# On Diagnosabilities of Systems with Incomplete Test

KIYOSHI FURUYA* and YOSHIHIRO TOHMA*

Hakimi and Amin [2] gave necessary and sufficient conditions for identification of all faulty units in a system on the assumption that the tests are complete. We extend those theories to the case where even fault-free units may fail tests of faulty ones.

We define a system to be $(t, r)$-diagnosable if all faulty units can be identified from test outcomes, provided the number of faulty units and that of test failures do not exceed $t$ and $r$ respectively. Similarly, we define totally-$\tau$-diagnosability, where $\tau$ represents the summation of them.

We first give the necessary and sufficient condition for a system, in which no two units test each other, to be totally-$\tau$-diagnosable. Then, we extend the analysis to general case, and give the condition for a system, on which no such restriction is placed, to be $(t, r)$-diagnosable.

## 1. Introduction

Along with the progress of LSI technologies, computer system configurations with distributed intelligence have become popular. In these systems, an approach for attaining high reliabilities is to adopt system level diagnosis and consequently to make them self-diagnosable.

Previous studies of system level diagnosis based on a directed graph model have assumed complete tests [1], [2], [3]. However, tests may be incomplete in cases and they may or may not detect transient faults. Hence, the extension of the previous theories of the system level diagnosis to cases where the diagnosis can tolerate test failures will increase their feasibility to realistic applications.

The purpose of this paper is to show conditions on the testing graph for a system with incomplete tests to be one-step diagnosable, that is all faulty units can be identified from test outcomes. It is assumed here that fault-free units may fail tests only for faulty ones, but not for fault-free ones (unidirectional test failures).

We define two concepts: $(t, r)$-diagnosability and totally-$\tau$-diagnosability, where $t$ and $r$ represent numbers of faulty units and test failures, respectively, and $\tau$ is the summation of them. Then we give the necessary and sufficient condition for a system, in which no two units test each other, to be totally-$\tau$-diagnosable. We also give the condition for a system, on which no such restrictions are placed, to be $(t, r)$-diagnosable. All of our results are an extension of the theorems given by Hakimi and Amin [2].

## 2. A Model and Definitions

A system under consideration consists of $n$ units with testing capability. The test assignment of the system is represented by a testing graph $G=(V, E)$, where $V$ is the set of vertices and $E\subseteq V\times V$ is the set of directed edges. A vertex and an edge correspond to a unit and a test connection, respectively. An edge $(v_i, v_j)$ belongs to $E$ if and only if $v_i$ tests $v_j$.

Each unit can be in one of two states, fault-free or faulty. Assume that $v_i$ tests $v_j$. Then, the outcome of the test is denoted by $a_{ij}\in\{0, 1\}$, and its value is determined according to the following rules.

1) If both of $v_i$ and $v_j$ are fault-free, $a_{ij}=0$.
2) If $v_i$ is faulty, the test outcome is unreliable, i.e., $a_{ij}=0$ or 1 (arbitrary).
3) If $v_i$ is fault-free and $v_j$ is faulty,
   $a_{ij}=1$ provided the test was successful, and
   $a_{ij}=0$ provided the test failure occurred.

Among some categories of system level diagnosability, our consideration are concerned only with the one-step diagnosabilities. Therefore, the word 'one-step' will be omitted in the sequel.

A system is defined to be $(t, r)$-diagnosable if all faulty units can be identified from a set of test outcomes $\{a_{ij}\}$, provided the number of faulty units and that of test failures (by fault-free units) do not exceed $t$ and $r$, respectively. When $r=0$, i.e., tests are assumed to be complete, the system is simply said as usual to be $t$-diagnosable.

Further, a system is defined to be totally-$\tau$-diagnosable if all faulty units can be identified from a set of test outcomes $\{a_{ij}\}$, provided the summation of faulty units and test failures (by fault-free units) does not exceed $\tau$.

It should be noted that the totally-$\tau$-diagnosability is a stronger condition than the $(t, r)$-diagnosability for some combination of $t$ and $r$ with $t+r=\tau$. However, it will be shown later that for systems, in which no two units test each other, the condition for being $(t, r)$-diagnosable is the same as that for being totally-$\tau$-diagnosable.

*Dept. of Computer Science, Faculty of Engineering, Tokyo Institute of Technology, Tokyo 152.

