非单调关联系统可靠性技术

FEI DANDIAO GUANLIAN XITONG KEKAOXING JISHU

周经伦　孙权　冯静/著

国防科技大学出版社

国防科技大学学术著作
专项经费资助出版

非单调关联系统可靠性技术

周经伦　孙　权　冯　静　著

国防科技大学出版社
湖南·长沙

图书在版编目(CIP)数据

非单调关联系统可靠性技术/周经伦,孙权,冯静著.—长沙:国防科技大学出版社,2008.9

ISBN 978-7-81099-476-7

Ⅰ.非… Ⅱ.①周… ②孙… ③冯… Ⅲ.多关联系统—系统可靠性—研究 Ⅳ.N945.17

中国版本图书馆 CIP 数据核字(2008)第 002084 号

国防科技大学出版社出版发行

电话:(0731)4572640 邮政编码:410073

http://www.gfkdcbs.com

责任编辑:耿 筠 责任校对:徐 飞

新华书店总店北京发行所经销

国防科技大学印刷厂印装

*

开本:850×1168 1/32 印张:8.5 字数:221 千

2008 年 9 月第 1 版第 1 次印刷 印数:1-1000 册

ISBN 978-7-81099-476-7

定价:28.00 元

前　言

传统的单调关联系统可靠性分析方法难以满足实际工程中系统可靠性设计分析的需要，迫切需要研究非单调关联系统的可靠性分析技术，这项技术已成为可靠性共性的关键前沿技术之一。

本书系统地论述了非单调关联系统可靠性基本理论、最新的定性定量分析研究成果、计算机辅助技术以及实际应用等内容。通过对非单调关联系统结构理论研究，获得了非单调系统结构特性和判别系统结构非单调性的准则和方法。在非单调关联故障树分析方法方面，得到了基于 BDD 的计算故障树顶事件概率和质蕴含集的新算法，新算法的主要优点是，省去了一般算法中大量的不交化运算过程（不交化是可靠性定量分析中的一个最主要的运算），从而使运算速度大大提高。在非单调关联系统的重要度方面，概率重要度是各种重要度中最基本的重要度，许多重要度的概念都与之有关，但传统的定义中，单调系统中的概率重要度与非单调系统中的正逆概率重要度分别定义，而且正逆概率重要度算法涉及正逆相关割集和无关割集的概念，计算复杂，这限制了重要度

在实际工程中的应用。本书通过引入正逆临界集的概念,统一了单调系统中的概率重要度与非单调系统中的正逆概率重要度在概念上的差异,并且得到了基于 BDD 的计算概率重要度的方法,该算法充分利用了 BDD 的优点,简便并易于计算机处理。在系统故障安全性方面,提出了非单调故障安全系统的构造方法。最后讨论了非单调系统测试性,利用系统结构特性与质蕴含集特性,得到了一类特别的非单调系统——混合单调系统的最小测试集产生方法。

本书的完成得到了国防科技大学学术专著专项经费的资助。本书的完成也得到了方逵、唐勇、刘波、汪有涛等同志的帮助,这些同志为此项研究做了大量的工作,本文中的某些概念和结论是作者和他们长期一起讨论的结果。

阅读本书,必须具有系统可靠性分析的基本知识。作者期望本书的出版对读者能有所裨益,并热忱欢迎提出各种不同的看法和批评意见。

作 者

2008.01.06

目　录

第 1 章　非单调关联系统基本理论

1.1　非单调关联系统的工程背景 …… (3)
1.2　非单调关联系统的基本概念 …… (8)
1.3　结构函数表达式与质蕴含 …… (10)
1.4　单调与非单调系统结构特性 …… (14)
1.5　质蕴含集算法 …… (21)

第 2 章　基于 BDD 的非单调故障树分析

2.1　非单调关联故障树的基本概念 …… (34)
2.2　非单调关联故障树算法其及问题 …… (37)
2.3　BDD 的概念与性质 …… (40)
2.4　非单调关联故障树到 BDD 的转化 …… (51)
2.5　非单调关联故障树顶事件失效概率的计算 …… (64)
2.6　非单调关联故障树质蕴含集的算法 …… (68)

