第14卷 第2期 郑州工学院学报 Vol.14 No.2
1993年 6 月 Journal of Zhengzhou Institute of Technology Jun. 1993

$(t1/t\frac{1}{2})/s$——诊断系统的模型及优化设计*

徐江锋

(郑州工学院计自系)

摘 要: 由于计算机技术的迅速发展，故障诊断理论已运用到了许多计算机系统中，以便提高系统的可靠性。本文在黄/陈[1]诊断模型的基础上，提出了一个更实际的三值诊断模型，并在此模型下给出了一种新的故障诊断策略——$(t1/t_2^1)/s$——可诊断，最后又着重研究了该系统的优化系统 D_{1A}。研究结果表明，$(t1/t_2^1)/s$——可诊断系统与 $t(=t_1+t\frac{1}{2})/s$——可诊断系统相比，要少用近一半的测试边，与 t——可诊断系统相比，要少用近四分之三的测试边。

关键词: 系统诊断，三值逻辑，D_{1A} 系统。

中国图书分类号: TP277

随着计算机的不断发展，它的应用范围越来越广泛，人们经常地利用计算机系统（如多机系统，网络及分布式系统等）来进行各种各样的信息传递及信息处理。然而，有时会因系统中部分子系统或部件发生故障，致使整个系统的计算结果都发生错误，如果不能有效地识别出系统中发生故障的子系统，那么整个系统都不能正常地运行。因此，如何识别一个系统中的子系统是否发生故障，从而提高整个系统的可靠性及可用性，是计算机领域的一个重要研究课题，计算机系统诊断所要解决的主要问题也正在于此。

系统诊断的基本思想是由 Preparata 等人[2]在 1967 年提出的，在前二十年的时间里，所有的研究都是把系统划分成"无故障"和"故障"两部分，然而，在许多复杂的计算机系统中，它的每个子系统都是由任务处理器与通讯处理器两部分组成的，因此，用三值逻辑来描述和分析这样的系统更加合适，这一思想是由黄开源[1]等人在 1985 年提出的。本文根据这一思想提出了一个更加实际的三值诊断模型。

系统诊断中的一个重要诊断策略——t/s——诊断是由 Friedman[3]等人在 1975 年提出的，它的基本思想是当系统中发生故障的子系统数目不超过 t 时，可把所有的故障子系统

* 收稿日期: 1992-12-03

限制在一个数目不超过 s(>t)的子集中，这样做可以大大降低对系统中测试数目的要求．本文在新的模型下，研究了$(t1/t\frac{1}{2})/s--$可诊断，并着重研究了优化系统 D_{1A} 的$(t1/t\frac{1}{2})/s$--可诊断．研究结果表明，与 t/s—可诊断系统相比，$(t1/t\frac{1}{2})/s--$可诊断系统可少用近一半的测试边，而与 t—可诊断系统相比，则少用近四分之三的测试边，其中$t=t1+t\frac{1}{2}$．这意味着我们可花费小的代价得到高的系统可靠性，因而，它可应用于更加广泛的多机网络系统中．

1 诊断模型与$(t1/t\frac{1}{2})/s--$可诊断

在许多多机系统，分布式系统及计算机网络中，每个子系统都是由一个任务处理器和一个通讯处理器组成的，通讯处理器专门负责子系统间的信息传递，两个处理器能独立地进行工作，也即当任务处理器发生故障时，通讯处理器仍有可能正确地进行子系统间的信息传递．但是，当一个子系统的通讯处理器发生故障时，不管它的任务处理器状态如何，都不能对其它子系统进行正确的测试．基于上述分析，并在黄/陈[1]模型基础上，我们提出了新的模型假设．

首先给出对子系统的划分方法:

① 如果一个子系统无故障，则称为 0 型子系统，用○表示．

② 如果一个子系统仅任务处理器发生故障，而通信处理器无故障，则称之为 1/2 型子系统，用○表示．

③ 如果一个子系统的通讯处理器发生故障，则称之为，型子系统，用○表示．

新的模型假设为:

