③

14-20

系统级故障诊断的一个三值模型*

A Three-Valued Model of System-Level Fault Diagnosis

TP306.3

杨晓帆　　　何中市　　　陈廷槐
Yang Xiaofan　　He Zhongshi　　Chen Tinghuai
（重庆大学计算机研究所，重庆，630044；第一作者 32 岁，男，副教授，博士）

A

摘　要　提出了系统级故障诊断的一个三值模型，定义了一类可诊断系统，给出了其特征，并研究了它们的最优设计问题。

关键词　故障诊断；多处理机系统；最优设计　　三值模型

中国图书资料分类法分类号　TP306.3

ABSTRACT　We propose a three-valued model of system-level fault diagonsis, define a class of diagnosable systems, give a characterization of them, and study their optimal design.

KEYWORDS　fault diagnosis; multiprocessor system; optimal design

0　引　　言

随着多处理机系统规模的扩大和对系统可用性要求的提高，追切需要快速识别系统中的故障处理机，系统级故障诊断的基本思想是：首先让系统中的处理机相互测试，然后对测试结果进行分析，找出故障处理机[1~4]。

对系统级故障诊断的研究大都是在二值模型上进行的，即是说每个处理机只有两种可能状态：故障或无故障，并且每个测试只有两个可能结果：通过或未通过。二值模型的缺点是太简单，在很多情况下不能满足实际需要。因此，在多值模型上研究系统级故障诊断，这已成为重要的研究课题[5~9]。例如：Butler[5]模型中测试有三种可能结果：通过，未通过，无结果。Sengupta 和 Sen[6,7]，Kozlowski 和 Krawczyk[8]研究的模型中每个处理机有三种可能状态：无故障，永久故障，间歇故障。黄开源和陈廷槐[9]模型中每个处理机由任务处理器和通信处理器两部分组成，每个处理机有三种可能状态：无故障，任务处理器有故障而通信处理器无故障，通信处理器有故障。

在传统的二值 PMC 模型中，假设测试程序总能覆盖目前发生的所有故障。这是很难做到的。本文提出了一种更符合实际的三值 PMC 模型，进而定义了一类新的可诊断系统，给出了其特征，并且研究了相应的最优设计问题。

---

* 收文日期　1996-01-25
国家自然科学基金资助项目

1　术语和符号

本文假定处理机只发生永久故障。

为了诊断，可以把多处理机系统看成一个有向图，它的顶点表示处理机，它的边(u,v)表示处理机 u 对处理机 v 进行测试。用 $\sigma(u,v)=0$[1] 表示处理机 v 通过了（未通过）处理机 u 的测试。把全体测试结果称为症候，记为 σ.

在系统级故障诊断中，必须假定测试能够为诊断提供足够的信息，这些假定被称为测试模型。

本文假定测试是这样进行的：处理机 u 在执行某个系统任务的同时，把它分配给它测试的处理机 v 去执行，如果 v 执行该任务得到的结果与 u 的结果相同，v 就通过了 u 的测试，这个测试过程很容易实现[10]。

基于上述假定，可把处理机分成三类，进而提出如下新的三值测试模型：

1）"0" 类无故障处理机　无故障处理机总能通过它的测试，而故障处理机总不能通过它的测试；

2）"1/2" 类无故障处理机　无故障处理机总能通过它的测试，而故障处理机不一定能通过它的测试；

3）故障处理机　其它处理机不一定能通过它的测试。

这种模型称为三值 PMC 模型，见表 1。

表 1　二值 PMC 模型

处理机 u	处理机 v	$s(u,v)$
"0"无故障	无故障	0
"0"无故障	有故障	1
"1/2"无故障	无故障	0
"1/2"无故障	有故障	0.1
有故障	无故障	0.1
有故障	有故障	0.1

表 2　二值 PMC 模型

处理机 u	处理机 v	$s(u,v)$
无故障	无故障	0
无故障	无故障	1
有故障	无故障	0.1
有故障	有故障	0.1

把三值 PMC 模型和二值 PMC 模型[1]（表 2）作一个比较，二值 PMC 模型假定故障处理机不可能通过无故障处理机的测试。三值 PMC 模型假定某些系统任务能够覆盖目前发生的故障，而另一些系统任务不一定能覆盖目前发生的故障，因此，三值 PMC 模型更符合实际情况。

