应用马尔科夫状态图法进行可靠性评估

胡宇驰*

(电子科技大学通信与信息工程学院 成都 610054)

【摘要】应用马尔科夫状态图法，对一个实际的硬件式可修容错计算机系统进行了可靠性评估。并针对两种容错方式分别得出各自的评估数据，通过实际的数据分析了其优缺点及最佳适用范围。

关 键 词 马尔科夫状态图法； 可靠性； 容错； 评估

中图分类号 TP202+.1

近年来，国内外在容错计算机可靠性性能评估方面的研究较为活跃，主要工作集中在以下几个方面：

1) 集成环境的开发：将系统仿真、软件实现的故障注入、系统可靠性与性能评估及目标系统硬件调试集成在一起，用于系统实现的各个阶段；

2) 针对具体目标系统的可靠性与性能评估与分析，采用模型与度量相结合的方法，失效数据的收集则采用目标系统实测的方法。

目前已有很多成熟的理论和方法，如蒙特卡洛法、二项式展开法、故障树法、最小路集(割集)法和马尔科夫状态图法，以及最新的通用随机 Petri 网法等，可对一些较为复杂的系统作可靠性分析和评估。本文采用马尔科夫状态图法，对一个实际的硬件式可修容错计算机系统作出了可靠性评估。

1 可靠性的基本概念

可靠性是指一个系统在一定的环境下，在所给定的时间内能按预定的要求完成一定功能的概率。它表明系统中若存在故障，只要不影响正常功能的执行和完成，系统仍然是可靠的。同时，可靠性是相对于一定的工作条件和一定的时间范围而言，而提高系统可靠性的一个基本方法就是使用容错技术，即一个系统在出现运行性故障时，能够依靠系统内驻的能力，保持系统连续正确地执行其程序和输入输出功能，则这个系统叫做故障容错系统。运行性故障是指系统中硬件的若干逻辑变量出现了不确定的逻辑值偏移或软件设计中的故障，而正确执行是指程序、数据和计算结果没有出错，且执行时间没有超出预定的时间[1]。

描述系统可靠性的基本参数包括可靠度、平均故障时间和平均故障间隔时间以及可维修度、平均维修时间和可用度等。

设有一个具有 N 个元件的系统，经运行时间 t 后，有 $F(t)$个元件失效，其余 $S(t)$个元件仍保持完好，则分别定义元件的可靠度 $R(t)$和不可靠度 $Q(t)$为

$$R(t)= S(t)/ N$$

$$Q(t)= F(t)/ N$$

式中 $R(t)$和 $Q(t)$都是时间 t 的函数。由计算可得

$$R(t) = \exp(-lt) \tag{1}$$

式(1)表明系统的可靠度与元件失效率 l 成指数关系。从开始研究可靠性以来，指数分布一直得

2000年10月8日收稿

* 男 24岁 在职硕士生

到广泛应用，因为它计算简单，参数的估计容易，且故障率具有可加性，所以当系统中各元件的故障都服从指数分布时，其系统的故障时间也应服从指数分布。

可用度是比可靠性应用更广泛的概念，且可表示可修系统。可用度是指部件在规定的条件下，在任意时刻正常工作的概率[2]。由于在时刻 t 正常工作的部件数一般都大于从 t=0 一直工作到时刻 t 的部件数，所以可用度 $A(t)$一般大于可靠度 $R(t)$，可用度又分为瞬时可用度和稳态可用度。

瞬时可用度 $A(t)$是指可修系统在时刻 t 处于正常状态的概率

$$A(t)=P\{\text{系统在时刻 } t \text{ 处于正常状态}\}$$

稳态可用度 A 是指系统在 $t\to\infty$时的可用度，又称为平稳状态的可用度，即

$$A=\lim_{t\to\infty}A(t) \tag{2}$$

2 应用马尔科夫状态图法求可维修系统的可靠性

2.1 马尔科夫状态图法概述

马尔科夫状态图法(Markov Status Graph)既适用于不可修系统，又适用于可修系统。除了要求系统满足马尔科夫过程外，还要求系统和部件只能取离散状态，即正常或失效两种状态；系统故障率 l 和维修率 m 均为常数；状态转换可在任一时刻进行，但在相当小的时间间隔 Δt 内，不会发生两个或两个以上的部件状态转换。以上的假设都适用于容错计算机系统的冗余结构，虽然不能解决所有冗余结构的可靠性评估问题，但对一些典型冗余结构，不失为一种可靠性评估方法。

