9th IEEE Int. Symp. on Fault Tolerant Computing, pp.157-160, June 1979.

ON THE DIAGNOSABILITY OF SYSTEMS WITH SELF-TESTING UNITS

Hideo FUJIWARA and Hiroshi OZAKI

Department of Electronic Engineering
Osaka University
Yamada-Kami, Suita-Shi
Osaka, 565 JAPAN

Abstract

The diagnostic model introduced by Preparata et al. assumes that 1) each unit has the capability of testing any other unit; and 2) no unit tests itself. In this paper we eliminate these assumptions and consider a new diagnostic model in which there exist some units without capability of testing other units and some units with capability of testing themselves. For this model we consider the following three problems: 1) Necessary and sufficient conditions for the existence of testing links to form t-diagnosable systems. 2) Methods for optimal assignment of testing links to achieve a given diagnosability. 3) Necessary and sufficient conditions for a given system to be t-diagnosable.

I. Introduction

While the investigation of self-diagnosable computer architectures has been proceeded [1]-[3], many studies have been concerned with the analysis and synthesis problems of self-diagnosable systems in graph-theoretic models [4]-[11]. The graph-theoretic model was first formulated by Preparata et al. [4], and it assumes that 1) each unit has the capability of testing any other unit; and 2) no unit tests itself.

However, in the real computer systems these assumptions may not always hold. Hence in order to have a more realistic assumption, we eliminate the above assumptions and consider a new diagnostic model in which there exist some units without capability of testing other units and some units with capability of testing themselves. If a test outcome of a faulty unit is unreliable, then self-testing may or may not yield any information. Hence, we assume that the outcome of self-testing is always reliable; that is if the test outcome of a self-testing unit u is good, then we can conclude that u is fault-free. For this model we consider the following three problems: 1) Necessary and sufficient conditions for the existence of testing links to form t-diagnosable systems. 2) Methods for optimal assignment of testing links to achieve a given diagnosability. 3) Necessary and sufficient conditions for a given system to be t-diagnosable.

II. Diagnostic Model

A system is supposed to be partitioned into n subsystems, or <u>units</u>, not necessarily identical. Some units have the capability of testing other units of the system by applying stimuli and observing the ensuing responses. Some units have the capability of testing themselves. Some units do not have the capability of testing. Let $V=\{u_1,u_2,\ldots,u_n\}$ be the set of all units. Let $V_1 \subseteq V$ be the set of units without capability of testing. Let $V_2 \subseteq V$ be the set of units that are capable of testing themselves and other units. Each unit in $V-V_1-V_2$ is capable of testing other units but not itself. The relation of testability can be represented by a function Γ mapping V into 2^V such that $u_j \in \Gamma(u_i)$ if and only if u_i tests u_j. Hence, a system S will be represented by a quadruple $S=(V,V_1,V_2,\Gamma)$. When Γ is undefined, it is denoted by the dash, that is, $S=(V,V_1,V_2,-)$. Clearly, this diagnostic model can be also represented by a directed graph $G=(V,\Gamma)$, called a diagnostic graph, where the arc (u_i,u_j) is an ordered pair of vertices in V such that $u_j \in \Gamma(u_i)$. For $X \subseteq V$, we define the following functions: $\Gamma(X)=\bigcup_{u\in X}\Gamma(u)$, $\Delta(X)=\Gamma(X)-X$, $\Gamma^{-1}(X)=\{u \mid \Gamma(u)\cap X \neq \phi\}$, $\Delta^{-1}(X)=\Gamma^{-1}(X)-X$.

Each unit in V_1 cannot test itself and other units, and each unit not in V_2 cannot test itself. Therefore, the function Γ must satisfy the following connection condition.

<u>Connection Condition</u>

1) For $u \in V_1$, $\Gamma(u)=\phi$ (the empty set).
2) For $u \in V-V_2$, $u \notin \Gamma(u)$.

The testing unit u_i evaluates the tested unit u_j as either fault-free or faulty. The test outcome is indicated by the weight $\sigma(u_i,u_j)$ on the arc (u_i,u_j) of G and obeys the following rule:

For $u_i \neq u_j$,

- $\sigma(u_i,u_j)=0$ if u_i and u_j are fault-free,
- $\sigma(u_i,u_j)=1$ if u_i is fault-free and u_j is faulty,
- $\sigma(u_i,u_j)=0,1$ if u_i is faulty and u_j is fault-free,
- $\sigma(u_i,u_j)=0,1$ if u_i and u_j are faulty.