现在，引入下列新的定义：

定义 1　如果 U_0 是系统中全体"0"无故障处理机的集合，$U_{1/2}$ 是全体"1/2"无故障处理机的集合，U_1 是全体故障处理机的集合，则称$(U_0,U_{1/2},U_1)$是该系统的一个故障模式。

定义 2　如果两个故障模式$(U_0,U_{1/2},U_1)$和$(V_0,V_{1/2},V_1)$满足 $U_1\neq V_1$，则称这两个故障模式是相异的。

定义 3　如果故障模式$(U_0,U_{1/2},U_1)$满足 $|U_1|\leqslant t_1$ 和 $|U_{1/2}|\leqslant t_{1/2}$，则称之为$(t_1,t_{1/2})$-故障模式。

定义 4　一个系统被称为$(t_1,t_{1/2})$-可诊断的，如果该系统中任何两个相异的$(t_1,t_{1/2})$-故

障模式都不可能产生相同的症候。

由上述定义可知：如果故障处理机数不超过 t_1，并且“1/2”无故障处理机数不超过 $t_{1/2}$，那么 $(t_1, t_{1/2})$- 可诊断系统中的全体故障处理机总能被正确定位。

为了把 $(t_1, t_{1/2})$- 可诊断系统与二值 PMC 模型下的可诊断系统作一个比较，下面介绍一个 t- 可诊断系统的概念[1]。

在二值 PMC 模型下，如果 U_0 是一个系统中全体无故障处理机的集合，U_1 是全体故障处理机的集合，则称 (U_0, U_1) 是该系统的一个故障模式。如果两个故障模式 (U_0, U_1) 和 (V_0, V_1) 满足 $U_1 \neq V_1$，则称这两个故障模式是相异的。一个系统被称为 t- 可诊断的，如果在故障处理机数不超过 t 的条件下，该系统中任何两个相异的故障模式都不可能产生相同的症候[1]。

由上述定义可知：$(t_1, 0)$- 可诊断系统就是 t_1- 可诊断系统。因此，$(t_1, t_{1/2})$- 可诊断系统是 t- 可诊断系统的推广。

为了方便，我们在系统 $S(U,E)$ 上引入下列符号：

1）对于 U 的两个子集 X 和 Y，令 $X \oplus Y = (X - Y) \cup (Y - X)$；

2）对于 U 的两个子集 X 和 Y，令

$$\Gamma^{-1}(X,Y) = \{v \in X\text{：系统 } S \text{ 中有从处理机 } v \text{ 到 } Y \text{ 中某个处理机的测试}\}$$

3）对于 U 的一个处理机 u，令

$$\Gamma^{-1}(u) = \{v \in U\text{：系统 } S \text{ 中有从处理机 } v \text{ 到处理机 } u \text{ 的测试}\}$$

由上述定义可知： $\Gamma^{-1}(u) = \Gamma^{-1}(U, \{u\})$.

2 $(t_1, t_{1/2})$- 可诊断系统的特征

设计可诊断系统是有效诊断的前提。为此，有必要研究可诊断系统应该满足的充分必要条件，这种条件被称为可诊断系统的特征。在此首先给出了 $(t_1, t_{1/2})$- 可诊断系统的一个特征，然后给出了 $(t_1, t_{1/2})$- 可诊断系统的一个充分条件和一个必要条件。

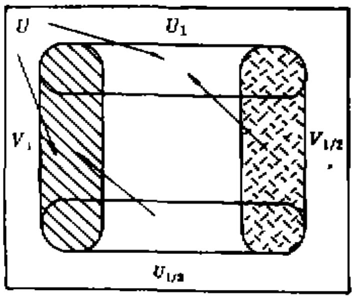

图 1 $(t_1, t_{1/2})$- 可诊断系统的特征

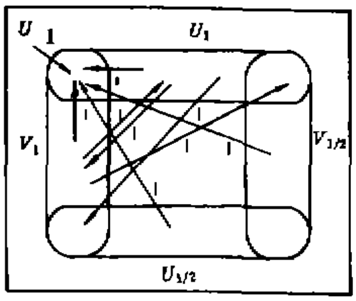

图 2 一个症候

图中未画出的测试结果均为 0

定理 1　系统 $S(U,E)$ 是 $(t_1,t_{1/2})$- 可诊断的 $\Leftrightarrow$ 对于 S 中任何两个相异的 $(t_1,t_{1/2})$- 故障模式 $(U_0,U_{1/2},U_1)$ 和 $(V_0,V_{1/2},V_1)$，下面三个条件至少有一个成立：