① 如果一个无故障子系统，即 0 型子系统，被另外的无故障子系统所测试，则测试输出为 0．

② 如果一个 1/2 型子系统被一个 0 型子系统测试，则测试输出为 1/2．

③ 如果一个 1 型子系统被一个 0 型子系统测试，则测试输出为 1．

④ 如果一个子系统被一故障子系统测试，不管它是 1/2 型的还是 1 型的，则测试输出是 0，1/2 或 1，亦即是完全不确定的．

上面的假设也可用图1表示：

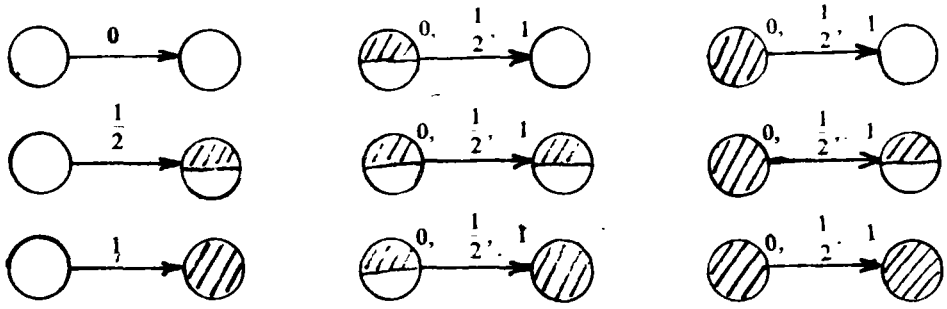

图 1　三值诊断模型的测试输出

特别应强调的是，对于 1／2 型故障子系统，在测试期间，我们可利用其通讯处理器来正确地传递信息，产生一些虚拟测试，如图2中虚线所示．这样我们可得到更多的测试信息，有利于系统诊断．

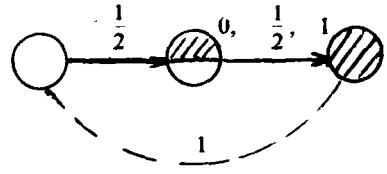

图 2 一个虚拟测试的例子

对任一系统 S，假若它有 n 个子系统，那么我们可用有向图 G＝(V，E)来表示．其中 V＝{u_1，u_2，…，u_n}是 S 的 n 个子系统集．且(u_i，u_j)∈E，当且仅当子系统 u_i 对于系统 u_j 进行测试，(u_i，u_j)的测试输出用边权 ω_{ij} 来表示．S 的所有测试输出组成的集合称之为 S 的一个症候．

定义 1：设图 G＝(V，E)代表 S，则定义故障集$F1/F\frac{1}{2}\therefore V$为：

$F1/F\frac{1}{2}=F1\bigcup F\frac{1}{2}$，且

若$u_i\in F1$，则u_i是1型子系统；

若$u_i\in F\frac{1}{2}$，则u_i是$\frac{1}{2}$型子系统．

定义 2：设 $G_\omega=(V,E)$是一带权有向图，$F1/F\frac{1}{2}$ 是 V 的子集，如果 $F1/F\frac{1}{2}$ 满足：

1) 对所有的$u_i\in(V-F1/F\frac{1}{2})$和$u_j\in F1$，$\omega_{ij}=1$；

2) 对所有的$u_i\in(V-F1/F\frac{1}{2})$和$u_j\in F\frac{1}{2}$，$\omega_{ij}=\frac{1}{2}$；

3) 对所有的u_i，$u_j\in(V-F1/F\frac{1}{2})$，$\omega_{ij}=0$

则称$F1/F\frac{1}{2}$是一个相容故障集．

定义 3：系统，$G=(V,E)$是$(t1/t\frac{1}{2})/s--$可诊断的，当且仅当在系统中$\frac{1}{2}$型故

障子系统的数目不超过 $t\frac{1}{2}$，1 型故障子系统的数目不超过 $t1$ 时，对任意的症候，所有的故障子系统都能被确定在一个数目不超过 $s \geqslant t1 + t\frac{1}{2}$ 的子系统集中.

