分析方法研究/吕济民等著.—北京：清华大学出版社，2023.11

(航天资源规划与调度)

ISBN 978-7-302-64859-8

Ⅰ.①大… Ⅱ.①吕… Ⅲ.①航天测控—系统可靠性—研究 Ⅳ.①V556

中国国家版本馆 CIP 数据核字(2023)第 217132 号

责任编辑：陈凯仁
封面设计：刘艳芝
责任校对：欧 洋
责任印制：曹婉颖

出版发行：清华大学出版社
网 址：https://www.tup.com.cn，https://www.wqxuetang.com
地 址：北京清华大学学研大厦 A 座 **邮 编**：100084
社 总 机：010-83470000 **邮 购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：天津鑫丰华印务有限公司
经 销：全国新华书店
开 本：170mm×240mm **印 张**：8 **字 数**：159 千字
版 次：2023 年 12 月第 1 版 **印 次**：2023 年 12 月第1 次印刷
定 价：65.00 元

产品编号：101253-01

《航天资源规划与调度》编辑委员会

（2021 年 7 月）

丛书序言

FOREWORD

2021年9月15日，习近平总书记在驻陕西部队某基地视察调研时强调，太空资产是国家战略资产，要管好用好，更要保护好。人造地球卫星作为重要的太空资产，已经成为获取天基信息的主要平台，天基信息是大国博弈制胜的利器之一，也是各科技强国竞相角力的主战场之一。随着“高分辨率对地观测系统”“第三代北斗卫星导航系统”等国家重大专项工程建设及民营、商业航天产业的蓬勃发展，我国卫星呈“爆炸式”增长，为社会、经济、国防等重要领域提供了及时、精准的天基信息保障。

另外，受卫星测控站地理位置限制，我国卫星普遍存在的入境时间短、测控资源紧缺等问题日益突出；突发自然灾害、军事斗争准备等情况下的卫星应急响应已成为新常态；随着微电子、小卫星等技术的快速发展，卫星集成度越来越高、功能越来越多，卫星已具备一定的自主感知、自主规划、自主协同、自主决策能力，传统地面离线任务规划模式已无法适应大规模多功能星座发展和协同、高时效运用的新形势。这些问题都对卫星管控提出了新的更高要求。在此现状下，为应对飞速增长的卫星规模、有限的管控资源和应急响应的新要求，以现代运筹学和计算科学为基础的航天资源调度技术起到至关重要的作用，是保障卫星完成多样化任务、高效运行的关键。

近年来，在诸多学者与航天从业人员的推动下，航天资源调度技术取得了丰富的研究成果，在我国“北斗”“高分”“高景”等系列卫星为代表的航天资源调度系统中得到长期的实践与发展。目前，国内已出版了多部航天领域相关专著，但面向近年来发展起来的敏捷卫星调度、大规模多星协同、空天地资源协同调度、自主卫星在线调度等新问题，仍然缺乏详细和系统的研究和介绍。本套丛书涵盖航天资源调度引擎、基于精确算法的航天资源调度、基于启发式算法的航天资源调度、空天地资源协同调度、航天影像产品定价、面向应急救援的航天资源调度、航天资源调度典型应用等众多内容，力求丰富航天资源调度领域前沿研究成果。

本套丛书已有数册基本成形，也有数册正在撰写之中。相信在不久以后会有不少新著作出现，使航天资源调度领域呈现一片欣欣向荣、繁花似锦的局面，这正是丛书编委会的殷切希望。

丛书编委会

2021年7月

前言

PREFACE

卫星测控系统是航天工程的一个重要组成部分，其可靠性直接关系到航天工程的成败。而我国测控通信系统的可靠性度量目前仍停留在定性为主，定量为辅的状态，无法对系统顶层设计提供相关技术支撑。由于航天工程要求高、投入大，后续任务的建设规模相比前期任务进一步扩大，系统设计的不精确可能造成经费投入的低效率及可靠性指标分配的不合理，为了使系统设计及建设更具科学性和合理性，对测控通信系统可靠性的定量化研究十分必要。

国内对于卫星测控系统的可靠性设计与分析，主要是基于经典的单元/系统可靠性分析理论进行的。GJB/Z 66—1994《航天测控系统总体设计指南》以经典可靠性理论为基础，给出了测控与通信系统的可靠性设计、试验与评价要求。在《航天测控系统工程》中以经典系统可靠性设计与分析理论为基础，介绍了串联、并联、混联、备份等系统的可靠性预计与分配技术。历史文献的可靠性评估方法有一个较为明显的缺陷：无法应用到大规模的、内部结构随时间改变的工程应用系统。

多阶段任务系统(phased mission systems，PMS)是描述可变工程系统的经典模型，PMS的可靠性分析是相关系统寿命分析的基础，在产品设计和维修预测等领域有着广泛应用。随着工程系统朝着大型化、复杂化演变，PMS模型也呈现出规模愈发庞大的发展趋势，这给现有的PMS可靠性分析方法带来了相当大的挑战。针对大型PMS阶段多、可修部件多的特点，本书提出了三种解析方法分析PMS的可靠性。

本书的主要内容分为四部分，分别提出了三种PMS的可靠性估算方法。本书论述的第一种方法是用于分析广义可修PMS可靠性的行为向量方法。所谓广义PMS是指不要求任务在每个阶段都成功，行为向量方法可应用于估算含大量可修部件和少量阶段PMS的可靠性。本书论述的第二种方法在行为向量方法的基础上融合了截断策略，使行为向量方法能够有效应用于含大量部件但阶段数较少的中等规模PMS。本书称该方法为混合算法。本书论述的第三种方法是分析大型PMS可靠性的抽样方法。抽样方法提出了离散时间可用度的概念，并通过增加离散抽样点，使离散时间可用度逐步逼近PMS可靠性真值，这种离散化抽样的思路为系统可靠性评估提供了新的解决方案。

本书的主要特色在于书中论述的三种方法能够有效评估中大规模可修PMS

可靠性，特别是第三种抽样方法能够有效应用于同时含大量可修部件、大量阶段的广义 PMS，对诸如卫星测控系统等变结构系统的任务可靠性评估有重大意义。本书适合作为管理科学与工程及遥感应用领域相关专业的高年级本科生及研究生教材，也可作为从事大型系统可靠性分析技术研究科研工作者的参考书。

本书是笔者在国防科技大学系统工程学院求学与工作期间完成的。本书的完成离不开笔者导师武小悦教授的悉心指导，以及团队同事陈英武、贺仁杰、姚锋、刘晓路、陈盈果、张忠山、陈宇宁、何磊、杜永浩的大力支持和指导。本书在撰写过程中参考了许多参考文献，本书的完成也离不开这些学者的贡献和启发。笔者在此向所有给予指导、帮助与启发的各位老师与学者表示衷心感谢。由于笔者水平有限，书中难免存在不妥与待完善之处，欢迎专家学者和读者朋友批评指正，提出宝贵意见，笔者将不胜感激。

著　者

2023 年 6 月于长沙

目录

C O N T E N T S

第1章

绪 论

1.1 研究背景及意义

可靠性是评价产品质量好坏、评价产品寿命的一个重要指标。国际标准化组织将可靠性定义为单元在给定的环境、给定时间内完成规定功能的能力[1]。可靠性作为专门课题来研究起源于第二次世界大战期间[2]，当时各国的武器装备在特殊战场环境下均出现不同程度的故障，不同程度地损害了部队的作战效能，这一问题促使人们开始了早期的可靠性研究。从20世纪60年代开始，可靠性研究逐步拓展到维修性、保障性等领域。随着科学技术的不断发展，可靠性研究在20世纪70年代步入成熟阶段，到20世纪80年代进入深化发展阶段。可靠性研究作为提高产品寿命和系统效能的一种有效途径，逐渐受到了各个国家、各个部门的重视。