1) $\Gamma^{-1}(U-U_1-V_1-U_{1/2}-V_{1/2},U_1\oplus V_1)\neq\varnothing$；

2) $\Gamma^{-1}(V_{1/2}-U_1-U_{1/2},U_1-V_1)\neq\varnothing$；

3) $\Gamma^{-1}(U_{1/2}-V_1-V_{1/2},V_1-U_1)\neq\varnothing$（见图 1）。

证明　“$\Rightarrow$”用反证法：

假设存在 $(t_1,t_{1/2})$- 可诊断系统 $S(U,E)$，它有两个相异的 $(t_1,t_{1/2})$- 故障模式 $(U_0,U_{1/2},U_1)$ 和 $(V_0,V_{1/2},V_1)$ 使得上面三个条件都不成立。构造症候 σ 如下。

对于 S 中下列五类测试 (u,v)，令 $\sigma(u,v)=1$

(a) $u\in U-U_1-V_1-U_{1/2}-V_{1/2},v\in U_1\cap V_1$；

(b) $u\in U_{1/2}-V_{1/2}-V_1,v\in U_1\cap V_1$；

(c) $u\in V_{1/2}-U_{1/2}-U_1,v\in U_1\cap V_1$；

(d) $u\in U_1-V_1-V_{1/2},v\in V_1$；

(e) $u\in V_1-U_1-U_{1/2},v\in U_1$.

对于 S 中其余测试 (u,v)，令 $\sigma(u,v)=0$（见图 2）。则这两个相异的 $(t_1,t_{1/2})$- 故障模式都有可能产生症候 σ，这与“S 是 $(t_1,t_{1/2})$- 可诊断系统”的假定矛盾，必要性得证。

“$\Leftarrow$”设在系统 $S(U,E)$ 中，对于任何两个相异的 $(t_1,t_{1/2})$- 故障模式 $(U_0,U_{1/2},U_1)$ 和 $(V_0,V_{1/2},V_1)$，命题中的三个条件至少有一个成立。

如果条件 1) 成立，不妨设测试 (u,v) 满足 $u\in U-U_1-V_1-U_{1/2}-V_{1/2}$ 和 $v\in U_1-V_1$，则当第一个故障模式发生时，$\sigma(u,v)=1$；而当第二个故障模式发生时，$\sigma(u,v)=0$.

如果条件 2) 成立，设测试 (u,v) 满足 $u\in V_{1/2}-U_1-U_{1/2}$ 和 $v\in U_1-V_1$，则当第一个故障模式发生时，$\sigma(u,v)=1$；而当第二个故障模式发生时，$\sigma(u,v)=0$.

如果条件 3) 成立，设测试 (u,v) 满足 $u\in U_{1/2}-V_1-V_{1/2}$ 和 $v\in V_1-U_1$，则当第一个故障模式发生时，$\sigma(u,v)=0$；而当第二个故障模式发生时，$\sigma(u,v)=1$.

因此，任何两个相异的 $(t_1,t_{1/2})$- 故障模式不可能产生的症候，即系统 S 是 $(t_1,t_{1/2})$- 可诊断的，充分性得证。　　证毕

定理 2　对于 $(t_1,t_{1/2})$- 可诊断系统中每个处理机 u，$|\Gamma^{-1}(u)|\geqslant t_1+t_{1/2}$

证明　用反证法：

假设有一个 $(t_1,t_{1/2})$- 可诊断系统 $S(U,E)$ 中存在处理机 u 使 $|\Gamma^{-1}(u)|<t_1+t_{1/2}$，则可以把 $\Gamma^{-1}(u)$ 分成两部分 T_1 和 T_2，使 $|T_1|<t_1$，$|T_2|\leqslant t_{1/2}$。现在构造两个相异的 $(t_1,t_{1/2})$- 故障模式 $(U_0,U_{1/2},U_1)$ 和 $(V_0,V_{1/2},V_1)$ 如下：

$$U_1=T_1,\quad V_1=T_1\cup\{u\},\quad U_{1/2}=V_{1/2}=T_2$$

$\because$　$U_1\oplus V_1=\{u\}$，且 $(U-U_1-V_1-U_{1/2}-V_{1/2})\cap\Gamma^{-1}(u)=\varnothing$

$\therefore$　$\Gamma^{-1}(U-U_1-V_1-U_{1/2}-V_{1/2},U_1\oplus V_1)\neq\varnothing$；

$\because$　$V_{1/2}-U_1-U_{1/2}=\varnothing$. $\therefore$　$\Gamma^{-1}(V_{1/2}-U_1-U_{1/2},U_1-V_1)\neq\varnothing$；

$\because$　$U_{1/2}-V_1-V_{1/2}=\varnothing$. $\therefore$　$\Gamma^{-1}(U_{1/2}-V_1-V_{1/2},V_1-U_1)\neq\varnothing$.