定理 1: 系统 S 是 $(t1 / t\frac{1}{2}) / s - -$ 可诊断的，当且仅当对任给的症候，它的所有相容故障集 $(F1 / F\frac{1}{2})$，……，$(F1 / F\frac{1}{2})_k$，满足. $|\bigcup_{i=1}^{k}(F1 / F\frac{1}{2})_i| \leqslant S$. 其中，$|(F1)_1| \leqslant t1$，$|(F\frac{1}{2})_i| \leqslant t\frac{1}{2}$，$i = 1, 2, \cdots, k$.

此定理可由定义 3 直接推出.

2 D_{1A} 系统——一类$(t1 / t\frac{1}{2}) / s - -$可诊断系统

这一部分将着重研究一类优化的$(t1 / t\frac{1}{2}) / s - -$可诊断系统——$D_{1A}$. 首先介绍 $D\delta A$ 系统，而后讨论其特殊情形，即 D_{1A} 系统.

定义 4: 系统 G= (V, E) 是 $D\delta A$ 系统，当且仅当对所有的边$(u_o, u_j) \in E$，满足 $(j-i) \bmod n = (\delta \cdot m) \bmod n$，其中 $\delta < n$，$m = 1, 2, \cdots$，$A < n$，$V = \{u_1, u_2, \cdots, u_n\}$.

令 $\delta = 1$，那么 G= (V<E) 就是一个 D_{1A} 系统. 对于 PMC 模型[2]，如果系统 G= (V, E) 是 t--可诊断的，那么要求 A>t，即 G= (V, E) 至少要有 n·t 条测试边；Friedman[5]证明了如果 A>[t/2]，那么 D_{1A} 系统是 t/s 可诊断的，换句话说，我们可以仅用 n·[(t+1)/2]条测试边构造一个 t/s--可诊断系统，显然，这样的系统比原来的系统少用了近一半的测试边. 由于任一系统的任务处理器要比通讯处理器复杂，所以，在新的模型中，假定$t1 \leqslant t\frac{1}{2}$是合理的. 令，$t = t1 + t\frac{1}{2}$我们将证明 D_{1A} 系统当 A>[t1/2]时，是$(t1 / t\frac{1}{2}) / s - -$可诊断的，也就是说，存在一类$(t1 / t\frac{1}{2}) / s - -$可诊断系统，仅需 n·[(t1+1)/2]或 n·[(t+1)/4]条测试边.

引理 1[4]: 若系统 S 是$(t1 / t\frac{1}{2}) / s - -$可诊断的，则$n \geqslant 2(t1 + t\frac{1}{2}) + 1$，其中 n 是 S 中子系统的数目.

引理 2[5]: 如果$(t1 / t\frac{1}{2}) / s - -$可诊断系统 G=(V, E)的子图 G′仅包含 z 个故障子系统，那么在 G--G′中产生测试响应 $\underbrace{0\ 0\ \cdots\ 0}_{t1 + t\frac{1}{2} - z}$ 的测试链$C(|C| = t1 + t\frac{1}{2} - z + 1)$的最后

一个子系统是无故障的.

定义 5: 设 G= (V, E) 是一个 D_{1A} 系统, 定义$F|_i$为 G 中第 i 个最大的连续 1 型故障子集, 它满足$F|_i \bigcup F|_j$(i≠j)不产生新的最大连续 1 型故障子集; 且定义 $f_i=|F1_i|$.

研究图 3 所表示的 D_{12} 系统, 该系统包含 u_0, u_1, …, u_8 九个子系统, 其中 u_2, u_3, u_6 是 1 型故障子系统, u_7 是 1/2 型故障子系统, 那么 $F|_1=\{u_2, u_3\}$, $F|_2=\{U_6\}$, $f_1=2$, $f_2=1$, 且 $F|_1| \ |F|_2=\{u_2, u_3, u_6\}$,, 不构成新的最大连续 1 型故障子集.