马尔科夫状态图法处理问题的一般步骤为：

1) 根据系统各部件状态变化的规律，给出系统马尔科夫状态空间图，状态转移率一般是指失效率和维修率；

2) 根据系统状态转移图列出系统状态转移概率矩阵 $\boldsymbol{T}$，并给出状态方程系数矩阵 $\boldsymbol{A}=|\boldsymbol{T}-\boldsymbol{U}|$，列出状态方程；

3) 根据状态方程求出各状态概率 $P_i(t)$，根据 $P_i(t)$的定义得出可靠度、不可靠度等指标，其计算可借助拉氏变换。

2.2 利用马尔科夫状态图法对一个硬件式容错计算机系统进行可靠性评估

下面针对一个硬件式容错计算机系统，运用整体马尔科夫模型来评估其性能指标。整个系统采用双总线结构，包括3个处理器、2个 I/O 接口设备和3个存储器。假设所有功能相同的设备都有相同的属性，即失效率、维修率等指标都相同。

对于构造容错系统整体的马尔科夫模型，本文没有采用专用软件，而是在构件模型时作了一些假设，以便把系统复杂度控制在可计算范围内，即：

1) 故障的发生是不相关的，部件的失效率和维修率是常数；

2) 故障不传播；

3) 故障检测与系统重构非完善，覆盖率为常数，在算法上使用变步长的 Runge-Kutta 方法。

2.2.1 处理器采用多数表决方式

通过以上假设，可以构造出处理器采用多数表决方式下的马尔科夫状态图。由于状态过多，马尔科夫状态图过于复杂，本文仅给出状态 p_0的转移过程，如图1所示。图中状态(3,3,2,2 p_0)表示在某时刻状态 p_0有(3Processor,3Memory,2I/O,2Bus)。假设经过一段时间 Δt，有1个处理器失效，在此过程中要进行故障检测与系统重构，切除故障模块。设重构成功的概率为 c_p，则转移到 p_1的概率为$3l_pc_p\Delta t$, p_0向 p_2、p_3、p_4跃迁的过程依此类推，当系统处在其他状态时则与 p_0状态雷同。在该冗余方式下，可以得到21个状态的 Markov 状态转移图，分别是 $p_0, p_1,\cdots, p_{20}$。