## 3. Conditions for the Diagnosability

Most notations in this paper follow [2]. The cardinalities of set $X$ is denoted by $|X|$. Given $G=(V, E)$, the number of edges incident to $v\in V$ is denoted by $d_{in}(v)$. Then for $X\subset V$, $v\in V$ with $v\notin X$, define a set of edges as follows:

$$E(X, v)=\{(x, v)\in E|x\in X\}.$$

Similarly, for $X$, $Y\subset V$ with $X\cap Y=\phi$, define $E(X, Y)$ as

$$E(X, Y)=\{(x, y)\in E|x\in X, y\in Y\}.$$

We first show a condition which is necessary for a system to be $(t, r)$-diagnosable. The condition, of course, is also necessary for the system to be totally-$\tau$-diagnosable with $\tau=t+r$.

**Lemma 1:** Let $G=(V, E)$ be the testing graph of a system. In order to make the system $(t, r)$-diagnosable, the following condition is necessary:

$$\text{for any } v\in V,\ d_{in}(v)\ge t+r.$$

**Proof:** To see the necessity of the condition, assume that it does not hold. Then there exists $v_0\in V$ with $d_{in}(v_0)\le t+r-1$, i.e., a unit $v_0$ is tested by at most $t+r-1$ other units. We show that the same set of test outcomes $\{a_{ij}\}$ can be yielded regardless of whether $v_0$ is fault-free or not. Consider a case in which $t-1$ units testing $v_0$ are faulty and the remaining $r$ or less of them are fault-free. If $v_0$ is fault-free, then all the test outcomes for $v_0$ by the fault-free units are 0. On the other hand, the same outcomes can be yielded even if $v_0$ is faulty, provided all of these $r$ or less fault-free units fail in testing $v_0$. Further, the other test outcomes by fault-free units which do not test $v_0$ are, of course, the same independently of the state of $v_0$, and test outcomes by faulty units may be assumed arbitrarily. Thus, the whole set of test outcomes $\{a_{ij}\}$ can be the same independently of the state of $v_0$. Consequently, the identification of the state of $v_0$ is impossible, and the system is not $(t, r)$-diagnosable. Q.E.D.

The condition of Lemma 1 is not sufficient in general cases. However, it can be shown that the condition is sufficient for a system, in which no two units test each other, to be not only $(t, r)$-diagnosable but also totally-$\tau$-diagnosable. Before proceeding to the theorems, we show a lemma which characterizes the diagnosability of systems with incomplete test.

**Lemma 2:** Let $V_f$, $V'_f\subset V$ be two distinct sets of vertices corresponding to two distinct sets of faulty units that yield the same set of test outcomes $\{a_{ij}\}$ with no more than $r$ and $r'$ test failures, respectively. Then, under the notations of

$$V_{f1}=V_f\cap V'_f,\ V_{f2}=V_f\cap\bar{V}'_f,$$
$$V_1=\bar{V}_f\cap V'_f,\ V_2=\bar{V}_f\cap\bar{V}'_f, \tag{1}$$

it holds that

$$|E(V_2, V_{f2})|\le r \text{ and } |E(V_2, V_1)|\le r'. \tag{2}$$

**Proof:** Assuming $|E(V_2, V_{f2})|\ge r+1$, we shall reach a contradiction. First, consider a case in which all units of $V'_f$ are faulty and those of $\bar{V}'_f=V-V'_f$ are fault-free. Since units of $V_2$ and $V_{f2}$ are all fault-free, for any test $(v_i, v_j)\in E(V_2, V_{f2})$ the test outcome $a_{ij}$ is 0. Secondly, consider another case in which all the units of $V_f$ are faulty and those of $\bar{V}_f=V-V_f$ are fault-free. Since the number of test failures in this case does not exceed $r$, there exists at least one test $(v_i, v_j)\in E(V_2, V_{f2})$ of which outcome $a_{ij}$ is 1. This contradicts the hypothesis that $V_f$ and $V'_f$ yield the same set of test outcomes $\{a_{ij}\}$. Thus we conclude $|E(V_2, V_{f2})|\le r$. Another inequality $|E(V_2, V_1)|\le r'$ can be proved similarly. Q.E.D.

**Theorem 1:** Let $G=(V, E)$ be the testing graph of a system in which no two units test each other. The system is totally-$\tau$-diagnosable, if and only if for any $v\in V$, $d_{in}(v)\ge\tau$.

**Proof:** The necessity follows from Lemma 1.

The sufficiency is proved by showing that no two distinct sets of faulty units can yield the same set of test outcomes. Assuming such sets of faulty units, we shall reach a contradiction, under the hypothesis that the total numbers of faulty units and test failures do not exceed $\tau$ and for any $v\in V$, $d_{in}(v)\ge\tau$.