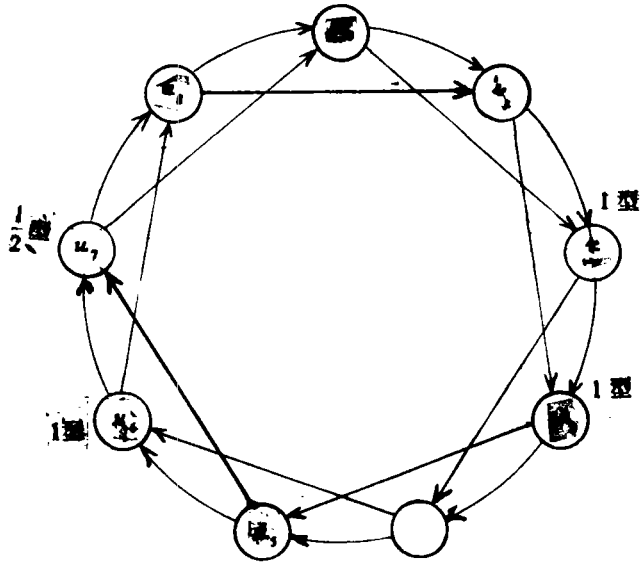

图 3 一个 D_{12} 系统

定理 2: 任给一个 D_{1A} 系统如果 A>[t1/2], 那么它是$(t1/t\frac{1}{2})/s--$可诊断的. 其中$t1+t\frac{1}{2} \leqslant S \leqslant 2(t1+t\frac{1}{2})-A$.

证明: 假设 G= (V, E) 是一个 D_{1A} 系统, A>[t1/2], |V|=n. 只要证明了在任一症候下, 都能识别出 S_a<S 个子系统, 包含 G 的所有故障子系统, 那么根据定理 1, G= (V, E) 一定是$(t1/t\frac{1}{2})/s--$可诊断的. 设$F1_1 \bigcup \frac{F}{2} \bigcup \cdots \bigcup F/k$代表了 G 中的所有 1 型故障子系统, 现在我们分两种情形来讨论.

情形 1: 假设对所有的 $F1_i$, i=1, 2, ……, k, 都有 f_i<A, 那么 G 中的任一无故障子系统及 1/2 型故障子系统, 都至少被一个无故障子系统或 1/2 型故障子系统所测试, 通过这些 1/2 型故障子系统, 可产生一些虚拟测试, 因而 G 中就一定存在一个包含全部无故障子系统的环. 若设$T1$, $T\frac{1}{2}$分别代表 G 中 1 型, 1/2 型故障子系统的数目, 则对任意症候, G 中一定存在一个长度至少为$n-T1-T\frac{1}{2}$的全为 0 的响应环. 由引理 1

知，$n \geqslant 2(t1 + t\frac{1}{2})^H$，而 T1<t1，$T\frac{1}{2} \leqslant t\frac{1}{2}$，从而$n - T1 - T\frac{1}{2} > t1 + t\frac{1}{2}$，所以该响应环所对应的所有子系统都是无故障的，剩余子系统都是故障的，因而$S_a = T1 + T\frac{1}{2} \leqslant t1 + t\frac{1}{2} \leqslant S$.

