論 文

Redundant Digital System 에서의 고장진단에 관한연구

正會員 金 己 燮* 正會員 金 正 善**

On the Fault Diagnosis in a Redundant Digital System

Gi Seop KIM* *and* Jung Sun KIM**, *Regular Members*

要 約 본 논문에서는 m개의 고장까지 극복할 수 있는 기능적 m-리던던트(Functional m-redundant)시스템을 그래프 이론에 바탕을 두고 정의하였다. 이 시스템은 리던던시를 효과적으로 이용하여 추가적인 테스트 기능없이 각 부시스템의 출력을 서로 비교함으로써 $t(t \geq m)$고장진단 가능하고 진단을 위한 시스템 정지가 필요없도록 설계되었다. 또한 이 시스템에 대한 진단 모델을 제시하였고 이 모델이 preparata의 진단 모델로 바뀌어질 수 있음을 보였으며 이를 이용하여 기능적 m-리던던트 시스템의 진단 특성을 Preparata에 의해 제시된 방법으로 해석하였다.

ABSTRACT In this paper, a functional m-redundant system, which is m-fault tolerant, is defined based on the graph-theory. This system is designed to be $t(t \geq m)$ fault-diagnosable by comparing its unit's outcomes without additive test functions, so, the system down for diagnosis is not needed. The diagnostic model for this system is presented. It is to avail the redundancy of the system effectively. It is shown that this model can be converted into Preparata's model. Thus, the diagnostic characteristics of a functional m-redundant system is analyzed by the method originated by Preparata et al..

1. Introduction

Nowadays, owing to the increasing necessity and extensive application of computer system, the importance of system reliability and availability also increases.

A system which has the capability of finding out all the faulty subsystems in itself is called a self-diagnosable system and is highly available.

According to Preparata's model[1], a self-diagnosable system is divided into several units and each unit has the function of testing any other one or more units, so each unit is tested by one or more other units. Therefore, every unit should have the function of testing other units besides its own main function.

If one or more faulty units are found, they should be immediately repaired or replaced with fault-free units. But in some special cases, the down time for repairing the faulty unit is not allowed(in real-time applications), or manual access and replacement is impossible(e. g. space-ship, satellite etc.). And in the case of a very large computer system, the lost time cost is too high. For all these cases, the high reliability and availability are required. The system should be designed to perform its function normally against some faults(that is, it should be fault-tolerant), and fault diagnostic processing should be done on-line.

The concept of fault-tolerant system, which has been being studied since the computer was origina-

* 三星電子
Samsung Electronics Co., Ltd.
** 韓國航空大學電子工學科
Dept. of Avionics Engineeing, HanKuk Aviation College, Seoul 122 Korea.
論文番號 : 84 - 10 (接受 1983. 12. 7)

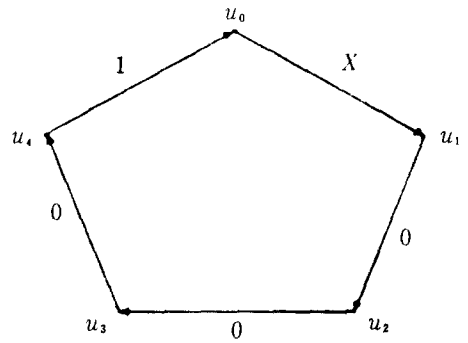

Fig. 1 A diagnostic model of system with 5 units.

ted, is using the redundancy and the study based on the graph-theory was firstly introduced by J. P. Hayes[7].

In this paper, a functional m-redundant system, which is a m-fault tolerant system, is defined based on the graph-theory. This system is designed to be $t(t \geq m)$ fault-diagnosable by comparing its outcomes without additive test functions, and since the diagnostic method of this system is comparing each outcome, the system down for diagnosis is not needed. These are achieved by using the redundancy effectively.

In chapter 2, the diagnostic model given by Preparata et al. is described, and in chapter 3, the structure of a functional m-redundant system is presented. In chapter 4, a method which can be used to analyze the diagnostic characteristics of this system is presented and it is analyzed by this method.