For $u_i=u_j$,

- $\sigma(u_i,u_i)=0$ if u_i is fault-free
- $\sigma(u_i,u_i)=1$ if u_i is faulty.

Reprinted from FAULT-TOLERANT COMPUTING 1979

This weight function σ is termed syndrome of the system. Given a directed graph $G=(V,\Gamma)$ of a system S and a syndrome σ of S, the fundamental problem is to identify the faulty units. A consistent fault set F with respect to σ must satisfy the following conditions:

1) $\sigma(u_i,u_j)=1$ for all u_i,u_j such that $u_j\in\Gamma(u_i)$, $u_i\in \overline{F}=V-F$ and $u_j\in F$.
2) $\sigma(u_i,u_j)=0$ for all u_i,u_j such that $u_j\in\Gamma(u_i)$ and $u_i,u_j\in \overline{F}$.
3) $\sigma(u_i,u_i)=1$ for all u_i such that $u_i\in\Gamma(u_i)$ and $u_i\in F$.

A system $S=(V,V_1,V_2,\Gamma)$ is said to be one-step t-fault diagnosable (shortly, t-diagnosable) if for any syndrome σ, and at most one consistent fault set F with respect to σ such that $|F| \leq t$, where $|X|$ denotes the cardinality of a set X, all faults in F can be located (identified).

III. Existence Condition for Diagnosable Systems

In this section, we consider the following problem: Given a system $S=(V,V_1,V_2,-)$; find necessary and sufficient condition for the existence of a function Γ to form a t-diagnosable system. Note that the function Γ must satisfy the connection condition as mentioned above.

Theorem 1: Given a system $S=(V,V_1,V_2,-)$,
1) in case of $|V_2| \geq t$, there always exists a function Γ such that $\hat{S}=(V,V_1,V_2,\Gamma)$ is t-diagnosable, and
2) in case of $|V_2| < t$, there exists a function Γ such that $\hat{S}=(V,V_1,V_2,\Gamma)$ is t-diagnosable if and only if $|V| + |V_2| - |V_1| \geq 2t + 1$.

Proof: The proof in case of $|V_2|\geq t$ is obvious. In case of $|V_2|<t$, the sufficiency can be proved as follows. Let Γ be a function such that $\Gamma^{-1}(u)=\{u\}$ for $u \in V_2$ and $\Gamma^{-1}(u)=V-V_1-\{u\}$ for $u\in\overline{V}_2$. Clearly, Γ satisfies the connection condition.

If there exists at least one fault-free unit in V_2, we can uniquely find a consistent fault set. If all the units in V_2 are faulty, then we can see that there exist at most $t-|V_2|$ faulty units in $V-V_1-V_2$. Since $|V|-|V_1|-|V_2| > 2(t-|V_2|)+1$, the subsystem consisting of $V-V_1-V_2$ is $(t-|V_2|)$-diagnosable [4]. Therefore all the faulty units in $V-V_1-V_2$ can be identified. On the other hand, $t > |V_2|$ implies $|V|-|V_1| -|V_2| > t$, and thus we can find at least one fault-free unit u_0 in $V-V_1-V_2$. Using this unit u_0, each unit in V_1 can be evaluated as either fault-free or faulty. In this way we can uniquely find a consistent fault set. Hence, the system $\hat{S}=(V,V_1,V_2,\Gamma)$ is t-diagnosable.

Conversely, the necessity can be proved as follows. Consider a maximally connected graph $G=(V,\Gamma)$ satisfying the connection condition, that is,

$\Gamma^{-1}(u)=V-V_1$ for all $u \in V_2$,
$\Gamma^{-1}(u)=V-V_1-\{u\}$ for all $u \in V-V_1-V_2$, and
$\Gamma^{-1}(u)=V-V_1$ for all $u \in V_1$.