情形 2：假设存在 $F1_i$(1<i<k)，有 f_i>A，因 A>[t1/2]，且 T1<t1，所以只可能存在一个这样的 $F1_i$，不失一般性，可假设它为 $F1_1$，即 f_1>A，而剩余的一切 $F1_i$ 均有 f_i<A．设$F1_1 = \{u_{1+1}, u_{1+2}, \cdots, u_{1+f_1}\}$，则除$u_{1+f_1+1}$外所有的 0 型，1/2 型子系统都至少被一个 0 型或 1/2 型子系统测试，通过这些 1/2 型子系统，我们可执行一些虚拟测试，使得所有的 0 型子系统，除u_{1+f_1+1}（若是的话）外都能被一个 0 型子系统测试，这样在系统中一定存在一个仅包含 0 型子系统，也即无故障子系统的测试链 C，其长度为 $n - T1 - T\frac{1}{2}$，响应模式为 $R = \begin{matrix} 0 & 0 & \cdots & 0 \\ & & \cdots & \\ & & & n - T1 - T\frac{1}{2} - 1 \end{matrix}$．因 $n - T1 - T\frac{1}{2} - 1 \geqslant 2(t1 + t\frac{1}{2}) + 1 - T\frac{1}{2} - T1 - 1 \geqslant 2(t1 + t\frac{1}{2}) - (t1 + t\frac{1}{2}) = t1 + t\frac{1}{2}$，所以，根据引理 2，链 C 的最后$n - T1 - T\frac{1}{2} - t1 - t\frac{1}{2}$个子系统是无故障的．设 u_x 是链 C 的最后一个子系统，u_x 则是无故障的．若 $u_x = u_i$，则 u_x 能识别出 $F1_1$ 中的前 A 个子系统为 1 型故障子系统，若 $u_x \neq u_i$，则 u_x 能够通过一些虚拟测试识别出 $F1_1$ 中的前 A 个元素为 1 型故障子系统．再利用引理 2，我们又可识别出 A 个新的无故障子系统，加上前面识别出的$n - T1 - T\frac{1}{2} - t1 - t\frac{1}{2}$个，此时，共识别出了$n - T1 - T\frac{1}{2} - t1 - t\frac{1}{2}$+A 个无故障子系统．若新识别出的 A 个无故障子系统．又可识别出一些新的故障子系统，那么，再利用引理 2，又可识别出同等数目的新的无故障子系统．重复上述过程，直到不能再识别出新的故障子系统为止．假设 m 是识别出的所有故障子系统数（m>A），则识别出的无故障子系统数为，$n - T1 - T\frac{1}{2} - t1 - t\frac{1}{2} + m$，因而系统中未被识别出的子系统及已识别出的故障子系统总数为：

$$S_a = n - (n - T1 - T\frac{1}{2} - t1 - t\frac{1}{2} + m) = T1 + T\frac{1}{2} + t1 + t\frac{1}{2} - m$$

最坏的情况是$T1 = t1$，$T\frac{1}{2} = t\frac{1}{2}$，$m = A$，此时$S_a = 2(t1 + t\frac{1}{2}) - A$，

故$t1 + t\frac{1}{2} \leqslant S_a \leqslant 2(t1 + t\frac{1}{2}) - A$.

[证毕]

下面我们通过一例来说明该定理．

例：考虑图 4 中的 D_{12} 系统 G=（V，E），V={u_0，u_1，……u_{10}}，其中 u_1，u_2 是 1

型故障子系统，u_4，u_5，u_8是1/2型故障子系统，则$t1=2$，$t\frac{1}{2}=3$，$F1_1=\{u_1, u_2\}$，因u_4是1/2型的故障子系统，u_3可通过u_4对u_6施加一虚拟测试，因而G=（V，E）中存在一个链C仅包含无故障子系统，即$u_3 \xrightarrow{\text{虚拟}} \rightarrow u_6 \rightarrow u_7 \rightarrow u_9 \rightarrow u_{10} \rightarrow u_0$，它的测试响应为

$$R=\begin{matrix}0\ 0\ 0\ 0\ 0\\ 11-3-2-1=5\end{matrix}$$

，所以可识别出$n-T1-T\frac{1}{2}-t1-t\frac{1}{2}=11-2-3-2-3=1$个无故障子系统，即$u_0$。通过$u_0$又可识别出$u_1$，$u_2$为1型故障的，从而又可识别出$u_{10}$，$u_9$是无故障的，并且不能再识别出新的故障子系统与无故障子系统，故