2. Fault Diagnosis in a Digital System

A system of n units is one-step t-fault diagnosable if all faulty units within the system can be identified without replacement provided the number of faulty units present does not exceed t. For one-step diagnosability, the characteristics of fault-diagnosable system was prescribed[2] and optimal system design was presented[1]. To build up new logic, these are reviewed in this chapter.

2-1. A Graph-theoretical Model for Diagnosis

The fault diagnosable system is composed of several units, and each unit can test one or more units and can be tested by one or more other units. If each unit is denoted by a node, and each test link by an edge, the fault diagnosable system S can be represented as digraph $G(V, E)$, and $(u_i, u_j) \in E$ if and only if unit u_i tests unit u_j in S. V is a set of all units and E is a set of all tests. The outcome of a test in which u_i tests u_j is denoted by a_{ij} where $a_{ij}=1$ if unit u_i finds unit u_j to be faulty and $a_{ij}=0$ if unit u_i finds unit u_j to be nonfaulty. If u_i is faulty, then the outcome a_{ij} is unreliable. The set of test outcomes a_{ij} represents the syndrome of the system.

Fig. 1 shows a diagnostic model of system composed of 5 units, when u_0 is assumed to be faulty. There are two possible syndromes.

2-2. One-step Fault Diagnosis

For a given digraph $G(V, E)$ of system S and syndrome σ, if, for $V_f \subset V$, 1) $(u_i, u_j) \in E$ with $u_i, u_j \in V_f$ implies $a_{ij}=0$, and 2) $(u_i, u_j) \in E$ with $u_i \in V_f$, $u_j \in V_f$ implies $a_{ij}=1$, then V_f is called Consistent Fault Set (CFS) of a system S. If such V_f which $|V_f| \leq t$ can be identified by system's syndrome σ obtained from test outcomes, the system S is t-diagnosable.

For a given digraph $G(V, E)$ and $u \in V$, let $\Gamma u = \{u_i | (u, u_i) \in E\}$ and $\Gamma X = \{\cup_{u \in X} \Gamma u - X\}$, $X \subset V$. Then necessary and sufficient conditions for a system S to be one-step t-fault diagnosable are given by Hakimi and Amin[2] as follow.

Theorem 2 of (Ref. 2): Let $G(V, E)$ be the digraph of a system S of n units. Then S is t-diagnosable if and only if;

1) $n \geq 2t+1$;
2) $d_n^*(u) \geq t$, for all $u \in V$; and
3) for each integer p with $0 \leq p < t$, and each $X \subset V$ with $|X| = n-2t+p$, $|\Gamma X| > p$.

Proof: By the proof of theorem 2 of (Ref. 2)

Optimal one-step t-fault diagnosable system design was Presented by Preparata et al.

Definition 5 of (Ref. 1): A one-step t-fault diagnosable system is said to be optimal if $n=2t+1$ and each unit is tested by exactly t units.

*$d_n(t)$: "Indegree of t": the number of edges direted toword t in G.

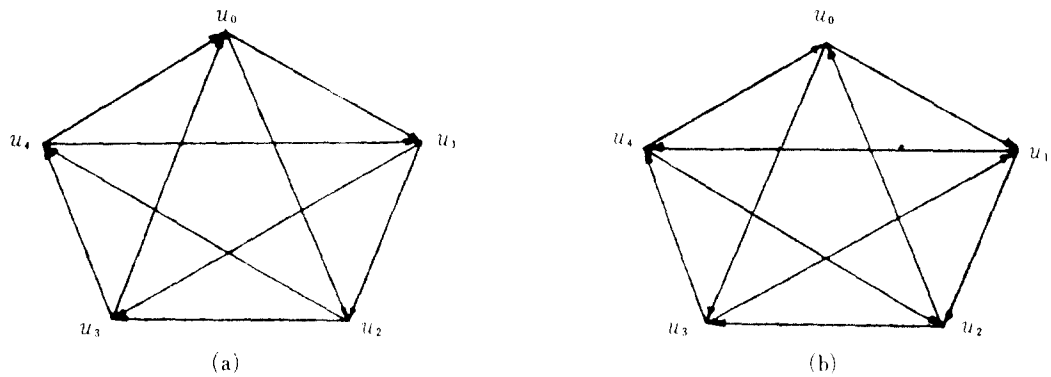

Fig. 2 (a) D_{12} system, (b) D_{22} system.