Let $V_f$, $V'_f\subseteq V$, with $|V_f|=t\le\tau$, $|V'_f|=t'\le\tau$, be two distinct sets of vertices. Assume that a set of test outcomes $\{a_{i,j}\}$ is consistent even if either set of units corresponding to $V_f$ or $V'_f$ is faulty, provided the number of test failures associated with $V_f$ and $V'_f$ do not exceed $r=\tau-t$ and $r'=\tau-t'$, respectively. Let $V_1$, $V_2$, $V_{f1}$, and $V_{f2}$ be the subsets of $V$ as defined in Eq. (1). Denote $|V_i|$ and $|\{(v_1, v_2)\in E|v_1, v_2\in V_i\}|$ by $n_i$ and $e_i$, respectively, for $i=1, 2, f1, f2$.

We first show that there is no covering relationship between $V_f$ and $V'_f$. Assume, without loss of generality, that $V_f\supset V'_f$. Then, the set of vertices $V$ is divided into two subsets $V_f$ and $V_2$. Consider a vertex $v\in V_{f2}=V_f\cap\bar{V}'_f$. Since $|V_f|=t$, $v$ is tested by at most $t-1$ other units of $V_f$. According to Lemma 2, the vertex $v$ is also tested by at most $r$ units of $V_2$. Hence,

$$d_{in}(v)=|E(V_f-\{v\}, v)|+|E(V_2, v)|\le(t-1)+r=\tau-1.$$

This contradicts the hypothesis. Thus, no covering relationship is concluded. Hence, we have

$$n_{f2}\ge 1 \quad\text{and}\quad n_1\ge 1 \tag{3}$$

Now, the enumeration of the numbers of edges incident to vertices in $V_1$ and $V_{f2}$, respectively, gives

$$\begin{aligned} n_1\tau &\le \sum_{v\in V_1} d_{in}(v) \\ &\le e_1+|E(V_{f2}, V_1)|+n_{f1}n_1+|E(V_2, V_1)|, \end{aligned} \tag{4}$$

$$\begin{aligned} n_{f2}\tau &\le \sum_{v\in V_{f2}} d_{in}(v) \\ &\le e_{f2}+|E(V_1, V_{f2})|+n_{f1}n_{f2}+|E(V_2, V_{f2})|. \end{aligned} \tag{5}$$

Then,

$$\begin{aligned}(n_1+n_{f2})\tau \le e_1+e_{f2}+n_{f1}(n_1+n_{f2})+|E(V_{f2},\ V_1)|\\ +|E(V_1,\ V_{f2})|+|E(V_2,\ V_1)|\\ +|E(V_2,\ V_{f2})|. \qquad (6)\end{aligned}$$

Since no two units test each other, $(v_i,\ v_j)\in E$ implies $(v_j,\ v_i)\notin E$. Therefore, $e_1\le n_1(n_1-1)/2$, $e_{f2}\le n_{f2}(n_{f2}-1)/2$ and $|E(V_{f2},\ V_1)|+|E(V_1,\ V_{f2})|\le n_1n_{f2}$. Further, $|E(V_2,\ V_{f2})|\le r$ and $|\mathrm{E}(V_2,\ V_1)|\le r'$ by Lemma 2. Substituting these inequalities into Eq.(6), we have

$$2\tau\le n_1+2n_{f1}+n_{f2}-1+2(r+r')/(n_1+n_{f2}). \qquad (7)$$

Since $n_1+n_{f2}\ge 2$ by Eq.(3), $2(r+r')/(n_1+n_{f2})\le r+r'$. Then,

$$2\tau\le n_1+2n_{f1}+n_{f2}-1+r+r'.$$

That is,

$$t+t'=(\tau-r)+(\tau-r')\le n_1+2n_{f1}+n_{f2}-1. \qquad (8)$$

On the other hand, since $|V_f|=n_{f1}+n_{f2}=t$ and $|V_f'|=n_1+n_{f1}=t'$,

$$t+t'=n_1+2n_{f1}+n_{f2}. \qquad (9)$$

This is a contradiction. Q.E.D.

**Corollary 1** (Theorem 1 in [2]): A system in which no two units test each other is $t$-diagnosable, if and only if each unit is tested by at least $t$ other units.

An example of a totally-$\tau$-diagnosable system is the $D_{\delta,t}$ design, which is proposed in [1]. The $D_{\delta,t}$ design is optimum in the sense that the minimum number of units and the minimum number of test connections are required.