第 3 章　非单调关联系统的重要度

3.1　重要度概念和工程应用 …… (77)
3.2　非单调关联系统中的各种重要度 …… (81)
3.3　基于 BDD 的重要度计算方法 …… (97)

第 4 章　非单调关联系统矩阵分析法

4.1　NC-FTA 的早期不交化 …… (104)
4.2　矩阵法 FTA 定性分析 …… (106)
4.3　矩阵法 NC – FTA 的定性分析 …… (111)
4.4　矩阵法 NC – FTA 的定量分析 …… (122)

第 5 章　非单调关联故障树的模块化分析

5.1　故障树预处理 …… (129)
5.2　故障树的模块化 …… (133)
5.3　非单调关联故障树定性分析的模块合成算法 … (142)
5.4　非单调关联故障树定量计算的模块合成算法 … (146)

第 6 章　非单调关联系统可靠性分析实例

6.1　硝酸冷却系统 …… (151)
6.2　液位调节系统 …… (160)
6.3　卫星转速控制系统 …… (164)
6.4　可修 n 中取连续 k 系统 …… (188)

6.5 一类不同可靠度部件非单调关联系统的最优设计 …… (195)

第 7 章 非单调关联系统的最小覆盖集

7.1 最简逻辑式的存在性 …… (204)
7.2 求逻辑函数的最简表达式 …… (212)
7.3 故障树的最小无冗余基 …… (216)

第 8 章 非单调关联系统的故障安全性

8.1 故障安全的概念 …… (220)
8.2 单调系统的故障安全特性 …… (221)
8.3 非单调的故障安全逻辑系统构造方法 …… (223)

第 9 章 混合单调系统的测试性

9.1 故障检测的基本概念 …… (229)
9.2 单调结构系统的最小测试 …… (232)
9.3 混合单调结构系统的最小测试 …… (236)

第 10 章 非单调关联系统建模的两种新方法

10.1 单调分解方法 …… (240)
10.2 Petri 网方法 …… (247)

参考文献 …… (258)

第 1 章　非单调关联系统基本理论

系统可靠性理论的中心问题就是要确定复杂系统可靠度与其单元可靠度之间的关系，这种逻辑关系的数学表示就是结构函数。对系统可靠性分析的关键问题就是定性分析和定量评估。

目前对单调关联系统的研究已日臻完善，形成了较为完整的理论体系，对两状态单调关联系统结构有了较为系统的研究，在实践中得到了很好的应用。但是，对非单调关联系统研究得还较少。20 世纪 70 年代初，Heidtmaun 提出了一类典型的非单调关联系统，即“n 中取 r 至 s 系统”，这一系统的可靠性模型在具有固定容量的计算机网络中有普遍意义，这类系统可直接研究非单调关联系统的可靠性。另一种方法是从故障树角度研究非单调关联系统，即故障树分析。最早提出非单调关联系统故障树模型的是 Lapp 和 Powers，他们在分析硝酸冷却装置的安全性时提出了这一模型，从而开创了非单调关联系统故障树研究的先例。带有自控反馈的系统一般是非单调关联系统。非单调关联系统由于其结构函数至少存在一对互补的事件单元，在对系统进行故障模式识别时，必须在全部 MCS 基础上，找出全部 PIS 来刻画，因此在对系统进行定性分析时，主要目的就是找出全部 PIS。目前求解 PIS 的方法有 Quine 的 Consensus 运算法、Nelson 的双取补法。这两种方法效率很低，包含了巨大的计算量。另外就是 KH 法和 locks 法。它们的实质是：把原故障树化为对偶树或逆树，求得对偶树的 MCS，再反算得全部“PIS”，这些方法的效率也很低。近几年出现的 BDD（二元决策图）方法用来求解 PIS 是一个重要的研究方向，该方法将非单调