随着军事科技水平和工程复杂度的提高，系统可靠性的建模与分析显得愈加重要。现代工程系统大多数是多功能的自动化系统，由于系统功能越来越复杂，系统使用的元器件数量越来越多。在这种情况下，如果不加强系统可靠性的控制，系统使用寿命就会逐渐下降，甚至影响任务达成，造成经济损失。目前，我国部分领域产品尚未打入欧美市场，其中一个原因是产品的可靠性较低。为实现制造业转型，对系统和产品进行可靠性预计和管理显得至关重要，同时这也是系统设计过程中必不可缺的环节，是通往高品质和高端制造的必由之路[3]。另外，可靠性预计也为大型系统的维修保障工作提供了数据基础，是保证使命任务达成，保障人员生命安全的重要依托。

现代科技的迅速发展使工程产品和系统结构越来越复杂，规模也越来越庞大，构成产品的元器件越来越多，产品需要在多变的工作环境和压力下运行，这些问题为系统可靠性分析带来了巨大的挑战。近年来，一个新的概念——多阶段任务系统(phased-mission systems，PMS)成为描述该类复杂系统的有效手段[4]。顾名思义，相对于传统的单阶段系统，PMS包含多个不重叠的阶段。由于执行任务和环

境压力的变化，系统结构会按时间顺序划分为各个不同的阶段，具有这类特点的系统均可称为 PMS。例如，卫星发射测控系统就是一个典型的 PMS。卫星发射测控任务通常包含火箭发射、火箭分离、卫星入轨三个测控阶段。这三个阶段互不重叠，按时间先后顺序依次出现。在不同阶段，测控系统利用不同设备执行测控任务，某些设备可能在发射阶段使用频繁，而在入轨阶段完全闲置，这构成了三阶段的 PMS。PMS 的例子还有很多，例如，飞行辅助系统包括起飞升空、巡航、下降着陆等阶段。在许多工程领域，PMS 可用于描述系统结构随时间改变，或部件参数随时间改变的系统。

近年来，PMS 可靠性的建模和分析受到学界的广泛关注。为了简化模型，PMS 建模过程通常提出“阶段时间固定”和“阶段顺序确定”这两个假设。“阶段时间固定”和“阶段顺序确定”假设广泛存在于固定规程、预定任务的工程应用中。例如，对于高铁列车速度监控系统，列车到站和出发加速是严格遵循调度表实施的，这两个假设存在合理性。对于航天任务，每个阶段的捕捉、跟踪、测控、释放任务都是预先计划好的，存在合理性，本书第 2～4 章中的 PMS 可靠性分析方法均基于这两个假设。

另外，“部件工作和维修时间服从指数分布”的假设也广泛存在于 PMS 模型中，特别是考虑可修部件的 PMS 模型通常都包含该假设。众所周知，系统可靠性分析的一个重要目的是研判系统结构的合理性，部件参数分布对可靠度结果的影响并不是主要的。当部件工作和维修时间服从一般分布时，计算可靠性的更新过程推导极为复杂。“部件寿命服从指数分布”假设的主要目的是充分利用随机过程中的连续时间马尔可夫链（continuous time markov chains，CTMC）理论[5]，避免繁杂的微分方程组推导，有助于提高算法的简洁性和可操作性。本书第 2～4 章提出的 PMS 可靠性分析方法均基于这一假设展开讨论。

部件的可修性是可靠性分析中必须考虑的一个因素。在诸多工程领域中，可快速拆换的模块化设备均可视为可修部件。通常来说，可修 PMS 既可以指包含可修部件的 PMS，也可指 PMS 失效崩毁后因继续维修而恢复的系统。因为可靠性分析的目的是计算系统首次故障时间，不考虑系统在失效崩毁后的情况，所以本书第 2～4 章讨论的可修系统单指包含可修部件的 PMS。

除了可修部件，部件状态的跨阶段依存性（s-dependence）也为 PMS 可靠性分析带来了相当大的挑战。部件的跨阶段依存性是指一个部件在新阶段的初始状态依赖于部件在前一阶段的行为。当同一部件出现在 PMS 不同阶段时，就会产生跨阶段依存性问题。由于跨阶段依存性问题，PMS 的可靠性不等于各阶段可靠性的简单乘积，这是 PMS 可靠性分析的基本难点之一。此外，一些特定的工程领域还存在诸如不完全覆盖（imperfect coverage，IPC）、共因失效（common cause failure，CCF）等问题，这些特殊情况进一步增加了 PMS 可靠性分析的难度。

目前，现代工程系统正在朝着大型化、复杂化的方式演变。PMS 作为现代工

程系统的描述工具，也存在着模型规模庞大、结构复杂的发展趋势。大型 PMS 有部件数量多、阶段多、部件嵌套子系统的特点。如何计算大型 PMS 的可靠度，是可靠性理论分析的研究热点，也是亟待解决的工程实践问题。特别是航天测控系统具有规模庞大、设备可修等特点，研究大型可修 PMS 的可靠性分析方法，能够为我国航天事业的健康发展提供重要保障。

本书面向上述需求，论述了三种可靠性分析方法：

1. 分析广义可修 PMS 可靠性的行为向量方法

广义 PMS 与普通 PMS 的主要区别是：如果广义 PMS 要成功完成任务，不要求系统在每个阶段都成功，因此这对广义 PMS 的可靠性分析构成了一定挑战。行为向量方法是一种评估广义可修 PMS 可靠度的解析方法，它主要应用于包含大量部件和少量阶段的可修 PMS。该方法不仅可以分析广义 PMS，还能规避状态爆炸问题和二元决策图变量排序问题，是一种运算复杂度低且易于编程实现的可靠性分析手段。

2. 分析中型 PMS 可靠性的行为向量与截断策略混合算法

针对 PMS 阶段增多时行为向量方法将遭遇计算量爆炸的问题，本书设计了递减的截断策略，用以删除权重低的计算单元并得出 PMS 可靠度的近似值。截断策略可以在系统阶段增多时显著减少算法内存消耗，并降低运算耗时，是将行为向量方法拓展到中型 PMS 的有效手段。截断策略应用了递减的截断阈值，将截断误差直接控制在预定参数下，避免了经典截断方法中探讨误差的烦琐步骤。

3. 分析大型 PMS 可靠性的抽样方法

在 PMS 规模增大时，大部分解析方法都将遭遇计算量爆炸的问题。针对这一问题，本书设计了分析大型系统的抽样方法，主要应用于含大量阶段和大量可修部件的 PMS。该方法提出了离散时间可用度的概念，并基于此设计了新的 PMS 可靠度评估方法。这种方法将离散时间可用度作为 PMS 可靠度的近似值，并通过离散化程度加深来逐渐逼近可靠度真值。这种离散化抽样的思路为系统可靠性评估提供了新的解决方案。

本书提出的系统可靠性分析评估方法，还能够应用于具有如下特征的其他工程应用系统：①任务到达时间随机性。例如在中高轨卫星的测控任务无法明确具体时间要求，只能大致描述任务的时间范围或执行次数。②系统内部的部件允许备份和快速更换。在系统可靠性分析中，设备的备份策略在很大程度上会影响到系统任务可靠性，不同的备份策略对系统可靠性建模与分析会产生不同的影响。③系统可靠性分析的周期长，计算量大。根据工程上常用的调度算法，通常是以周为单位进行测控调度的，即每次生成一周的调度方案，在下个周期内按照预定的调度方案进行卫星的测控，其间再针对卫星系统运行过程中的突发情况（如卫星故障、测控设备故障等）进行测控调度方案的微调，而一周内测控任务达到上万个，涉