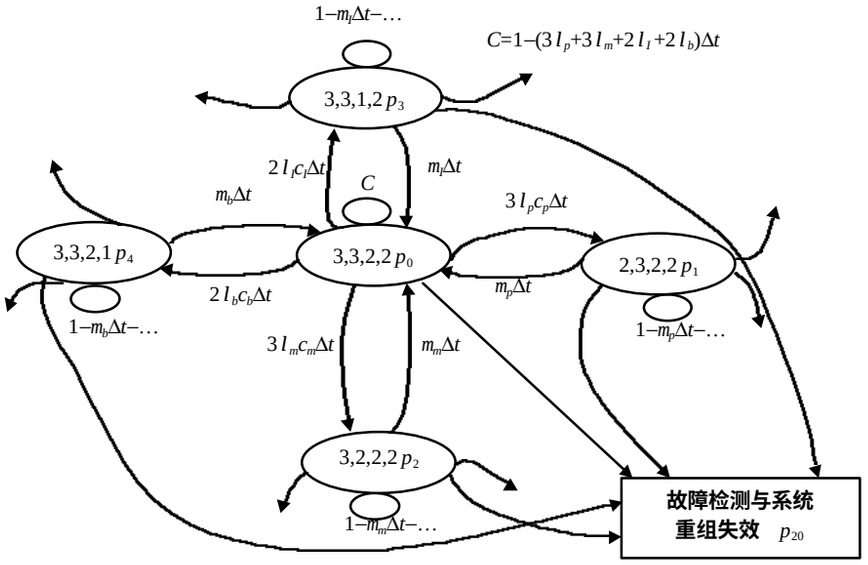

图1　处理器采用多数表决方式下的马尔科夫状态转移图

为了减少可变参数的数量，假定： 1) **所有部件的失效率都相等，即** $l_p=l_m=l_b=l_I=l$；2) **所有部件的故障检测和系统重组的覆盖率都相等，即** $c_p=c_m=c_b=c_I=a$；3) **所有部件的维修率都相等，即** $m_p=m_m=m_b=m_I=m$。

由马尔科夫链得到马尔科夫状态微分方程如下

$$[p_0(t)', p_1(t)', \cdots, p_{19}(t)', p_{20}(t)']=[p_0(t),p_1(t),\cdots, p_{19}(t),p_{20}(t)]A \tag{3}$$

$$\boldsymbol{A}=\begin{bmatrix} -10\,l & 3\,l\,a & 3\,l\,a & \wedge & \wedge & 0 & 0 & 10\,l\,(1-a) \\ m & -9\,l-m & 0 & \wedge & \wedge & 0 & 0 & 7\,l\,(1-a) \\ m & 0 & -9\,l-m & \wedge & \wedge & 0 & 2\,l & 7\,l\,(1-a) \\ \wedge & \wedge & \wedge & \wedge & \wedge & \wedge & \wedge & \wedge \\ \wedge & \wedge & \wedge & \wedge & \wedge & \wedge & \wedge & \wedge \\ 0 & 0 & 0 & \wedge & \wedge & -8m & 0 & 0 \\ 0 & 0 & m & \wedge & \wedge & 0 & -8m & 0 \\ 0 & 0 & 0 & \wedge & \wedge & 0 & 0 & 0 \end{bmatrix} \tag{4}$$

式中　$\boldsymbol{A}$ 为状态转移概率矩阵，这一矩阵方程(方程组)称为查普曼–柯尔莫戈罗夫(Chapman-Kolmoqorov)**方程，由此可以解出系统处于任意状态的概率**[3]。

由于状态 p_{16}, p_{17}, p_{18}, p_{19}, p_{20}**分别表示处理器失效，存储器失效、**I/O **失效、总线失效和故障检测与系统重组失效，所以系统的瞬间可利用度** $A(t)$**为**

$$A(t)=1-p_{16}(t)-p_{17}(t)-p_{18}(t)-p_{19}(t)-p_{20}(t) \tag{5}$$

在计算该系统的可靠度时，将状态 p_{16}，p_{17}，p_{18}，p_{19}，p_{20}**作为吸收状态。**

对式(5)**应用龙格–库塔方法求此微分方程的数值解。表**1、**表**2**分别是在不同的参数下得到的系统可用度和可靠度值(精度为**10^{-10}**)。**

表1 多数表决方式下模块失效率对系统可靠度的影响(m=0.9 a=0.99)

t	l			
	0.001	0.000 1	0.000 01	0.000 001
1	0.999 883 060 5	0.999 988 930 5	0.999 998 899 3	0.999 999 890 0
10	0.998 835 712 9	0.999 897 449 6	0.999 989 884 5	0.999 998 989 8
100	0.988 352 787 6	0.998 982 387 6	0.999 899 733 6	0.999 989 988 3
1 000	0.889 388 026 0	0.989 877 699 2	0.998 998 672 1	0.999 899 977 7
10 000	0.309 659 314 2	0.903 272 164 9	0.990 032 595 8	0.999 000 316 9
100 000	0.000 008 106 1	0.361 567 593 0	0.904 680 686 9	0.990 048 109 7