Now, we present the necessary and sufficient condition for a system to be $(t,\ r)$-diagnosable, even when the system may have pairs of units that test each other.

**Theorem 2:** Let $G=(V,\ E)$ be the testing graph of a system of $n$ units. The system is $(t,\ r)$-diagnosable, if and only if the following three conditions are satisfied:

1) $n\ge 2t+1$;
2) for any $v\in V$, $d_{in}(v)\ge t+r$;
3) for any integer $p$, $0\le p\le t$, and any $X\subset V$ with $|X|=n-2t+p$, there exist no two disjoint subsets of vertices $Z_1$, $Z_2\subset\bar{X}=V-X$ such that $|Z_1|=|Z_2|=t-p$, $|E(X,\ Z_1)|\le r$, and $|E(X,\ Z_2)|\le r$.

**Proof:** The necessity of condition 1) is already known (Theorem 1 in [1]), and that of condition 2) is the direct consequence of Lemma 1. In order to see the necessity of condition 3), assume that it does not hold. Then, for some integer $p$, $0\le p\le t$, and a set $X\subset V$ with $|X|=n-2t+p>0$, there exist two disjoint sets of vertices $Z_1$, $Z_2\subset\bar{X}$ such that $|Z_1|=|Z_2|=t-p$, $|E(X,\ Z_1)|\le r$, and $|E(X,\ Z_2)|\le r$. Let $Y=V-(X\cup Z_1\cup Z_2)$, $V_f=Y\cup Z_1$, and $V_f'=Y\cup Z_2$. Then $|Y|=p$ and $|V_f|=|V_f'|=t$. Therefore, two distinct sets of units, which correspond to $V_f$ and $V_f'$, respectively, can yield the same set of test outcomes with respective sets of test failures on $E(X,\ Z_1)$ and $E(X,\ Z_2)$. Such test outcomes are shown in Fig. 1. Hence, the system is not $(t,\ r)$-diagnosable. This means that condition 3) is necessary for the system to be $(t,\ r)$-diagnosable.

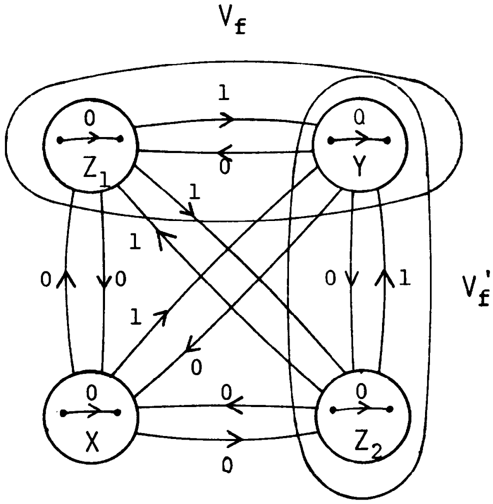

Fig. 1 The set of test outcomes for which $V_f$ and $V_f'$ cannot be distinguished.

In contrast, let us assume a system to satisfy all conditions of the theorem. If the system is not $(t,\ r)$-diagnosable, there exist in $G=(V,\ E)$ such two distinct sets $V_f$, $V_f'\subset V$ with $|V_f|$, $|V_f'|\le t$ that yield the same set of test outcomes $\{a_{ij}\}$ with no more than $r$ test failures. Let $V_1$, $V_2$, $V_{f1}$, and $V_{f2}$ be subsets of $V$ as defined in Eq.(1).

First, we show that $n-t>|V_2|\ge n-2t$. Since $|V_f|=|V_{f1}|+|V_{f2}|\le t$ and $|V_f'|=|V_{f1}|+|V_1|\le t$, $|V_2|=n-|V_1|-|V_{f1}|-|V_{f2}|\ge n-2t+|V_{f1}|\ge n-2t$. To see another inequality $|V_2|<n-t$, assume that it does not hold. Then, $|V_2|\ge n-t$ and $|\bar{V}_2|\le t$, where $\bar{V}_2=V-V_2$. Therefore, for any $v\in\bar{V}_2$,

$$|E(V_2,\ v)|\ge d_{in}(v)-(t-1)\ge r+1$$

According to Lemma 2, however, this contradicts that the two distinct sets of faulty units, corresponding to $V_f$ and $V_f'$, respectively, yield the same set of test outcomes. Hence, we conclude that $|V_2|<n-t$.