及的测控系统部件达几万件，导致任务可靠性的分析计算量很大。④其他对系统结构造成影响的动态不确定性。在测控系统的运行过程中，由于一些偶发事件的影响，如测控设备故障、卫星应急抢修等事件，导致难以一次性建立固定的可靠性模型，模型需要针对故障的发生进行动态调整，从而难以开展全过程的可靠性分析评估。

1.2 国内外研究综述

1.2.1 PMS 可靠性建模与分析方法综述

从公开文献上看，PMS 可靠性建模与分析的研究始于 20 世纪 70 年代，Esary 等[4]及 Burdick 等[6]较早地提出了 PMS 的概念。总体来说，现有的 PMS 可靠性分析方法主要基于成熟经典的可靠性分析理论，针对 PMS 的特点逐步改进而来。按照建模能力，PMS 可靠性分析方法可分为静态方法和动态方法，如图 1.1 所示。静态方法主要用于分析不可修 PMS，而动态方法用于分析可修 PMS。静态方法主要包括可靠性框图(reliablity block diagram，RBD)、静态故障树(static fault tree)、二元决策图(binary decision diagram，BDD)、布尔代数(Boolean algebra)、贝叶斯网络(Bayesian network)等；动态方法包括动态故障树、齐次马尔可夫链、Petri 网仿真等模型。

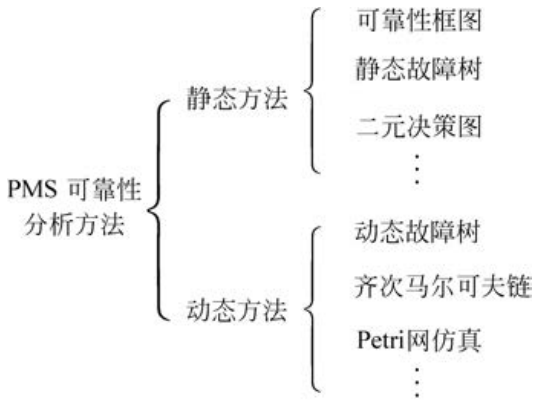

图 1.1 PMS 可靠性分析方法按建模能力的分类

按照模型使用的数学理论，PMS 可靠性分析方法可分为解析方法(analytical methods)和仿真方法，其中解析方法又可分为组合模型方法(combinatorial model methods)、马尔可夫链方法(markov chain methods)和两者相结合的模块化方法(modular method)，如图 1.2 所示。

在这些方法中，仿真方法适用范围最广，方法假设少，对各类复杂工程问题的建模能力最强。仿真方法主要包括蒙特卡罗仿真、离散事件仿真、Petri 网仿真等。马尔可夫链方法基于随机过程中的连续时间马尔可夫链理论，它的主要优点在于分析部件的维修性。组合空间方法虽然难以分析可修部件，但可有效规避状态空

图 1.2 PMS 可靠性分析方法按数学理论的分类

间方法遭遇的状态爆炸问题(state-explosion problem)。组合模型方法主要包括布尔代数、可靠性框图、静态故障树、二元决策图等模型。

本书第 2～4 章研究的重点是解析方法中的模块化方法,模块化方法又称为层次化方法(hierarchical methods)。学者提出模块化方法的主要目的是分析大型可修 PMS 的可靠性。模块化方法结合了马尔可夫链方法和组合模型方法的优点,但该方法通常都需要“部件行为相互独立”的假设。1.1 节指出,典型 PMS 模型经常提出“阶段时间固定”的假设,但现实工程中某些 PMS 的阶段转移是由不确定的事件触发的,此时阶段持续时间是一个不固定的随机变量。针对该型 PMS,可以采用马尔可夫再生过程或半马尔可夫过程建模法。

当 PMS 规模增大时,系统可能包含大量的部件和大量的阶段。所谓大型 PMS 是指含有大量部件和大量阶段的 PMS,事实上,一些文献[7-9]提及的大型 PMS 忽略了阶段数的增长。针对大型 PMS,单纯的组合模型或马尔可夫链方法通常会遭遇计算量爆炸问题,这些方法会因计算机内存不足而无法得出结果。为解决这一问题,近年来涌现出近似、上下界、截断等方法。这些方法在传统解析方法的基础上,添加了矩阵压缩、截断、上下界分析等策略,以得出 PMS 可靠度近似解为目的。另外,本书第 2～4 章提出的抽样方法也为大型 PMS 可靠性分析提供了新的解决方案。

综上所述,对于大规模可修 PMS 的可靠性分析问题,每种方法都存在自身的优势与缺陷,表 1.1 总结了各方法的优缺点。在实际工程实践中,需要根据 PMS 的规模和计算平台的容量,来选择合适的可靠性分析方法。

表 1.1 PMS 可靠性分析方法对比

项 目	解析方法			仿真方法
	组合模型方法	马尔可夫链方法	模块化方法	
可修部件的建模能力	弱	强	一般	强
含大量部件的 PMS 的建模能力	强	弱	强	强

续表

项　　目	解析方法			仿真方法
	组合模型方法	马尔可夫链方法	模块化方法	
含大量阶段的 PMS 的建模能力	弱	强	强	强
结果精度	高	高	高	一般

1.2.2 PMS 可靠性分析的仿真方法

仿真方法是分析系统可靠性的一种便捷而有效的手段，是工程领域最常用的方法。仿真方法的特点是适用范围广、研究对象灵活、几乎可以描述工程中的所有特殊情况，如设备维修、共因失效、不完全覆盖等问题都可以用仿真方法来描述。当解析方法难以精确描述上述情景时，仿真方法可以弥补解析方法的缺陷，成为分析大规模复杂 PMS 可靠性的有力工具。仿真方法的理论基础是大数定理，通过若干次仿真实验统计出 PMS 可靠性结果。

分析 PMS 可靠性的仿真方法主要包括：蒙特卡罗仿真[10-12]、离散事件仿真[13-15]和 Petri 网仿真[16-23]等。仿真方法的执行步骤大体一致——首先根据模型参数对各部件的寿命、修复时间和阶段持续时间等变量进行抽样，然后基于部件状态判断任务成败，通过多次仿真得到大量样本，最后统计得到任务可靠性的实验值。

目前越来越多的 PMS 可靠性仿真分析文献采用了 Petri 网方法。Petri 网方法可分为三类：第一类 Petri 网描述所有部件的状态转移，利用令牌(token)的转移来仿真部件的失效和维修行为。第二类 Petri 网用于监测系统失效，其变迁条件为 PMS 可靠性逻辑函数。第三类 Petri 网用令牌转移描述阶段前进，变迁的延迟时间为阶段持续时间，该 Petri 网的运行优先级低于前两组 Petri 网。Petri 网模型可以描述随机的阶段持续时间和服从一般分布的部件参数。建模过程中，只需增加库所数量即可描述多状态的部件。事实上，Petri 网方法对复杂工程问题的建模能力是很强的。

目前，绝大多数商用可靠性分析软件都包含仿真分析模块，这些软件通常都包含可靠度预计、可靠性数据分析管理、维修保障分析管理等模块。其中商业化比较成功的软件包括 Relex Studio[24]（又称为 Windchill Quality Solution），据报道，该软件为洛克希德马丁公司、波音公司和通用动力公司的产品提供可靠性分析服务[25]。此外，ITEM Software 公司的 ITEM Toolkit[26]、ReliaSoft 公司的 BlockSim 软件[27]都具有 PMS 可靠性分析功能。相比于这些价格高昂的软件平台，GRIF 软件[28]和 Trivedi 教授开发的 SHARPE 软件[29]目前提供免费版。