We shall prove that if $|V|+|V_2|-|V_1| < 2t+1$, then $\hat{S}=(V,V_1,V_2,\Gamma)$ is not t-diagnosable. Suppose a syndrome σ such that $\sigma(u,u)=1$ for all $u\in V_2$ and $\sigma(u,v)=0$ for all $u\in V_2$, $v\in V_1$. Then it can easily be seen that all units in V_2 are faulty and all units in V_1 are fault-free. This implies that there exist at most $t-|V_2|$ faulty units in $V-V_1-V_2$. Since $|V|+|V_2|-|V_1|<2t+1$, that is, $|V|-|V_1|-|V_2| < 2(t-|V_2|)+1$, the subsystem consisting of $V-V_1-V_2$ is not $(t-|V_2|)$-diagnosable [4]. Hence we cannot identify all the faulty units in $V-V_1-V_2$. This implies that S is not t-diagnosable. This is a contradiction. Q.E.D.

Corollary 1: Given a system $S=(V,V_1,V_2,-)$, then there exists a function Γ such that $S=(V,V_1,V_2,\Gamma)$ is t-diagnosable if and only if

$$t \leq \max \left\{|V_2|, \left\lfloor\frac{|V|+|V_2|-|V_1|-1}{2}\right\rfloor\right\}.$$

When both V_1 and V_2 are empty, we can show that the condition of Theorem 1 and Corollary 1 means $|V| \geq 2t+1$. This coincides with Theorem 1 of Preparata et al. [4], which is a special case of Theorem 1 and Corollary 1.

IV. Optimal Connection Assignments

In the last section, we have shown the necessary and sufficient condition for the existence of a function Γ to form a t-diagnosable system. In this section we consider the design of optimal t-diagnosable systems provided that the above condition holds. The optimal t-diagnosable system is defined as a t-diagnosable system in which the number of arcs is minimum.

In the model of Preparata et al. [4], if a system S is t-diagnosable, then each unit of S is tested by at least t other units. In our model we have the similar results as follows. Let $S=(V,V_1,V_2,\Gamma)$ be a t-diagnosable system. Let $U \subseteq V_2$ be the set of all self-testing units, that is, $U=\{u \mid u \in\Gamma(u)\}$. Then we have the following lemma.

Lemma 1: If S is t-diagnosable, then $|\Gamma^{-1}(u)| \geq t$ for all $u \in V-U$.

From Lemma 1, we can see that the number of arcs of a t-diagnosable system is at least $(|V|-|U|)t+|U|$. Since $U \subseteq V_2$, we have

$$(|V|-|U|)t + |U| \geq (|V|-|V_2|)t + |V_2|.$$

Therefore, we have the following lemma.

Lemma 2: If $S=(V,V_1,V_2,\Gamma)$ is an optimal t-diagnosable system, then the number of arcs of S is at least $(|V|-|V_2|)t + |V_2|$.

When V_2 is empty, Lemma 2 coincides with the result of Preparata et al.[4].

Theorem 2: If $S=(V,V_1,V_2,\Gamma)$ is t-diagnosable, then $S_*=(V,V_1,V_2,\Gamma_*)$ is also t-diagnosable, where Γ_* is defined as follows:

$\Gamma_*^{-1}(u)=\{u\}$ for $u \in V_2$, and

$\Gamma_*^{-1}(u)=\Gamma^{-1}(u)$ for $u \in \overline{V}_2$.

Proof: Assume that S_* is not t-diagnosable. Then, there exist two consistent fault sets F_1 and F_2 with respect to a syndrome σ_* such that $|F_1| \leq t$ and $|F_2| \leq t$.

From σ_*, we define a syndrome σ for the system S as follows:

For $u_j \in \Gamma(u_i)$, $u_i \in V$ and $u_j \in \overline{V}_2$, $\sigma(u_i,u_j)=\sigma_*(u_i,u_j)$.

For $u_j \in \Gamma(u_i)$, $u_i \in V$ and $u_j \in V_2$, $\sigma(u_i,u_j)=\sigma_*(u_j,u_j)$.

Then we can see that both F_1 and F_2 are also consistent fault sets of S with respect to the above syndrome σ. Therefore, S is not t-diagnosable.

Q.E.D.