根据定理 1 可知：系统 S 不是 $(t_1,t_{1/2})$- 可诊断的，矛盾。命题得证。 证毕

定理 3 如果系统 $S(U,E)$ 中每个处理机 u 都满足 $|\Gamma^{-1}(u)|\geqslant 2t_1+t_{1/2}$，那么该系统是 $(t_1,t_{1/2})$- 可诊断的。

证明 任取 S 中两个相异的 $(t_1,t_{1/2})$- 故障模式 $(U_0,U_{1/2},U_1)$ 和 $(V_0,V_{1/2},V_1)$，不妨设 $v\in U_1-V_1$。因为

$$|U_1\cup V_1\cup U_{1/2}-\{v\}|\leqslant|U_1-\{v\}|+|V_1|+|U_{1/2}|<2t_1+t_{1/2}$$

以及 $|\Gamma^{-1}(u)|\geqslant 2t_1+t_{1/2}$，所以在 $\Gamma^{-1}(v)$ 中有一个顶点属于 $(U-U_1-V_1-U_{1/2}-V_{1/2})\cup(V_{1/2}-U_1-U_{1/2})$. 现在分为两种情形：

情形 1 $\Gamma^{-1}(v)$ 中有一个顶点属于 $(U-U_1-V_1-U_{1/2}-V_{1/2})$，则 $\Gamma^{-1}(U-U_1-V_1-U_{1/2}-V_{1/2},U_1\oplus V_1)\neq\varnothing$.

情形 2 $\Gamma^{-1}(v)$ 中有一个顶点属于 $(V_{1/2}-U_1-U_{1/2})$，则 $\Gamma^{-1}(V_{1/2}-U_1-U_{1/2},U_1-V_1)\neq\varnothing$.

根据定理 1，系统 S 是 $(t_1,t_{1/2})$- 可诊断的。 证毕

3 $(t_1,t_{1/2})$- 可诊断系统的最优设计

系统级故障诊断的中心任务，是要用最小的开销完成诊断任务，测试数是诊断开销的一个组成部分，设计测试数最小的可诊断系统(最优的可诊断系统)是系统级故障诊断的一个重要问题，该问题被称为最优设计问题。本节研究 $(t_1,t_{1/2})$- 可诊断系统的最优设计问题。

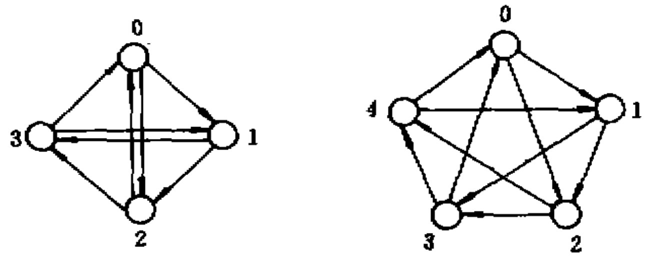

图 3 两个 $D_{1,2}$

(a) 四个顶点的 $D_{1,2}$; (b) 五个顶点的 $D_{1,2}$

首先，描述一类 n- 处理机系统 $D_{\delta,t}$，其处理机被标记为 $0,1,\cdots,n-1$，(p,q) 是 $D_{\delta,t}$ 中的测试 $\Leftrightarrow q-p=\delta m(\mathrm{mod}\ n)$，其中，$m=1,\cdots,t$. 图 3 中给出了两个 $D_{1,2}$.

Preparata 等人[1]在二值 PMC 模型下证明：$D_{\delta,t}$ 是最优的 $(t_1,t_{1/2})$- 可诊断系统。现在，我们在三值 PMC 模型下证明：在一定条件下，$D_{1,t_1+t_{1/2}}$ 是最优 $(t_1,t_{1/2})$- 可诊断的。

用 $T(n,t_1,t_{1/2})$ 表示有 n 个处理机的最优 $(t_1,t_{1/2})$- 可诊断系统的测试数，根据定理 2 和定理 3，可得下面的结论：

定理 4 $n(t_1,t_{1/2})\leqslant T(n,t_1,t_{1/2})\leqslant n(2t_1+t_{1/2})$.