毫无疑问，仿真方法存在一定的缺陷。真实的工程系统通常都是可靠性极高的，为了达到满意的仿真结果精度，往往需要极高的仿真次数，这导致仿真方法比

解析方法需要更多的运算时间，这一差距对于中小规模 PMS 尤为明显。另外，由于仿真随机数种子的限制，仿真次数并不是越多越好，仿真达到一定次数时会出现重复仿真的现象。特别是对高可靠度的系统，由于时间成本和计算机内存的限制，仿真结果精度往往差强人意，不利于系统的可靠性设计工作。

综上所述，尽管仿真方法存在各种优点，但它对于模型简单、可靠度高的 PMS 并不是最佳的分析方法，特别是对于产量高、销量大的产品，仿真方法和仿真软件难以得出高精度的可靠度结果，这对产品售后服务和维护保养都是不利的。相比之下，解析方法因其精度高的特点，在商业软件中也占有相当重要的地位。1.2.3 节主要介绍非仿真方法中的组合模型方法。

1.2.3 PMS 可靠性分析的组合模型方法

组合模型方法是指包括可靠性框图模型[4,30]、静态故障树模型[6,31-34]和决策图模型[35-50]在内的静态可靠性分析方法。组合模型方法主要用于分析不可修的 PMS，通常具有简洁直观、模型规模小、求解速度快等特点。

1. 可靠性框图与故障树方法

可靠性框图（RBD）是描述 PMS 结构的一种直观有效的方式。Esary 等[4]提出了基于 RBD 模型的 PMS 可靠性分析方法。该方法将各部件 C 拆分为一系列串联的单元 $C_1, C_2, \cdots, C_p$。例如，第三阶段的部件 K 会被拆分为 K_1, K_2, K_3，这种拆分策略能够有效地标记某个阶段失效的部件，从而解决 PMS 的跨阶段依存性问题，但是这种拆分方法只适用于微型不可修 PMS。

类似于 RBD，故障树（fault tree，FT）也是描述 PMS 结构的一种有效方式，基于故障树的系统可靠性分析方法称为故障树分析（fault tree analysis，FTA）。FTA 是一种将系统故障成因由总体至部分按树状逐次细化的分析方法。通常，FTA 将 PMS 故障作为分析目标（即顶事件），然后逐级寻找导致这一故障的原因，一直找到部件的故障因素（即底事件），而介于顶事件和底事件之间的事件称为中间事件。用适当的逻辑门将顶事件、中间事件、底事件连接起来便形成了故障树。图 1.3 是一个典型的静态故障树模型。

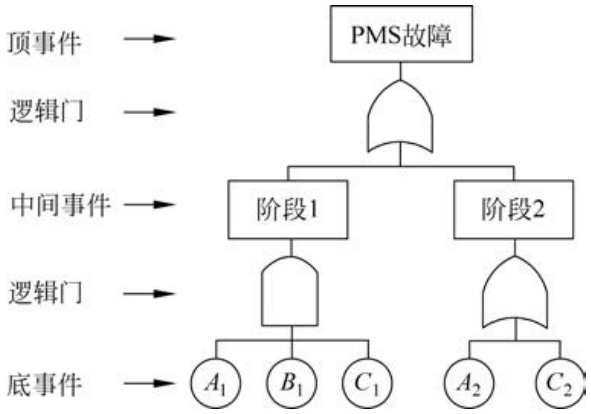

图 1.3 静态故障树模型示例图

故障树可分为静态故障树(static fault tree)[6,33]和动态故障树(dynamic fault tree)[31-32,34]。静态故障树采用静态逻辑门对系统建模,而动态故障树则至少包含一个动态逻辑门。静态逻辑门包括与门、或门等,而动态逻辑门包括顺序相关门、功能相关门、优先与门等[51]。基于故障树的PMS可靠性分析可以采用类似Esary论文中的部件拆分法,也可以采用决策图分析法。总体来说,静态故障树方法主要用于分析不可修PMS的可靠性,而动态故障树主要用于分析可修PMS。

在RBD或FT模型的基础上,一些学者[52-53]提出了PMS可靠性分析的布尔代数方法。该方法将系统失效表示为阶段失效组合(phase failure combination)的布尔代数表达式,从而将PMS不可靠度表达为各部件状态的组合。布尔代数方法方法是一种静态方法,只适用于小型不可修PMS。

2. 决策图方法

事实上,上述方法只能用于小规模不可修PMS。与之相比,决策图方法[35-50]能够有效分析部件数较多的PMS。决策图是二元决策图(BDD)、三元决策图(ternary decision diagram, TDD)和多值决策图(multi-valued decision diagram, MDD)的统称。文献中大部分以BDD为背景的算法都可以推广到TDD、MDD中来。BDD[54]是基于香农分解的一种布尔函数图形表示方法,图1.4给出了布尔函数 $f=(x_1+y_1)\cdot(x_2\cdot y_2)$ 的BDD示例。

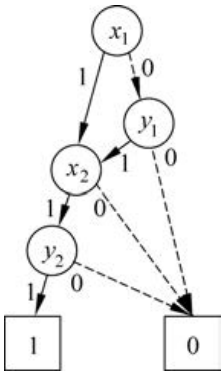

图1.4 布尔函数 $f=(x_1+y_1)\cdot(x_2\cdot y_2)$ 的BDD示例图

在BDD模型中,两个标识为1和0的没有输出边的节点分别称为"1节点"和"0节点",它们统称为吸收节点(sink nodes)。非吸收节点由变量 x_i 或 y_i 标识,并且具有两条分别标识为1和0的输出边,分别称为1边(1-edge)和0边(0-edge)。1边表示 x_i 或 $y_i=1$,用实线表示;而0边表示 x_i 或 $y_i=0$,用虚线表示。

Rauzy[41]提出了利用BDD分析故障树模型的可靠性分析方法。Zang[35]提出了基于BDD的PMS可靠性分析方法,该方法简称PMS-BDD。BDD方法除了擅长分析部件较多的PMS,还具有较高的建模可拓展性。只需要算法上的微调,决策图模型就可以分析多模失效问题[39,43]、不完全覆盖[9,36,38,40,45,55-59]和共因失效问题[60-66]。

尽管BDD模型存在诸多优点,但也存在如何选择最优"变量排序策略"(variable ordering scheme)的问题。根据给定排序策略生成的BDD称为有序二元决策图(ordered BDD, OBDD)[67]。针对同一个布尔函数表达式,不同的变量排序方式将生成不同规模的BDD。例如,对于布尔函数 $f=(x_1+y_1)\cdot(x_2\cdot y_2)$,两种不同的排序策略 $x_1\prec y_1\prec x_2\prec y_2$ 和 $x_2\prec x_1\prec y_2\prec y_1$ 会生成不同规模的BDD,如图1.5所示,其中 $x\prec y$ 表示变量 x 排在变量 y 之前。大量文献[68-70]指