关联系统故障树转换成一个 BDD,通过 BDD 求解全部 PIS,该方法的实现只受 BDD 大小限制,而与系统单元多少、PIS 多少无关,是一种很有前途的方法,值得关注和研究。

传统的非单调关联系统概念是针对故障树模型提出的,多数定义不够完善,缺乏准确性,给深入开展非单调关联系统可靠性研究带来了一定的困难。本章讨论单调与非单调关联系统一些基本概念及其系统结构函数的性质,分析非单调关联系统的结构特性,以建立非单调关联系统可靠性技术研究的理论基础。

为方便起见,我们先对本文用到的有关术语与符号作如下说明。

设系统 S 由 n 个单元组成。单元是系统中不可再分割的部分,如实际系统中的部件、元件及其组合。

系统与单元状态分两种:正常或故障。我们不区别故障与失效的概念,并且假设各单元发生故障的事件相互独立。

对于由 n 个单元组成的系统 S,第 i 个($i=1,2,\cdots,n$)单元的状态用布尔变量 x_i 表示,取值为 0 或 1,表示第 i 个单元正常或故障;S 的状态用布尔变量 ϕ 表示,取值为 0 或 1,表示系统 S 正常或故障。系统 S 某一时刻各单元的状态组合用布尔向量 $X=(x_1,x_2,\cdots,x_n)$ 表示,称为 S 的状态向量。$\phi(X)$ 表示各单元状态为 X 时系统 S 的状态变量。

记 $B=\{0,1\}$,B^n 是 B 的 Cartesian 乘积,即 $B^n=\overbrace{B\times B\times\cdots\times B}^{n}$。

对于 B^n 中的两个元素 $a=(a_1,a_2,\cdots,a_n)\in B^n$,$b=(b_1,b_2,\cdots,b_n)\in B^n$,定义:

$$a\leqslant b\Leftrightarrow a_i\leqslant b_i(i=1,2,\cdots,n;a_i,b_i\in B)。$$

$(1_i,X_i)$和$(0_i,X_i)$分别表示 B^n 中 X 的第 i 分量限制为 1 和 0,即

$$(1_i, X_i) = (x_1, x_2, \cdots, x_{i-1}, 1, x_{i+1}, \cdots, x_n),$$
$$(0_i, X_i) = (x_1, x_2, \cdots, x_{i-1}, 0, x_{i+1}, \cdots, x_n)。$$

运算符“+”、“·”和“,”在布尔表达式中表示逻辑或、逻辑与和补运算。例如，$\phi(x_1, x_2, x_3) = x_1 \cdot x_2 + x'_2 \cdot x_3$。为方便，我们常省去运算符“·”。

$\phi = \phi(X)$是定义在 B^n 上的布尔函数，用 $\phi_{x_i=1}$ 和 $\phi_{x_i=0}$ 分别表示 B^n 中 X 的第 i 分量限制为 1 和 0 的函数，即 $\phi_{x_i=1} = \phi(1_i, X_i)$，$\phi_{x_i=0} = \phi(0_i, X_i)$。

1.1　非单调关联系统的工程背景

可靠性理论发展到今天已取得了丰硕的研究成果，并成功地应用到许多大型复杂工程、系统中，取得了较好的经济效益和社会效益。一般情况下，我们对两状态单调关联系统和统计独立事件可以容易地处理，对两状态单调关联系统结构有了较为系统的研究。但我们知道，现实工程实际中的系统通常都是具有负反馈、回流和反相器等特殊特点的非单调关联系统，而这却是单调关联系统所不具有的。

反馈控制是指从被控制对象获取信息，反过来又把调节被控制量的作用反馈给被控制对象的一种控制方法。反馈控制的目的是要消除(或减少)被控制量与额定值之间的偏差，因而，控制作用的方向就必须与偏差的极性相反，并称这样的反馈为负反馈。当控制量高于额定值时，就必须通过控制作用使被控制量降低，当被控制量低于额定值时，就必须通过控制作用使被控制量升高。此时，反馈控制器的输出是系统状态的函数，因而系统失效的出现与