表2 多数表决方式下模块失效率对系统可用度的影响(m=0.9 a=0.99)

t	l			
	0.001	0.0001	0.00001	0.000001
1	0.999 991 176 5	0.999 999 245 1	0.999 999 925 8	0.999 999 992 7
10	0.999 990 129 0	0.999 999 234 6	0.999 999 925 7	0.999 999 992 6
100	0.999 990 128 7	0.999 999 234 6	0.999 999 925 7	0.999 999 992 6
1 000	0.999 990 128 7	0.999 999 234 6	0.999 999 925 7	0.999 999 992 6
10 000	0.999 990 128 7	0.999 999 234 6	0.999 999 925 7	0.999 999 992 6
100 000	0.999 990 128 7	0.999 999 234 6	0.999 999 925 7	0.999 999 992 6

2.2.2 处理器采用单工贮备方式 π

设3个处理器采用单工贮备冗余方式，其中1个处理器处于工作状态，2个处于贮备状态。对于贮备模块来说，又分为热贮备、温贮备和冷贮备三种贮备模式。根据上面的假设条件，得出系统的马尔科夫状态图如图2所示。

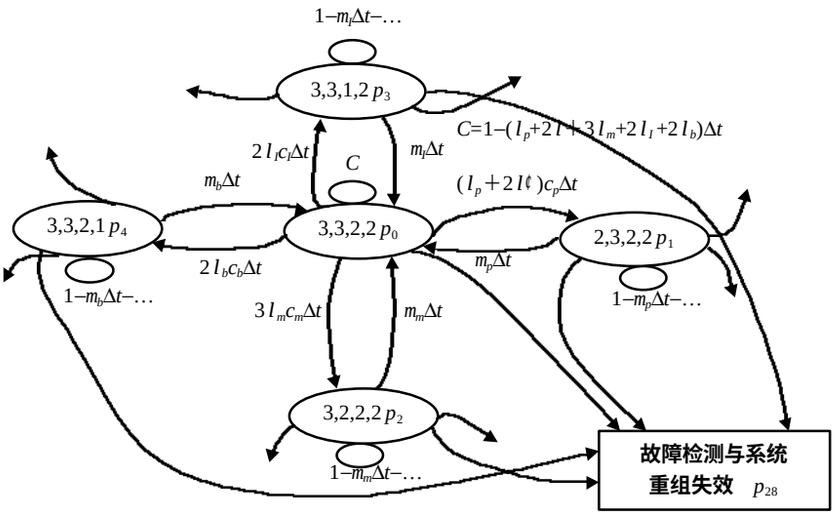

图2 处理器采用单工贮备方式下的马尔科夫状态转移图

在图2中，设贮备的处理器的模块失效率为l'，由 p_0~p_1的转移概率为(l_p+2l')$c_p\Delta t$，p_{28}为故障检测与系统重组失效状态。设某时刻设系统处于 p_0状态，经过 Δt 时间，有可能发生处理器失效、存储器失效、总线失效或 I/O 设备失效（根据前面的假设，某时刻只能一种部件失效），系统相应

由 p_0状态转移到 p_1、p_2、p_3和 p_4。如果在故障检测与系统重组的过程中发生故障，从而引起系统失效，系统则由 p_0状态转移到 p_{28}状态，转移概率为$((l_p+2l')(1-c_p)+3\lambda_m(1-c_m)+2l_l(1-c_l)+2l_b(1-c_b))\Delta t$，当系统处于其他状态时与 p_0状态雷同。

同第一种冗余模式的假设，可以得出第三种冗余模式下的可靠度和可用度如表3、4所示。

表3　单工温贮备方式下模块失效率对系统可靠度的影响(m=0.9　a=0.99)

t	l			
	0.001	0.000 1	0.000 01	0.000 001
	0.000 5	0.000 05	0.000 005	0.000 000 5
1	0.999 896 670 2	0.999 990 056 7	0.999 999 909 6	0.999 999 901 0
10	0.998 994 643 4	0.999 908 133 5	0.999 990 900 3	0.999 999 090 9
100	0.989 972 329 1	0.999 088 822 9	0.999 909 807 1	0.999 990 990 0
1 000	0.903 839 388 5	0.990 932 286 0	0.999 099 236 6	0.999 909 984 3
10 000	0.347 647 888 2	0.912 916 093 0	0.991 029 556 6	0.999 100 287 9
100 000	0.000 023 087 0	0.400 540 990 9	0.913 829 617 0	0.991 039 296 4