出，变量排序策略对 BDD 的规模影响很大。

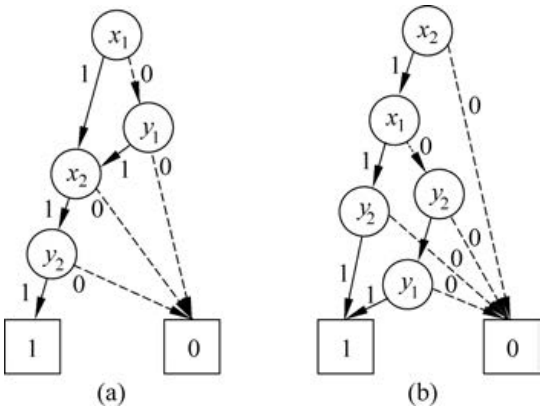

图 1.5 不同变量排序策略对 BDD 规模的影响

(a) $x_1 \prec y_1 \prec x_2 \prec y_2$；(b) $x_2 \prec x_1 \prec y_2 \prec y_1$

针对任意 PMS，是否存在一个最优的变量排序策略生成机制使 BDD 结构最小，一直是学界争论的焦点。Friedman 等[68] 于 1987 年给出了一种复杂度为 $O(n^2 3^n)$ 的最优排序策略生成算法，而 Bollig 等[69] 在 1996 年认为求解 BDD 的最优排序策略是一个 NP 问题。针对给定 PMS，如何给出一个合理的变量排序结构使 BDD 规模尽可能小，是近年来 BDD 研究的主要问题之一。Zang[35] 提出的 PMS-BDD 方法给出了两种 BDD 变量排序策略——前向阶段依赖操作和后向阶段依赖操作的变量排序算法。Xing 等[37] 指出，Zang 给出的系统 OBDD 生成算法并不适用于所有的排序算法，因此提出了一个针对任意排序规则的 BDD 生成算法（称为两阶段算法）。此外，Mo[42-43] 总结了 4 种 OBDD 变量排序策略，分别是前向阶段依赖操作（forword phased dependent operation，FPDO）、后向阶段依赖操作（backword phased dependent operation，BPDO）、前向串联（forward concatenation，FCON）和后向串联（backward concatenation，BCON），提出了适用于不同 PMS 的变量排序策略选择方案。

基于 BDD 的 PMS 可靠度计算方式有两种——第一种是枚举 BDD 通路的向下运算策略（top-down algorithm），第二种是遍历 BDD 节点的向上运算策略（bottom-up algorithm）。具体执行时，需要根据 BDD 的特点选择对应的计算方式。由于部件在前一阶段的行为会影响后续阶段，所以对于图 1.5(a)的 BDD 只能采用枚举 BDD 通路的向下运算策略。当给定的 BDD 中变量按照阶段先后顺序自下而上排列时（图 1.5(b)），宜采用遍历 BDD 节点的向上运算策略（此时也可以选择向下运算策略，但计算量更大）。

近年来，决策图在计算机辅助设计等工程领域得到了广泛的应用[47]，同时它也是 PMS 可靠性分析的热门方法。它的优点主要包括以下几方面。

(1) 决策图方法能够有效分析包含大量部件的 PMS，可规避状态爆炸问题。

(2) 决策图方法具有良好的拓展性，可作为分析多状态部件、多模失效、不完

全覆盖问题的基础平台。

然而，决策图方法也不可避免地存在以下缺陷。

(1) 决策图方法不能分析阶段内的部件维修行为。

(2) 当 PMS 的阶段增多时，决策图方法将遭遇运算量及内存占用爆炸问题。

对于可修 PMS，上述组合模型方法需要与马尔可夫模型相结合，形成模块化分析方法。下一节主要介绍分析 PMS 可靠性的马尔可夫模型。

1.2.4 PMS 可靠性分析的马尔可夫模型

马尔可夫链方法[71-78]，又称马尔可夫链方法或马尔可夫模型，是一种基于连续时间马尔可夫链理论的经典可靠性分析方法，它与 Petri 网模型被归类为状态空间方法(state-based methods)。通常来说，只有当 PMS 包含可修部件时，马尔可夫链方法才会被使用，这主要是由于马尔可夫链方法会遭遇著名的“状态爆炸问题”。所谓状态爆炸问题是指状态空间的规模随部件数增多而呈指数增长。例如，对于两部件组成的微型系统，状态空间包含 4 个状态——(1,1)，(1,0)，(0,1)，(0,0)。而当系统部件增加到 4 个时，状态空间将包含 16(2^4)个状态。事实上，状态空间的指数级增长严重限制了传统马尔可夫链方法的适用性。

将状态空间方法应用于 PMS 可靠性分析中的研究始于 20 世纪 80 年代[78]。Alam 等[71]提出传统的马尔可夫链方法并分析了微型可修 PMS 的可靠性。该方法首先建立一个包含所有部件的转移速率矩阵(transition rate matrix，TRM)$\boldsymbol{Q}$，而后按照阶段先后顺序计算任务结束时刻的状态概率向量。矩阵 $\boldsymbol{Q}$ 亦可称为无穷小生成子(infinitesimal generator)，$\boldsymbol{Q}$ 中的元素 q_{ij} 表示系统从状态 i 到状态 j 的转移速率。Alam 方法对所有阶段建立统一的方阵 $\boldsymbol{Q}$，也就是说，不同阶段对应的矩阵 $\boldsymbol{Q}$ 阶数相同，但 q_{ij} 值不尽相同。设初始状态概率向量为$\boldsymbol{v}$(0)，根据连续时间马尔可夫链理论，第一阶段结束时状态概率向量可表示为$\boldsymbol{v}(T_1)=\boldsymbol{v}(0)\cdot e^{\boldsymbol{Q}_1\cdot T_1}$，依次类推得出任务结束时的状态概率向量，PMS 可靠度等于状态概率向量中成功状态的概率和。矩阵指数 $e^{\boldsymbol{Q}\cdot T}$ 的计算方法包括泰勒展开法、帕德方法、常微分方程法等。

在 Alam 方法的基础上，Smotherman[72-73]等运用非齐次马尔可夫链分析了阶段时间不固定的可修 PMS 的可靠性。Dugan[79]提出了一种将故障树转化为马尔可夫模型，并将各阶段马尔可夫模型整合为统一马尔可夫链的 PMS 可靠性分析方法。Dugan 指出，合并后的马尔可夫链不再具有时间齐次性，因此该方法存在理论可行，但应用困难的问题。

上述方法需要构建一个包含所有部件的转移速率矩阵 $\boldsymbol{Q}$，一些文献中将其称为“马尔可夫模型的统一建模方案”[80-81]。运用统一建模方案的 PMS 可靠性方法不可避免地用到一个规模庞大的矩阵 $\boldsymbol{Q}$。为了解决这一问题，Somani 等[74]和 Kim 等[75]采用了各阶段独立建模的方案。各阶段独立建模的思路是单独建立各

个阶段的CTMC模型，而后再通过状态映射将阶段转移时刻的概率向量连结起来。由于单阶段通常只包含少量部件，所以矩阵 $\boldsymbol{Q}$ 的规模都不是很大，Somani为该策略开发了HARP-PMS软件包。在各阶段独立建模的基础上，Kim提出了基于矩阵 $\boldsymbol{Q}$ 特征值的可靠性递推公式，该方法可适用于阶段持续时间不固定的PMS。