否取决于固有的系统状态。

所以,研究非单调关联系统对于工程实际具有重要的普遍意义,是一个很有发展前途的研究方向。以下通过对一些非单调关联系统的典型实例的非单调性分析,说明非单调关联系统在工作实际中的一些应用。

(1) 实例 1

非单调关联系统在有些特殊情况下,当故障部件全部修理完毕后,此系统也可能仍是故障状态,而当在某几个部件故障时,此系统才正常。当然,系统刚开始工作时,全部部件完好,此时系统应该正常。以下通过一个简单系统的示例来说明系统的非单调性。

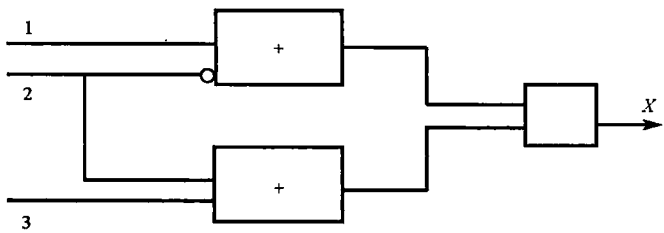

图 1.1-1 系统仿真图

如图 1.1-1,开始时部件 1、2、3 都正常,即仿真端 1、2、3 均为低电平 0,故系统状态为 0,属正常状态。开始工作以后,一旦 1 端由 0 变为 1 时,输出端 X 即由 0 变为 1,若此时 2 端也由 0 变为 1,也即 1、2 端同时变为 1 时,X 端却由 1 变为 0,即由故障转为正常,这就产生了非单调性。也就是所谓的非单调性的故障安全。

(2) n 中取 r 至 s 系统

此类系统颇具典型性,设在系统的 n 个组元中,有 r 至 s 个组元正常,则系统正常。如正常组元少于 r 或多于 s 个($s > r$),则系统故障,此类系统从系统结构函数上就可判断系统的非单调性,该

系统主要用于多处理机系统，在进行科学计算时，若全部 n 台处理机当中少于 r 台工作，则计算能力太小；若多于 s 台同时工作，则公用设备（例如总线）不能容纳那么多数据量，因而效率大降，故可认为 r 至 s 台处理机工作时系统正常，否则失效。类似情况也广泛地存在于任何具有固定容量的计算机网络中，尤其是微、小型机网络的广泛发展，这类系统可靠性模型显然具有普遍的理论和实际意义。

（3）反应堆功率自动调节系统

设系统的主要目的就是随时自动地通过电离室测出核反应堆的功率，将此测定值通过转换电路，经过电磁转换，反馈回系统控制电路，该控制电路再依据此信息通过控制核反应堆的自动棒的升降来自动调节堆芯的功率。因此控制系统存在反馈和负反馈，且部件是可修的，故此系统是一个可修的非单调关联系统。该系统在自动控制系统中是一个较典型的非单调关联系统，因该系统的工作依据主要是靠信息的反馈。堆芯中的功率过高或过低都会及时地反馈回控制电路，控制系统及时将新得到的数据与原额定数据进行比较，以此决定转换电路的工作是否正常。该非单调关联系统在实践中已得到了很好的运用。

（4）自旋卫星转速控制系统

一般自旋卫星至少有一对沿星体对称的切向安装的发动机，该发动机喷气使星体旋转，卫星入轨后，由姿控线路给出指令，使切向发动机喷气，卫星起旋。为了更有效地防止超转速，在星体对称轴的切向安装一对与切向发动机喷气方向相反的“反向发动机”。当锁定机构失灵或无法防止卫星转速持续增长到额定值上限的某一倍数时，逻辑线路便打开反向发动机的电磁阀，使反向发动机喷气，使卫星减速。该控制系统的最终目标就是防止自旋卫星转速失控（包括低转速和超转速两者），在此存在一种特殊的失效模式，即反向发动机阀门漏而喷气（故障）时，如果姿测、姿控和