表4　单工温贮备方式下模块失效率对系统可用度的影响(m=0.9　a=0.99)

t	l			
	0.001	0.000 1	0.000 01	0.000 001
	0.000 5	0.000 05	0.000 005	0.000 000 5
1	0.999 995 040 2	0.999 999 559 1	0.999 999 956 5	0.999 999 995 8
10	0.999 994 020 6	0.999 999 554 9	0.999 999 956 4	0.999 999 995 7
100	0.999 994 016 8	0.999 999 554 9	0.999 999 956 4	0.999 999 995 7
1 000	0.999 994 016 8	0.999 999 554 9	0.999 999 956 4	0.999 999 995 7
10 000	0.999 994 016 8	0.999 999 554 9	0.999 999 956 4	0.999 999 995 7
100 000	0.999 994 016 8	0.999 999 554 9	0.999 999 956 4	0.999 999 995 7

3　结　论

从表1~4可以看出，在同一失效率下，随着时间的增长，容错系统的可用度开始下降，最后收敛于一个常数，而可靠度却随着时间的增长趋于零。随着失效率降低，系统的可靠度和可用度都提高，与容错系统的实际情况较吻合。

从表1和表3中还可以看出，由同样的部件构成的冗余系统，由于采用的容错方式不一样，结果对系统的可靠度和可用度有很大的影响。以上面的模型为例，在第一种方式下，3个处理器采用表决方式，可以得到短时间内的高可靠度，而且这种方式还受到表决器可靠度的限制，一般采用多级表决方式来提高表决器的可靠度。在第二种方式下，3个处理器采用三模单工贮备方式工作，即1个处理器处于工作状态，其他2个处理器处于贮备状态。对于贮备的部件，分别可以采用热贮备、温贮备和冷贮备方式。对于电子类产品，采用热贮备或温贮备方式最好。在同样的系统参数条件下，采用贮备方式可得到较高的可靠度和可用度，但故障检测与系统重构的装置较复杂。

参 考 文 献

1 杨士元. 数字系统的故障诊断与可靠性设计(第二版). 北京: 清华大学出版社, 2000

2 杨为民, 阮 镰. 可靠性、维修性、保障性总论. 北京: 国防工业出版社, 1998

3 杨孝宗. 容错技术与 STRATUS 容错计算机. 哈尔滨: 哈尔滨工业大学出版社, 1998

4 Wu Chuanzhi, Fu Shilu, Jiang Yinhua. Matchment of MMP with two-state semi-MMP. Journal of University of Electronic Science and Technology of China, 1999, 28(3):320~323[吴传志, 付诗禄, 蒋银华. 调制马氏链与两状态调制半马氏链的匹配. 电子科技大学学报, 1999, 28(3): 320~323]

5 Qing Zhiguang, Wang Wenyong. Reliability and security of network authentication service. Journal of University of Electronic Science and Technology of China, 1997, 26(2): 190~193[秦志光, 汪文勇. 网络服务可靠性和安全性. 电子科技大学学报, 1997, 26(2): 190~193]

Evaluation of Reliability of a Fault-tolerance Computer System by Markov Status Graph

Hu Yuchi

(Inst. of Telecommunication & Information Eng., UEST of China Chengdu 610054)

Abstract In this paper, the reliability of a fault-tolerance computer system is evaluated by Markov status graph. Majority voting method and single store method are used to evaluate the reliability and usability of the fault-tolerance system. Through practical computation, the comparison data are also given.

Key words Markov status graph; reliability; fault-tolerance; evaluate