Now we consider the following problem: Given a system $S=(V,V_1,V_2,-)$, find methods for optimal assignment of testing links Γ so that $S=(V,V_1,V_2,\Gamma)$ is t-diagnosable. On the basis of Theorem 2, we can design a class of optimal t-diagnosable systems using the optimal design $D_{\delta t}$ introduced by Preparata et al. [4] as follows. A system S is said to belong to a design $D_{\delta t}$ when a testing links from u_i to u_j exists if and only if $j-i=\delta m$ (modulo n) and m assumes the values $1,2,\ldots,t$.

Method of design $D^I_{\delta t}$

1) For the set $\overline{V}_1=V-V_1$, construct a graph $G_0=(\overline{V}_1,\Gamma_0)$ such that the system corresponding to the graph G_0 is one of the optimal system $D_{\delta t}$ of Preparata et al.

2) Using the graph G_0, construct a graph $G=(V,\Gamma)$ such that

$\Gamma^{-1}(u)=\{u\}$ for all $u \in V_2$,

$\Gamma^{-1}(u)=\Gamma_0^{-1}(u)$ for all $u \in V-V_1-V_2$, and

$|\Gamma^{-1}(u)|=t$ for all $u \in V_1$.

A system constructed by the above method is said to belong to a design $D^I_{\delta t}$. From Theorem 2, it can easily be seen that a system $S=(V,V_1,V_2,\Gamma)$ belonging to design $D^I_{\delta t}$ is t-diagnosable. Moreover, the number of arcs of the system S is exactly $(|V|-|V_2|)t + |V_2|$. Therefore from Lemma 2 we can see that the system S is optimal.

Next we shall show another optimal design of t-diagnosable systems.

Method of design $D^{II}_{\delta t}$

(Case of $|V_2| \geq t$)

Construct a graph $G=(V,\Gamma)$ such that

$\Gamma^{-1}(u)=\{u\}$ for all $u \in V_2$, and

$\Gamma^{-1}(u) \subseteq V_2$ and $|\Gamma^{-1}(u)|=t$ for all $u \in V-V_2$.

(Case of $|V_2| < t$)

1) For $V-V_1-V_2$, construct a graph $G_0=(V-V_1-V_2,\Gamma_0)$ such that the system corresponding to the graph G_0 is one of the optimal systems $D_{\delta t'}$, where $t'=t-|V_2|$.

2) Using the graph G_0 construct a graph $G=(V,\Gamma)$ such that

$\Gamma^{-1}(u)=\{u\}$ for all $u \in V_2$,

$\Gamma^{-1}(u)=V_2 \cup \Gamma_0^{-1}(u)$ for all $u \in V-V_1-V_2$, and

$|\Gamma^{-1}(u)|=t$ for all $u \in V_1$.

A system constructed by the above method is said to belong to a design $D^{II}_{\delta t}$. It can be proved similarly as the proof of Theorem 1 that a system S belonging to the design $D^{II}_{\delta t}$ is t-diagnosable. Moreover the number of arcs of the system S is exactly $(|V|-|V_2|)t + |V_2|$. Therefore from Lemma 2 we can see that the system S is optimal. When both V_1 and V_2 are empty, the designs $D^I_{\delta t}$ and $D^{II}_{\delta t}$ coincide with the design $D_{\delta t}$ of Preparata et al. [4].

Example: To illustrate the designs of $D^I_{\delta t}$ and $D^{II}_{\delta t}$, we consider a system $S=(V,V_1,V_2,-)$ where $V=\{u_1,u_2,\ldots,u_6\}$, $V_1=\{u_6\}$, and $V_2=\{u_1\}$. Suppose that t=2, then we have a system which belongs to D^I_{12} as shown in Fig. 1. A system belonging to D^{II}_{12} is shown in Fig. 2.

V. Diagnosability of Systems

So far we have discussed optimal connection assignment problem for t-diagnosable systems. In this section we present the necessary and sufficient condition for a system with a diagnostic graph to be t-diagnosable. For the model of Preparata et al. [4], the necessary and sufficient condition for t-diagnosability was already shown by Allan et al. [6]. In this section we extend their results to our new model.

Given a system $S=(V,V_1,V_2,\Gamma)$ and its graph $G=(V,\Gamma)$, let $U \subseteq V_2$ be the set of all self-testing units, that is, $U=\{u \mid u \in \Gamma(u)\}$. Let P(G) be the set of all partitions of V with three disjoint blocks (X,Y,Z) such that

$|Z| \geq 1$,

$\Delta(X) \subseteq Y$ (i.e., $\Gamma(X) \subseteq X \cup Y$), and

$U \subseteq X \cup Y$.