引理 1 当 $n>2(t_1+t_{1/2})$ 时，$D_{1,t_1+t_{1/2}}$ 是 $(t_1,t_{1/2})$- 可诊断的。

证明 任取 $D_{1,t_1+t_{1/2}}$ 中两个相异的 $(t_1,t_{1/2})$- 故障模式 $(U_0,U_{1/2},U_1)$ 和 $(V_0,V_{1/2},V_1)$ 不妨设

(Ⅰ) $i\in U_1\oplus V_1$,

(Ⅱ) $i,i-1,\cdots,i-r\in U_1\cup V_1\cup U_{1/2}\cup V_{1/2}$，和

(Ⅱ) $i-r-1\in U-U_1-V_1-U_{1/2}-V_{1/2}$.

因为

$$r+1\leqslant|U_1\cup V_1\cup U_{1/2}\cup V_{1/2}|\leqslant|U_1|+|V_1|+|U_{1/2}|+|V_{1/2}|\leqslant 2(t_1+t_{1/2})$$

以及　$n>(2(t_1+t_{1/2})$，

所以 $r+2\leqslant n$，即 $i,i-1,\cdots,i-r,i-r-1$ 这 $r+2$ 个顶点是两两不同的。

现在令 $j=\max\{k:0\leqslant k\leqslant r,i-k\in U_1\oplus V_1\}$，不妨设 $i-j\in U_1-V_1$.

现在考察 $i-j-1,i-j-2,\cdots,i-j-t_1-t_{1/2}$ 这 $t_1+t_{1/2}$ 个顶点.如果这些顶点都属于 $(U_1\cap V_1)\cup(U_{1/2}-V_1)$，则

$$t_1+t_{1/2}\leqslant|(U_1\cap V_1)\cup(U_{1/2}-V_1)|\leqslant|U_1\cap V_1|+|U_{1/2}|<t_1+t_{1/2}$$

这是不可能的。所以可设 $i-j-m\in(U-U_1-V_1-U_{1/2}-V_{1/2})\cup(V_{1/2}-U_1-U_{1/2})$. 其中，$1\leqslant m\leqslant t_1+t_{1/2}$. 现在分为两种情形：

情形 1　$i-j-m\in(U-U_1-V_1-U_{1/2}-V_{1/2})$. 因为 $i-j\in U_1\oplus V_1$，并且根据 $D_{1,t_1+t_{1/2}}$ 的定义，$(i-j-m,i-j)$ 是 $D_{1,t_1+t_{1/2}}$ 的边，所以

$$\Gamma^{-1}(U-U_1-V_1-U_{1/2}-V_{1/2},U_1\oplus V_1)\neq\varnothing$$

情形 2　$i-j-m\in(V_{1/2}-U_1-U_{1/2})$，因为 $i-j\in U_1-V_1$，并且根据 $D_{1,t_1+t_{1/2}}$ 的定义，$(i-j-m,i-j)$ 是 $D_{1,t_1+t_{1/2}}$ 的边，所以

$$\Gamma^{-1}(V_{1/2}-U_1-U_{1/2},U_1-V_1)\neq\varnothing$$

根据定理 1 可知：系统 $D_{1,t_1+t_{1/2}}$ 是 $(t_1,t_{1/2})$- 可诊断的。　　证毕

根据定理 4 和引理 1，可得

定理 5　当 $n>2(t_1+t_{1/2})$ 时，$D_{1,t_1+t_{1/2}}$ 是最优的 $(t_1,t_{1/2})$- 可诊断系统。

例如，根据定理 5 可知：图 3(b) 中那个系统是最优(1,1)- 可诊断的。

根据定理 4 和定理 5，立即得到下面的结论：

推论 1　当 $n>2(t_1+t_{1/2})$ 时，$T(n,t_1,t_{1/2})=n(t_1+t_{1/2})$.