Thus there exists an integer $p$, $0\le p<t$, such that $|V_2|=n-2t+p$. Since $|V_2|=n-(|V_f|+|V_f'|)+|V_{f1}|$ on the other hand, $|V_f|+|V_f'|-|V_{f1}|=2t-p$. Therefore, applying relations $|V_f|$, $|V_f'|\le t$, we have $|V_{f2}|=|V_f|-|V_{f1}|\ge t-p$ and $|V_1|=|V_f'|-|V_{f1}|\ge t-p$. Then, let $Z_1$ and $Z_2$ be any subsets of $V_{f2}$ and $V_1$, respectively, such that $|Z_1|=|Z_2|=t-p$. Further, let $V_2$ be denoted also by $X$. Since $|E(V_2,\ V_{f1})|\le r$ and $|E(V_2,\ V_1)|\le r$ by Lemma 2, we have the following inequalities.

$$|E(X,\ Z_1)|\le r \quad\text{and}\quad |E(X,\ Z_2)|\le r.$$

These inequalities contradict condition 3). Q.E.D.

**Corollary 2** (Theorem 2 in [2]): A system of $n$ units is $t$-diagnosable, if and only if: 1) $n\ge 2t+1$; 2) $d_{in}(v)\ge t$, for all $v \in V$; and 3) for any integer $p$, $0 \leq p < t$, and any $X \subset V$ with $|X| = n - 2t + p$, $|\Gamma X| > p$, where $\Gamma X = \{v \in \bar{X} \mid {}^{\exists} x \in X, (x, v) \in E\}$.

**Proof:** Since no test failure is allowed here, $r=0$. If there exist no two disjoint subsets $Z_1$, $Z_2 \subset \bar{X}$ such that $|Z_1| = |Z_2| = t-p$ and $|E(X, Z_1)| = |E(X, Z_2)| = 0$,

$$\begin{aligned} |\Gamma X| &> n - |X| - |Z_1| - |Z_2| \\ &= n - (n - 2t + p) - 2(t-p) = p \end{aligned}$$

Contrarily, if there exist such $Z_1$ and $Z_2$, $|\Gamma X| \leq p$.

Q.E.D.

As an example, we show in Fig. 2, a (1,1)-diagnosable system with the minimum number of units and the minimum number of connections. This example shows that condition 3) of Theorem 2 imposes more severe restriction both on the number of units and on the number of test connections than that by conditions 1) and 2).

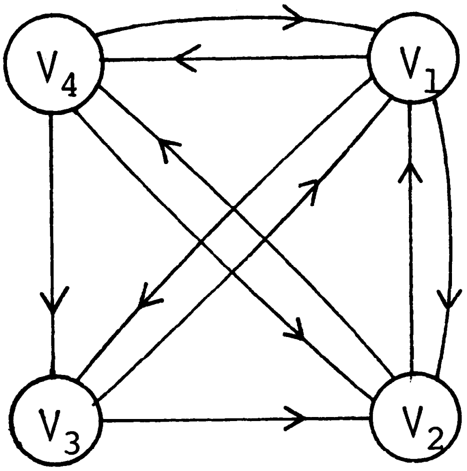

Fig. 2 An example of a (1, 1)-diagnosable system.

A problem of deciding whether a given system is $(t, r)$-diagnosable or not is a complicated one, because it needs extensive computations.

## 4. Conclusion

We have given the necessary and sufficient conditions for a system to be totally-$\tau$-diagnosable and $(t, r)$-diagnosable, assuming that even fault-free units may fail in testing faulty ones. An algorithm similar to that proposed by Kameda et al. [3] could be used for finding a set of faulty units. However, more computation time will be required due to additional backtrackings resulting from test failures.

Sequential and/or probabilistic method of diagnosis should also be investigated by taking not only unidirectional test failures but also bidirectional ones into consideration.

### References

1. Preparata, F. P., Metze, G. and Chien, R. T. On the Connection Assignment Problem of Diagnosable Systems, *IEEE Trans. Electron Comput.* **EC-16**, (Dec. 1967), 848-854.

2. Hakimi, S. L. and Amin, A. T. Characterization of Connection Assignment of Diagnosable Systems, *IEEE Trans. Comput.* **C-23**, (Jan. 1974), 86-88.

3. Kameda, T., Toida, S. and Allen, F. J. A Diagnosing Algorithm for Networks, *Information and Control* **29**, (1975), 141-148.

(Received April 12, 1984; revised October 1, 1984)