总体来说，统一建模方案和各阶段独立建模方案各有其优劣性。一方面，在系统某一阶段发生结构改变时，统一建模方案缺乏重用性。仅仅是对PMS某一阶段结构的微小改动，统一建模方案也不得不重新构建矩阵 $\boldsymbol{Q}$，这不利于后期的可靠性设计的工作，有违系统可靠性分析初衷。统一建模方案需要使用超大规模的矩阵 $\boldsymbol{Q}$ 也为矩阵存储问题带来了挑战。另一方面，各阶段独立建模方案有很好的模型重用性，某一阶段的改动并不会影响其他阶段，同时也降低了超大型矩阵 $\boldsymbol{Q}$ 出现的概率。然而遗憾的是，独立建模方案涉及的状态映射是该方案实用化的一个障碍。由于不同阶段中参与任务的设备通常不同，导致两阶段的状态概率向量无法直接匹配，如何计算状态映射的概率是独立建模方案的难点所在。一些文献[74]研究的状态映射计算方法只适用于特定PMS，并不具有一般性。表1.2总结了统一建模方案和独立建模方案各自的优缺点。

表1.2 马尔可夫链方法两种建模方案的对比

维　　度	马尔可夫链方法	
	统一建模方案	独立建模方案
模型重用能力	弱	一般
矩阵 $\boldsymbol{Q}$ 规模	巨大	大
阶段转移处理难度	低	高

事实上无论采用何种建模方案，当部件增多时，马尔可夫模型都会遭遇状态爆炸问题。对此，闫华[81]讨论了大规模稀疏矩阵 $\boldsymbol{Q}$ 的特点和生成机制，给出了 $\boldsymbol{Q}$ 的压缩存储方法。另外，闫华还提出了基于Krylov子空间投影的PMS可靠性近似计算方法。这种方法在一定程度上避免了状态爆炸问题，但涉及较多的微分方程和级数运算，编程实现难度较大。

现有文献中，大多数的马尔可夫模型都提出“部件失效时间和维修时间服从指数分布”的假设，这一假设是利用连续时间马尔可夫链数学理论的前提。如果没有这一假设(即部件失效时间和维修时间服从一般分布)，马尔可夫链方法通常须采用复杂的更新过程(renewal process)理论，精确解的计算难度较大。莫毓昌等[82]基于马尔可夫再生过程和拉普拉斯变换(Laplace transform)，提出了任务时间为一般分布，部件参数服从一般分布的PMS可靠性分析方法。Chryssaphinou等[83]基于离散时间半马尔可夫(semi-Markov)过程，分析了多状态系统的可靠性。

在近年来的PMS文献中，马尔可夫模型主要用于模块化方法[84-90]的底层建

模。通常,模块化方法通过马尔可夫模型(或 Petri 网)描述部件的失效和维修行为,再通过组合模型描述跨阶段依存关系。模块化方法提出的主要目的是在分析部件维修性的同时避免状态爆炸问题。早期的模块化方法文献中,Mura 等[84]基于 Petri 网和离散时间马尔可夫链提出了可修 PMS 的可靠性分析方法,该方法利用 Petri 网描述部件行为,并用离散时间马尔可夫链描述任务失效和阶段转移,该方法的计算效率与传统马尔可夫链方法相比有明显优势。基于 BDD 和马尔可夫模型,Ou 等[86]提出了模块联合概率的概念并分析了可修 PMS 的可靠性。此外,Wang 等[87]利用 BDD 和马尔可夫链分析了包含大量部件的可修 PMS 可靠性,2.1 节对该方法进行了较详细的阐述。Shrestha 等[88]利用多值多状态决策图(multi-state multi-valued decision diagram,MMDD)将 Wang 的方法推广应用到多状态 PMS。

现有研究表明,模块化方法是在建模能力和运算效率方面表现优秀的解析方法,已经成为了 PMS 可靠性分析的热点。第 2、3、4 章提出的行为向量方法和抽样方法都属于结合 BDD 和马尔可夫模型的模块化方法。

1.3 主要工作和创新点

1.3.1 研究内容和结构框架

本书第 2～4 章提出了计算大规模可修 PMS 可靠度的三种模块化方法——行为向量方法、行为向量与截断策略混合算法、抽样方法。三种方法的适用范围依次扩展,建模能力依次增强。本书各章节的结构框架如图 1.6 所示。

第 1 章是绪论,主要论述了多阶段任务系统可靠性分析的研究背景,研究意义,PMS 可靠性分析的国内外研究现状及创新点。

第 2 章详细论述了分析 PMS 可靠性的行为向量方法,它继承了经典模块化方法的优点——能够在分析可修部件的同时规避状态爆炸问题,在计算效率上比传统马尔可夫模型优势明显。行为向量方法相较于其他模块化方法的优点是它可应用于广义 PMS。

第 3 章详细论述了行为向量方法与截断策略混合算法。由于行为向量方法无法应用于包含大量阶段的 PMS,第 3 章提出了行为向量方法的改进算法,并引入截断策略来缓解计算量指数增长问题。加入截断策略后,算法可分析的阶段数明显增多。

第 4 章提出了全新的抽样方法,用于分析大规模可修 PMS 的可靠性。对于大规模可修 PMS,抽样方法比绝大部分解析方法都有计算效率上的优势,可应对 PMS 部件增多和阶段增多带来的问题。此外,抽样方法还避免了其他模块化方法无法分析“阶段内维修”的问题,模型假设更少。另外,第 4 章还提出了通过“离散

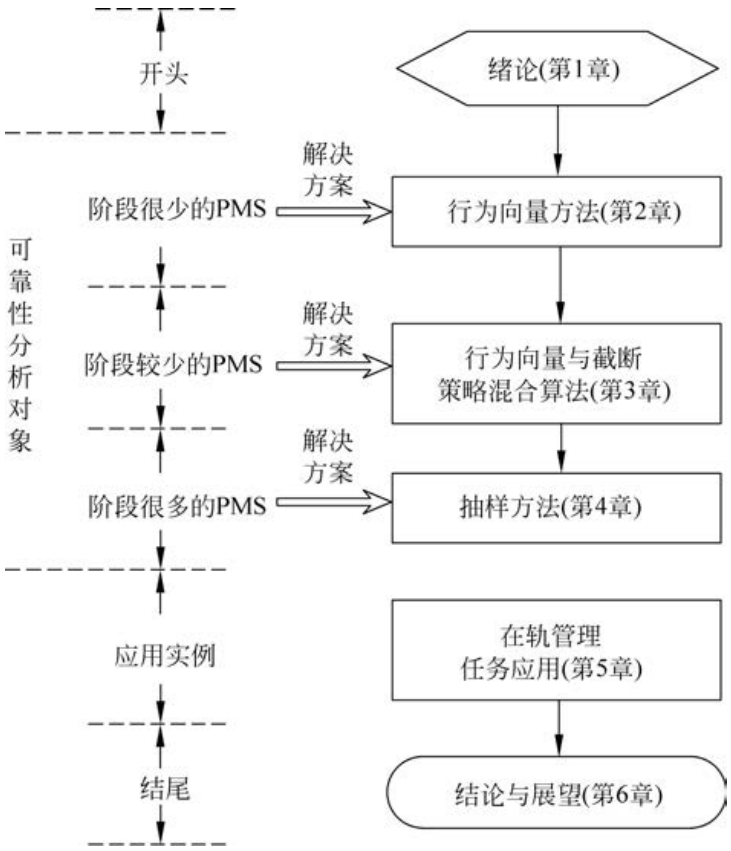

图 1.6 本书各章节的结构框架图

时间可用度”逼近 PMS 可靠度的求解思路。

第 5 章以航天测控系统为例，总结了航天测控系统可靠性的研究现状，并分别对单圈次和多圈次的卫星在轨管理任务建立了小型和大型 PMS 模型，通过实验对比了本书中三种解析方法和 Petri 网仿真方法的计算效率。