切向发动机正常的话，由于反向漏喷而使卫星转速偏低，姿控就指令切向发动机多喷气。这样会迅速地把卫星携带的极其有限的气源耗光，造成不可挽救的失败。相反的，在反向发动机故障同时，如果姿控或切向发动机也有故障，不去加大喷气，倒还有挽救的可能，这里就出现了非单调关联性质的问题，某种单故障最危险，多一种故障和它同时出现反而会好一些，这叫故障安全性。

(5)考虑系统故障维修时序的系统也是一类典型的非单调关联系统

在单调关联系统中，由于任一故障部件的修复都会必然增加系统的可靠性，因而不会存在次序问题。而对于非单调关联系统，由于系统的故障安全性决定了故障次序相关性和维修有序性，因而各部件的失效顺序变得非常重要。例如，对于某一部件的失效事件 u，在其出现以前，顶事件才发生(故障危险)。因而，在故障安全状态和故障危险状态下，都必须讲究监控、修理次序。在制定修理次序时，首先应该考虑修理该部件。

(6)LP 模型

LP 模型是关于硝酸冷却器的，图 1.1－2 是它的流程图。

热硝酸经过阀门 1 流经热交换器 2，2 中通水冷却。在冷却后的硝酸出口处测温。出口硝酸温度信号送到温度控制器中，与预定的温度值相比较。如果出口处硝酸温度偏高，则开大冷却水控制阀门 5 以加大冷却水流量，使硝酸温度降下来；如果出口处硝酸温度偏低，则关小阀门 5 以减少冷却水流量。用这个温度反馈控制系统来达到把热硝酸冷却到给定温度值的目的(出口硝酸下一步送到反应器，工艺要求有适当温度)。如果冷却水泵发生事故(例如停电)，则自动关闭阀门 1，以防止进一步发生危险，这叫做“关泵前馈控制”。此外，为防止电火花，这里的温度测量、控制器、控制阀 5 和硝酸入口阀 1，都不是电动的，而是气动的，用压缩空气来操作。阀 5 是“有气开通”型，所以气压 P_7 下降导致流量 M_8

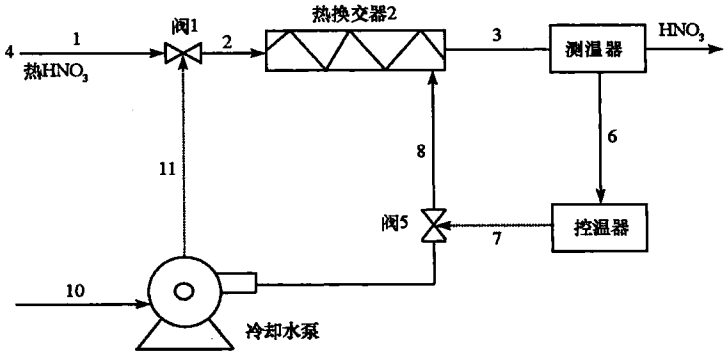

图 1.1-2　热硝酸冷却器

下降，阀 1 则是“有气关断”型。

以上可以看出，控制阀动作反向为故障危险，它和“无气压”、“控制器动作反向”、“低气压加测温器坏”、“低气压加控制器坏”等相结合，反而代表一种故障安全状态。显然，这是一个非单调关联系统。

以上介绍了在工程实际中常见到的几类非单调关联系统，而且这些系统已得到了较好的应用。当然，工程实际中并不仅仅局限于这几类非单调关联系统。在实践中还会经常遇到各种类型的非单调关联系统，这就需要具体问题具体分析。