Let k be a function from P(G) to the set of all positive integers such that for any $p \in P(G)$

$$k(p) = |Y| + \left\lceil \frac{|Z|}{2} \right\rceil .$$

For a graph $G=(V,\Gamma)$, we define

$\tau(G)= \min\{ k(p) \mid p \in P(G)\} - 1$,

but $\tau(G)=|V|$ when P(G) is empty.

Theorem 3: Given a system $S=(V,V_1,V_2,\Gamma)$ and its graph $G=(V,\Gamma)$, then the system S is t-diagnosable if and only if $k(p) > t$ for all $p \in P(G)$, that is, $t \leq \tau(G)$.

Proof-Necessity: Assume that there exists a partition $p=(X,Y,Z) \in P(G)$ with $k(p) \leq t$. Divide the set Z into two disjoint sets Z_1 and Z_2 such that $|Z_1| \leq \left\lceil \frac{|Z|}{2} \right\rceil$ and $|Z_2| \leq \left\lceil \frac{|Z|}{2} \right\rceil$. Let $F_1=Y \cup Z_1$ and $F_2=Y \cup Z_2$, then we have $|F_1|=|Y|+|Z_1| \leq k(p) \leq t$ and $|F_2|=|Y|+|Z_2| \leq k(p) \leq t$.

For these sets F_1 and F_2, we define a syndrome σ as follows:

$\sigma(u,v)=1$ if $u \in \overline{F_1}$, $v \in F_1$ and $v \in \Gamma(u)$,

$\sigma(u,v)=1$ if $u \in \overline{F_2}$, $v \in F_2$ and $v \in \Gamma(u)$,

$\sigma(u,u)=1$ if $u \in Y \cap U$,

$\sigma(u,u)=0$ if $u \in X \cap U$, and

$\sigma(u,v)=0$ otherwise.

Then we can easily see that both F_1 and F_2 are consistent fault sets with respect to the syndrome σ. Therefore, the system S is not t-diagnosable.

Sufficiency:

Assume that S is not t-diagnosable. Then there exist two consistent fault sets F_1 and F_2 with respect to a syndrome σ such that $F_1 \neq F_2$, $|F_1| \leq t$ and $|F_2| \leq t$. Let $X=V-(F_1 \cup F_2)$, $Y=F_1 \cap F_2$ and $Z=(F_1 \cup F_2)-(F_1 \cap F_2)$. Since $F_1 \neq F_2$, we have $Z \neq \phi$. Since both F_1 and F_2 are consistent fault sets, we have $\Delta(X) \subseteq Y$ and $U \subseteq X \cup Y$. Therefore, $p=(X,Y,Z)$ is in P(G). Moreover, $2|Y|+|Z|=|F_1|+|F_2| \leq 2t$. Hence we have $k(p)=|Y|+\lceil |Z|/2 \rceil \leq t$.

Q.E.D.

When a system is t-diagnosable but not (t+1)-diagnosable, then the number t is called the diagnosability of the system. From Theorem 3, we can see that $\tau(G)$ represents the diagnosability of the diagnostic graph G. When the set U is empty, the set P(G) coincides with the set of partitions introduced by Allan et al. [6]. Therefore, Theorem 3 is a generalization of the result of Allan et al. When V=U, that is, all the units are self-testing units, then P(G) is empty, and thus the condition of Theorem 3 always holds and S is t-diagnosable for any $t \leq |V|$.

For the diagnosability $\tau(G)$ we have the following theorem.

Theorem 4: Given a system $S=(V,V_1,V_2,\Gamma)$ and its graph $G=(V,\Gamma)$, then

$\tau(G) \leq |V_2|$ if $V=V_1 \cup V_2$, and

$\tau(G) \leq \left\lfloor \frac{|V|+|V_2|-|V_1|-1}{2} \right\rfloor$ otherwise.

Proof:

Case 1: $V = V_1 \cup V_2$.