第 6 章对全书的研究工作进行总结，并提出了今后值得研究的一些相关方向。

1.3.2 主要创新点

从近年 PMS 可靠性领域的文献不难发现，将多种解析方法结合起来是一个非常有价值的研究方向。本书在 BDD 和马尔可夫模型的基础上，设计并实现了三种 PMS 可靠性分析方法，其中主要创新点可概括为以下四点。

(1) 设计并实现了可应用于广义可修 PMS 的行为向量方法，并且规避了状态爆炸问题。相较于传统的马尔可夫链方法，行为向量方法的运算耗时更少，占用内存更低，它缓解了状态爆炸问题，在分析部件较多的 PMS 时优势明显；相较于经典模块化方法，行为向量方法的创新点在于它考虑了组合阶段需求，可应用于广义 PMS。

(2) 提出了降低行为向量方法计算量且精度可控的截断策略。截断策略允许行为向量方法忽略大批权重低的计算节点，从而提高计算效率，降低内存消耗。通

过加入截断策略，改进后的行为向量方法可适用于包含更多阶段的 PMS。此外，截断策略采用递减的截断阈值，使截断误差直接控制在预定参数下，避免了经典截断方法中探讨误差的繁琐步骤。

（3）设计并实现了分析大规模可修 PMS 可靠性的抽样方法。抽样方法的最主要优势在于算法的时间和空间（内存）消耗较低，它可有效分析含大量阶段和大量可修部件的 PMS，当分析对象规模增长时，抽样算法运算量不会呈指数增长。抽样方法可以分析包含上千阶段的 PMS，而其他绝大多数模块化均不具备这种运算能力。

（4）构建了离散时间可用度的概念，并提出了一种用离散时间可用度逼近系统可靠度的可靠性分析新方法。基于这种新的系统可靠性分析方法，抽样算法解决了传统模块化方法无法分析阶段内维修的问题。

综上所述，本书第 2～4 章提出了三种 PMS 可靠性分析方法——行为向量方法、行为向量与截断策略混合算法、抽样方法，这三种方法均可分析可修部件，并都能避免状态爆炸问题。对于含大量阶段的 PMS，三种解析方法的分析能力依次增强，内存占用依次降低，实验证明抽样方法是分析大型可修 PMS 主要的解析方法之一。

第2章

PMS可靠性分析的行为向量方法

1.2节国内外研究综述指出，分析可修PMS可靠性的解析方法主要分为两类：第一类为基于CTMC的马尔可夫模型，第二类为结合BDD与CTMC的模块化方法。由于模块化方法可有效缓解状态爆炸问题，因此在近年的可靠性文献中被广泛采用。本章首先介绍一种经典的模块化方法——Wang-Modular算法，而后提出一种新的模块化方法——行为向量方法。

本章提出的行为向量方法继承了Wang-Modular算法的优点——算法不仅考虑了可修部件，还能有效缓解状态爆炸问题。与Wang-Modular算法不同的是，行为向量方法的适用范围更广，它可应用于广义多阶段任务系统(generalized phased mission systems，GPMS)。行为向量概念易于理解，能避免经典模块化方法中涉及的BDD变量排序难题，模型复杂度低，编程实现容易。

本章首先介绍可靠性模块化经典方法中的Wang-Modular算法，目前有多篇重要文献中的算法基于该算法改进而来；其次，考虑到行为向量方法可应用于GPMS，介绍GPMS的概念及其工程背景，并提出“系统行为向量”和“部件行为向量”的概念，它们是算法规避状态爆炸问题的关键；再次，描述行为向量方法的运算步骤、模型假设和适用范围；最后，结合两个工程实例分析行为向量方法的计算效率和优缺点，并与传统马尔可夫模型和Wang-Modular算法进行对比。

2.1 经典模块化方法简介

模块化方法被定义为结合马尔可夫模型和组合模型的PMS可靠性分析方法[86]。国内外研究现状指出，马尔可夫模型擅于描述部件的可修性，但其缺陷在于状态爆炸问题。组合模型的优点在于其规避了状态爆炸问题，但它难以分析维修行为对系统可靠性的影响。学者提出模块化方法的目标是结合马尔可夫模型和组合模型各自的优点，在分析可修部件的同时规避状态爆炸问题，以便评估大型可修PMS的可靠性。

通常，模块化方法一方面利用组合模型来描述不同阶段间的状态转移关系，另一方面通过 CTMC 描述部件故障和修复的概率。因为组合模型贯穿了各个阶段，因此被认为是高层模型(high-level model)；而 CTMC 具体描述各部件具体的行为和状态，因此被认为是低层模型(low-level model)；所以，模块化方法又称为层次化方法。

本节介绍的经典模块化方法是由 Wang 等[87]在 2007 年提出的，一般称其为 Wang-Modular 算法，Shrestha 等[88]于 2011 年将该方法进一步推广应用于多状态部件。Wang-Modular 算法结合 BDD 和 CTMC，通过 BDD 描述跨阶段依赖关系，并通过 CTMC 分析设备的可维修性。Wang-Modular 算法是首个考虑大量可修部件的 PMS 可靠性分析方法。

考虑到行为向量方法在计算复杂度上等同于 Wang-Modular 算法，有必要对 Wang-Modular 算法的运算步骤进行简要介绍。该算法运用了 BDD 中的向下运算策略，该策略主要分为以下三个步骤。

步骤 1 生成各阶段的 BDD，然后融合生成整个 PMS 的 BDD。

步骤 2 找出 BDD 中从根节点到节点 1 的所有通路，计算每条通路的概率。

步骤 3 对所有通路的概率求和，得出 PMS 的可靠度。

考虑一个两阶段、两部件(A、B)的 PMS，系统的可靠性逻辑函数可表示为

$$\Phi=(A_1+B_1)\cdot(A_2\cdot B_2) \tag{2.1}$$

式中，A_1、A_2 分别为部件 A 在阶段 1、阶段 2 的状态；B_1、B_2 同理；线段上 1 表示部件良好，0 表示部件失效。首先，Wang-Modular 算法通过 BDD 融合机制建立整个 PMS 的 BDD，如图 2.1 所示。

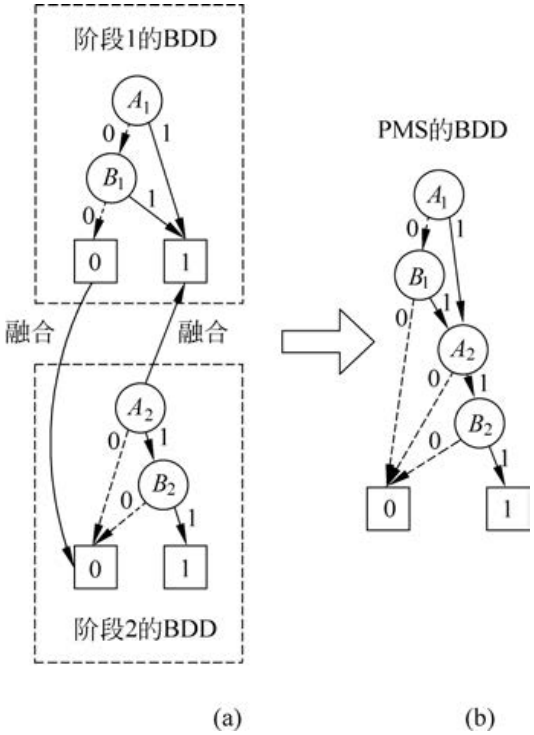

图 2.1 Wang-Modular 算法通过 BDD 融合机制建立

(a) 两阶段的独立二元决策树；(b) 合并后的二元决策树

然后，向下运算策略遍历BDD，找出从顶节点到吸收节点1的所有通路，包括：

$\text{path}_1 = (A_1$ 良好，A_2 良好，B_2 良好）

$\text{path}_2 = (A_1$ 失效，B_1 良好，A_2 良好，B_2 良好）

其中，path_1 和 path_2 表示多阶段图2.1(b)中从顶点到底部节点1(表示成功)的两条路径。而后根据部件 A、B 的CTMC，计算通路 path_1 和 path_2 的概率。例如，对于通路 path_1，要求部件 A 在阶段1和阶段2保持良好，且设备 B 在阶段2保持良好(未要求部件 B 在阶段1的状态)。因此 path_1 的概率 $\Pr\{\text{path}_1\}$ 可表示为

$$\Pr\{\text{path}_1\} = (\boldsymbol{v}_0^{(A)} \cdot \boldsymbol{U}_1^{(A)} \cdot \boldsymbol{U}_2^{(A)} \cdot (1,1)') \cdot (\boldsymbol{v}_0^{(B)} \cdot \boldsymbol{E}_1^{(B)} \cdot \boldsymbol{U}_2^{(B)} \cdot (1,1)') \tag{2.2}$$