1.2 非单调关联系统的基本概念

1.2.1 系统结构函数

系统可靠性研究的主要问题之一是确定系统可靠性与单元可靠性之间的定性定量关系。系统结构函数理论是一种研究系统可靠性的重要数学工具，利用系统结构函数，我们可以描述系统状态与其单元状态之间的逻辑关系，也可以获得一些系统结构单调与非单调特性和导致系统故障的故障模式。

定义 1.2.1 设系统 S 由 n 个单元组成，其状态向量为 $X=(x_1,x_2,\cdots,x_n)\in B^n$，布尔变量 $\phi\in B$ 表示系统 S 状态，若 X 与 ϕ 之间存在 $B^n\to B$ 的一个布尔函数 $=\phi(X)$，则称 $\phi(X)$ 为系统 S 的结构函数。

如果我们将单元状态变量 $x_i(i=1,2,\cdots,n)$ 和系统 S 状态变量 ϕ 视作 0－1 随机变量，那么分布 $F_i=P\{x_i=1\}$ 和 $F_s=P\{\phi(X)=1\}$ 分别是第 i 个单元和系统 S 的故障发生概率（也称失效分布或寿命分布）；而 $R_i=P\{x_i=0\}=1-F_i$ 和 $R_s=P\{\phi(X)=0\}=1-F_s$ 分别是第 i 个单元的可靠度和 S 的可靠度。

例如，对于如图 1.2－1 的两单元串、并联系统，它们的结构函数分别为 $\phi_1=x_1\cdot x_2$ 和 $\phi_2=x_1+x_2$，且有

$$F_{s_1}=P\{\phi_1=1\}=P\{x_1\cdot x_2=1\}=P\{x_1=1\}P\{x_2=1\}=F_1F_2,\tag{1.2.1}$$

$$F_{s_2} = P\{\phi_2 = 1\} = P\{x_1 + x_2 = 1\} = F_1 + F_2 - F_1F_2。$$

(1.2.2)

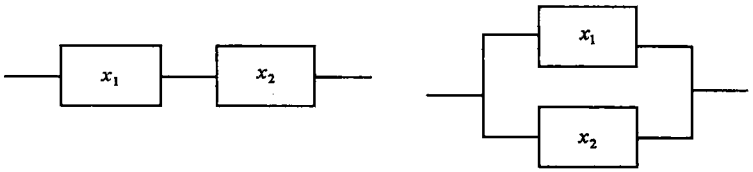

图 1.2-1　两单元串、并联系统

注意:(1.2.1)式和(1.2.2)式中分别用到了事件独立和不交化运算。

定义 1.2.2　结构函数 $\phi(X)(X\in B^n)$称为单调增加(单调减小)是指:$\forall X_1, X_2\in B^n$,若 $X_1\leqslant X_2$,则有 $\phi(X_1)\leqslant\phi(X_2)(\phi(X_1)\geqslant\phi(X_2))$。

定义 1.2.3　结构函数 $\phi(X)(X\in B^n)$称为非单调是指:$\phi(X)$既不是单调增加也不是单调减小的结构函数。

除了单调结构函数类之外,还有一类特别的非单调结构函数,它经过适当的变换仍可以化为单调结构函数。下面给出这类结构函数的定义。

定义 1.2.4　$\phi(X)$称为混合单调函数是指:如果存在变量 $X=\{x_1, x_2, \cdots, x_n\}$的某个子集$\{x_{i_1}, x_{i_2}, \cdots, x_{i_n}\}$,在 $\phi(X)$的表达式中,用 x'_{i_j}替换x_{i_j}或用x_{i_j}替换x'_{i_j}后,使得 $\phi(X)$变换成单调增加或者单调减少的函数。

如,对于 $\phi(X)=x'_1+x'_1x_2+x'_1x_3$,如果用 x_1 替换 x'_1,则 $\phi(X)$变换成单调增加的;如果用 x'_2 替换 x_2,用 x'_3 替换 x_3,则 $\phi(X)$变换成单调减少的函数。因此,$\phi(X)$是一个混合单调函数。