当 $n\leqslant 2(t_1+t_{1/2})$ 时，定理 5 中的结论不一定成立。事实上，我们有下面的结论：

定理 6　当 $n=2(t_1+t_{1/2})$ 时，$D_{1,t_1+t_{1/2}}$ 不是 $(t_1,t_{1/2})$- 可诊断的。

证明　构造 $D_{1,t_1+t_{1/2}}$ 中两个相异的 $(t_1,t_{1/2})$- 故障模式 $(U_0,U_{1/2},U_1)$ 和 $(V_0,V_{1/2},V_1)$ 如下：

$$\begin{aligned}U_1&=\{i:0\leqslant i\leqslant t_1-1\}\\U_{1/2}&=\{i:t_1\leqslant i\leqslant t_1+t_{1/2}-1\}\\V_1&=\{i:t_1+t_{1/2}\leqslant i\leqslant 2t_1+t_{1/2}-1\}\\V_{1/2}&=\{i:2t_1+t_{1/2}\leqslant i\leqslant 2t_1+t_{1/2}-1\}\end{aligned}$$

因为 $U-U_1-V_1-U_{1/2}-V_{1/2}=\varnothing$，所以

$$\Gamma^{-1}(U-U_1-V_1-U_{1/2}-V_{1/2},U_1\oplus V_1)\neq\varnothing$$

因为对于 $V_{1/2}$ 中每个顶点 p 和 U_1 中每个顶点 q，总有

$$q - p(\mathrm{mod}\ n) > t_1 + t_{1/2}$$

根据 $D_{1,t_1+t_{1/2}}$ 的定义，可得

$$\Gamma^{-1}(V_{1/2} - U_1 - U_{1/2}, U_1 - V_1) = \Gamma^{-1}(V_{1/2}, U_1) = \varnothing$$

因为对于 $U_{1/2}$ 中每个顶点 p 和 V_1 中每个顶点 q，总有

$$q - p(\mathrm{mod}\ n) > t_1 + t_{1/2}$$

根据 $D_{1,t_1+t_{1/2}}$ 的定义，可得

$$\Gamma^{-1}(U_{1/2} - V_1 - V_{1/2}, V_1 - U_1) = \Gamma^{-1}(U_{1/2}, V_1) = \varnothing$$

根据定理 1 可知：当 $n = 2(t_1 + t_{1/2})$ 时，$D_{1,t_1+t_{1/2}}$ 不是$(t_1, t_{1/2})$- 可诊断的 。 证毕

例如，根据定理 6 可知：图 3(a) 中那个系统不是(1,1)- 可诊断的。

当 $n \leqslant 2(t_1 + t_{1/2})$ 时，$(t_1, t_{1/2})$- 可诊断系统的最优设计问题是一个有待解决的问题。

4 结束语

本文提出了系统级故障诊断的一种三值 PMC 模型，它是经典的二值 PMC 模型的合理推广。笔者定义了一类新的可诊断系统，给出了它们的特征，并且系统地研究了它们的最优设计问题。围绕这个模型，下一步要做的工作包括：

1) 研究可诊断性问题(用多项式算法判定一个系统是否是可诊断系统)；

2) 研究诊断问题(用多项式算法识别可诊断系统中的故障处理机)。

参 考 文 献

1 Preparata F P, Metze G, Chien R T. On the connection assignment problem of diagnosable systems. IEEE Trans Electron Comput, 19676(12):848～854

2 Chen Tinghuai. Fault Diagnosis and Fault Tolerance: A systematic Approach to Special Topics. Berlin Heidelberg: Springer-Verlag, 1992. 68～80

3 杨晓帆. 容错和诊断-神经网络和多处理机系统中若干问题的研究:[博士学位论文]. 重庆:重庆大学计算机系, 1994

4 罗铸楷，胡谋，陈廷槐. 多值逻辑的理论及应用. 北京:科学出版社, 1992. 208～218

5 Butler J T. Relations among system diagnosis model with three-valued test outcomes. In: Proc 13th Int Symp Multi-Valued Logic. New York: IEEE Computer Society Press, 1983. 350～355

6 Sengupta A, Sen A. On system diagnosis with multiple-valued test outcomes. In: Proc 13th Int Symp Multi-Valued Logic. New York: IEEE Computer Society Press, 1983. 356～360

7 Sengupta A, Sen A. On the diagnosablitity of general model of system with three-valued test outcomes. IEEE Trans Comput, 1986, (2): 170～173

8 Kozlowski W E, Krawczyk H. A comparison-based approach to multicomputer system diagnosis in hybrid fault situations. IEEE Trans Comput, 1991, (11): 1 283～1 287

9 Huang Kaiyuan, Chen Tinghuai. Three-valued system diagnosis. In: Proc 15th Int Symp Multi-Valued Logic. New York: IEEE Computer Society Press, 1985. 336～340

10 Chwa K Y, Hakimi L. Scheme for fault tolerant computing comparison of modularly redundant and t-diagnosable system. Inform Contr, 1981, 49(2): 212～238