When V_1 is not empty, let $p_0=(V_1-\{v\},V_2,\{v\})$ for some $v \in V_1$. Then it can easily be seen that $p_0 \in P(G)$ and that

$$\min\{ k(p) \mid p \in P(G)\} \leq k(p_0)=|V_2|+\left\lceil\frac{1}{2}\right\rceil=|V_2|+1.$$

Therefore we have $\tau(G) \leq |V_2|$.

When V_1 is empty, then $V=V_2$ and thus we have $\tau(G) \leq |V_2|$.

Case 2: $V \neq V_1 \cup V_2$.

Let $p_0=(V_1,V_2,V-(V_1 \cup V_2))$, then it can easily be seen that p_0 is in P(G). Moreover we have

$$\min\{ k(p) \mid p\ P(G)\} \leq k(p_0)=|V_2|+\left\lceil\frac{|V|-|V_2|-|V_1|}{2}\right\rceil.$$

This implies taht

$$\tau(G) \leq |V_2|+\left\lceil\frac{|V|-|V_2|-|V_1|}{2}\right\rceil-1=\left\lfloor\frac{|V|+|V_2|-|V_1|-1}{2}\right\rfloor.$$

Q.E.D.

Corollary 2: Given a system $S=(V,V_1,V_2,\Gamma)$ and its graph $G=(V,\Gamma)$, then

$$\tau(G) \leq \max\{ |V_2|, \left\lfloor\frac{|V|+|V_2|-|V_1|-1}{2}\right\rfloor\}.$$

Corollary 2 shows the same results as Corollary 1. We have proved the same result in two different ways.

Acknowledgment

The authors wish to thank Prof. K. Kinoshita of Hiroshima University for his numerous suggestions.

References

[1] R.E.Forbs,D.H.Rutherford,C.B.Stieglitz,L.H.Tung, "A self-diagnosable computer,"AFIPS Proc.,1965.

[2] E.Manning,"On computer self-diagnosis,Part I: experimental study of a processor; Part II: generalizations and design principles," IEEE Trans. Elec. Comput.,EC-15, Dec. 1966.

[3] P.Ciompi,L.Simoncini,"Design of self-diagnosable minicomputers using bit sliced microprocessors," J. DA & FTC, vol.1,no.4, Oct. 1977.

[4] F.P.Preparata,G.Metze,R.T.Chien,"On the connection assignment problem of diagnosable systems," IEEE Trans. Elec. Comput.,EC-16, Dec. 1967.

[5] S.L.Hakimi,A.T.Amin,"Characterization of connection assignment of diagnosable systems," IEEE Trans. Comput.,C-23, Jan. 1974.

[6] F.J.Allan, T.Kameda,S.Toida,"An approach to the diagnosability analysis of a system," IEEE Trans. Comput., C-24, Oct. 1975.

[7] J.D.Russell,C.R.Kime,"System fault diagnosis: Closure and diagnosability with repair; Masking exposure and diagnosability without repair," IEEE Trans. Comput.,C-24, Nov., Dec., 1975.

[8] F.Barsi,F.Grandoni,P.Maestrini,"A theory of diagnosability of digital systems," IEEE Trans. Comput., C-25, June 1976.

[9] H.Fujiwara,K.Kinoshita,"Connection assignment for probabilistically diagnosable systems,"IEEE Trans. Comput., C-27, March 1978.

[10] H.Fujiwara,K.Kinoshita,"Some existence theorems for probabilistically diagnosable systems," IEEE Trans. Comput.,C-27,April 1978.

[11] H.Fujiwara,K.Kinoshita,"On the computational complexity of system diagnosis," IEEE Trans. Comput., C-27, Oct. 1978.

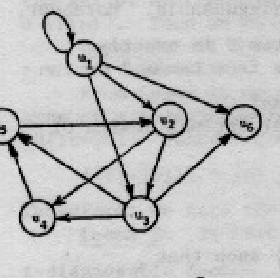

Fig. 1 Design D_{12}^{I}

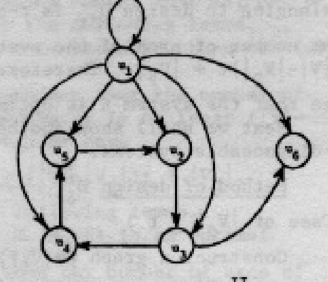

Fig. 2 Design D_{12}^{II}