$$S_a=11-3=8=2(t1+t\tfrac{1}{2})-A.$$

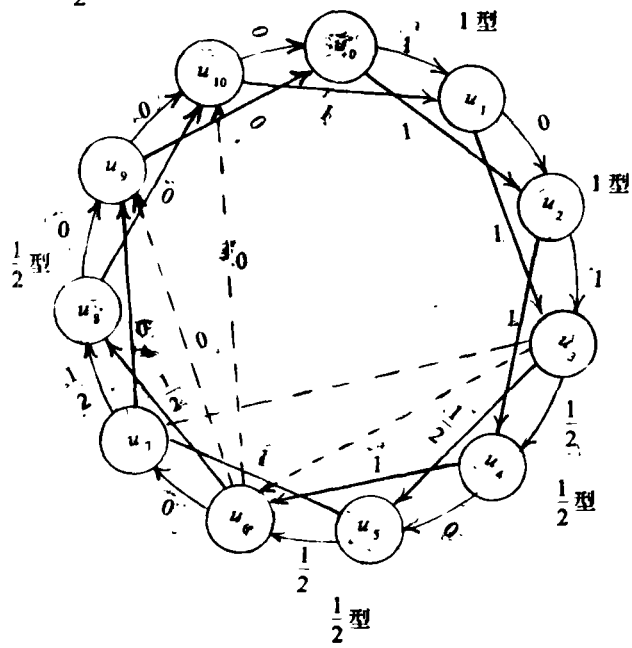

图4 一个有测试输出的D_{12}

从此例可以看出D_{12}系统是（2/3）/8--可诊断的，可以难验证它不是5/8--可诊断的，更不是5--可诊断的。一般地D_{1A}，系统是t/s--可诊断的，至少要求A>3，要是t--可诊断的，则要求A>5。所以，$(t1/t\frac{1}{2})/s$--可诊断系统与t/s--可诊断相比，要少用近一半的测试边，与t--可诊断相比，则要减少近四分之三的测试边。

参 考 文 献

(1) K. Huang and T. chen, "Three-valued System diagnosis," Proc. 15th IEEE Int. Symp. MVL, pp. 356—360, May 1985.

(2) F. Preparata, G. Metze and R. T. Chien, "On the connection assignment ptoblem of diagnosable systems." IEEE Trans. Electron. Comput., Vol. EC—16, pp. 848—854, Dec. 1967.

(3) A. D. Friedman, "A new measure of digital system diagnosis," in 1975 Proc. Int. Symp. Fault-Toleromt Computing, pp. 167—170, June 1975.

(4) K.Huang and J. Xu. "Characterization of $(t1/t_2^1)/s$—diagnosability, "Proc. 19th IEEE Int. Symp. MVL. May 1989.

(5) S. Karunanithi and A.D.Friedman, "Analysis of digital system using a new measure of system diagnosis," IEEE Trans. Comput., Vol. C—28, No. 2, pp. 121—133, Feb. 1979.

$(t1/t_2^1)/s$—Diagnosable System: Model and Design

Xu Jiang Feng

(Zhengzhou Insititute of Technology)

Abstract: Due to recent advances in computer technology, the theory of system—level fault diagnosis has been applied to computer systems for achieving higher relability. In this paper, a new measure of system diagnosis, $(t1/t_2^1)/s$—diagnosability, is used to study the diagnosability of digital systems. A generalized three-valued model, based on the Hang/Chens work [1], is proposed. D_{1A}systems are considered and constructed. The results show clearly that for $(t1/t_2^1)/s$—duagnosable systems, a reduction of almost one half in the number of the test links can be achieved in comparison to $t=(t1+t_2^1)/s$ a—diagnosable system [3]. Morever, as compared with $t(t1+t_2^1)$—diagnosable systems[2], a $(t1/t_2^1)/s$—diagnosable system can be constructed with a reduction of three fourths in the number of the tests.

Keywords: System Diagnosis, Three-Valued Logic, D_{1A}Systems.