式中，$\boldsymbol{v}_0^{(A)}$ 表示部件 A 的初始状态概率向量，假设 A 是初始完好的两状态部件，则 $\boldsymbol{v}_0^{(A)} = (1,0)$。

根据连续时间马尔可夫链理论，式中初始状态概率向量 $\boldsymbol{v}_0^{(A)}$ 可通过式(2.3)展开，即

$$\boldsymbol{v}_i^{(k)} = \boldsymbol{v}_{i-1}^{(k)} \cdot \boldsymbol{C}_i^{(k)} = \cdots = \boldsymbol{v}_0^{(k)} \cdot \prod_{j=1}^{i} \boldsymbol{C}_j^{(k)} \tag{2.3}$$

式中，转移概率矩阵 $\boldsymbol{C}_i^{(k)}$ 可表示为

$$\boldsymbol{C}_i^{(k)} = \begin{cases} \boldsymbol{E}_i^{(k)}, & \text{如果设备 } k \text{ 在阶段 } i \text{ 的状态无关紧要} \\ \boldsymbol{U}_i^{(k)}, & \text{如果设备 } k \text{ 在阶段 } i \text{ 一直可用} \\ \boldsymbol{D}_i^{(k)}, & \text{如果设备 } k \text{ 在阶段 } i \text{ 出现故障} \end{cases} \tag{2.4}$$

根据连续时间马尔可夫链理论，矩阵 $\boldsymbol{E}_i^{(k)}$ 可描述为

$$\boldsymbol{E}_i^{(k)} = \exp\left(\begin{bmatrix} -\lambda_i^{(k)} & \lambda_i^{(k)} \\ \mu_i^{(k)} & -\mu_i^{(k)} \end{bmatrix} \cdot T_i \right) \tag{2.5}$$

矩阵 $\boldsymbol{U}_i^{(k)}$、$\boldsymbol{D}_i^{(k)}$ 的具体形式详见文献[87-89]，部件 A 的CTMC如图2.2所示。

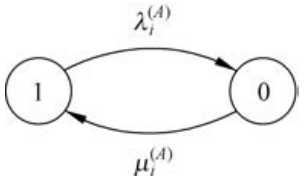

图2.2 两状态部件 A 的CTMC

最后，Wang-Modular算法将不同通路的概率相加，得到PMS的可靠度，即

$$R_{\text{PMS}} = \sum_k \Pr\{\text{path}_k\} \tag{2.6}$$

Wang-Modular算法的主要优点是规避了状态爆炸问题。事实上，Wang-Modular算法耗时和内存占用量与合成后BDD的规模成正比。根据决策图理论[41]，决策图的规模不会随部件增多而指数增长，因此相较于传统的马尔可夫模型，Wang-Modular算法可分析含更多部件的PMS，这是Wang-Modular算法优于传统马尔可夫模型最显著的特点。

但是，Wang-Modular算法也存在一定缺陷，这主要包括以下几点：

(1) 在计算效率上,随着 PMS 阶段增多,BDD 规模会呈指数级别增长。

(2) 在模型直观性上,Wang-Modular 算法的设计原理难以理解。

实验例证指出,当部件增多时,系统 BDD 规模的增长速度比指数增长慢,但比线性增长快[41],如图 2.3 所示。然而当阶段增多时,系统 BDD 的规模会无可避免地呈指数增长,该问题是由 BDD 生成算法导致的,Wang- Modular 算法目前无法规避此问题。

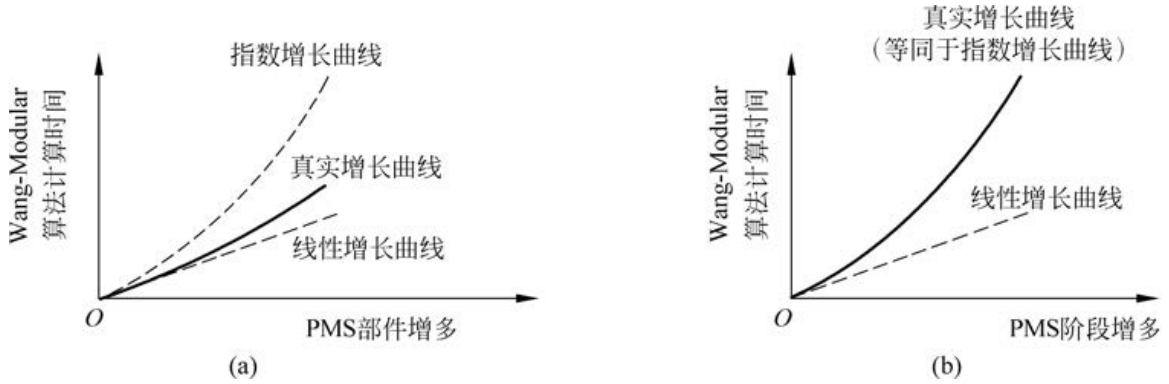

图 2.3 PMS 规模增大时 Wang-Modular 算法耗时

(a) 部件增多时;(b) 阶段增多时

Wang-Modular 算法的分析对象是传统 PMS,即传统的 PMS 假设各阶段的任务都成功,总任务才成功,该方法并未推广应用到广义多阶段任务系统中。然而,广义多阶段任务系统允许某些阶段出现失败,某些局部阶段的失败不一定导致整体任务失败。事实上,由于广义多阶段任务系统的二元决策图无法用子阶段二元决策图融合生成(但可以通过特定序贯策略生成),所以 Wang-Modular 算法应用在广义多阶段任务系统还有一定的难度。2.2 节将介绍广义多阶段任务系统的概念和例子,为介绍“行为向量方法”做出铺垫。行为向量方法在计算效率上等同于 Wang-Modular 算法,但它能够直观地应用于广义多阶段任务系统,而且行为向量方法容易理解,也更加直观。

2.2 广义 PMS 的概念和背景

在介绍行为向量方法之前,有必要先了解广义多阶段任务系统的定义及其工程背景。在传统 PMS 模型中,总任务成功要求各阶段子任务都执行成功,也就是说,只要各阶段子任务有一个执行失败,总任务即视为失败。然而在工程实际中,系统通常允许某些非关键阶段的任务执行失败,也就是说,不同阶段任务的成败通过一个特定的逻辑关系组合成整体任务的成败,这种逻辑组合关系称为组合阶段需求(combinatorial phase requirement,CPR)[55]。

CPR 可以用故障树来表示,phase-OR 表示各阶段任务故障的或门,phase-