For given integer δ and t, a system S is said to belong to a design $D_{\delta t}$ when a test link frome u_i to u_j exists if and only if $j-i=\delta m$ (modulo n) and m assumes the values 1, 2, $\cdots t$. Then, it can be proved (Ref. 1, theorem 3) that a system is onestep t-fault diagnosable if it employs a design $D_{\delta t}$ with $(\delta, n)=1$, i.e. δ and n are relatively prime.

Fig. 2 shows $D_{\delta t}$ system when $t=$ when $t=2$ and $\delta=1, 2$. In These systems, it is always possible to find a set of all faulty units from possible synd rome when the number of faulty units is assu sumed not to exceed 2.

3. Fault Tolerant System

The problem of reliable computing has been studied since the computer was originated. A fault-tolerant computing system is that it is a system which has the built-in capability (without external assistance) to preserve the continued correct execution of its programs and functions in the presence of a certain set of operational faults[8]. An operational fault is an unspecified(failureinduced) change in the value of one or more logic variables in the hardware of the system.

The fault tolerance can be achieved bydiagnostic procedure and redundancy of system's structure or operation. For fault tolerance, a system can diagnose the presence and locations of faults. To achieve high reliability and availability, the diagnostic procedure have to be done on-line. And it is desirable to use the redundancy most effectively.

3-1. t-FT System Model

J. P. Hayes[7] represented computing system as facility graph G_f, in which each node x_i denotes system's facility and each edge denotes access link between facilities.

In this paper, t-FT system is defined based on this model. When the function of system S is A, let A be divided into its subfunctions f_i. Then we can write $A=\{f_i / i=0, 1, \cdots, k;\ k$ is any integer greater than zero$\}$. Assume that unit u_i can perform any subset of A. When unit u_i performs subfunctions f_i and f_j, we write $u_i(i, j)$. Then a system S can be denoted by graph G, in which each node is leveled with any subset of A, and it is interpreted as a unit which can perform several subfunctions.

The t-FT system can be defined as follow.

Definition 1: A system of n units is t-FT system if, when $t\ (t<n)$ unit(s) is(are) removed, the union of all subfunctions which can be performed by remaining $n-t$ unit (s) is A.

3-2. Design of t-FT System

If any subfunction is executed by several units, a t-FT system can be implemented. To be effective t-FT system, it should be designed to be minimum t-fault diagnosable and diagnostic processing to be done on-line.

Since a system should be composed of minimum $2t+1$ units to be t-diagnosable when the unit with no self-diagnosing capability is used, t-FT system should be composed of minimum $2t+1$ units.

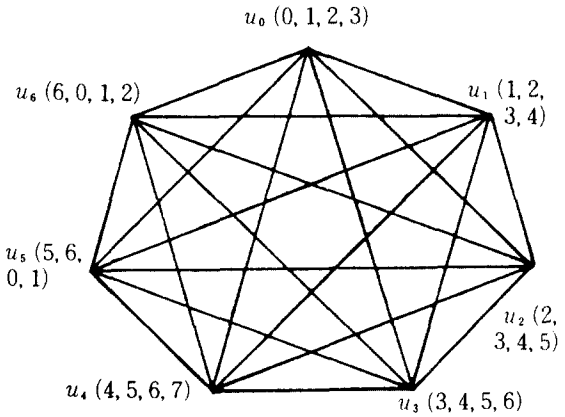

Fig. 3 A R_{13} system.

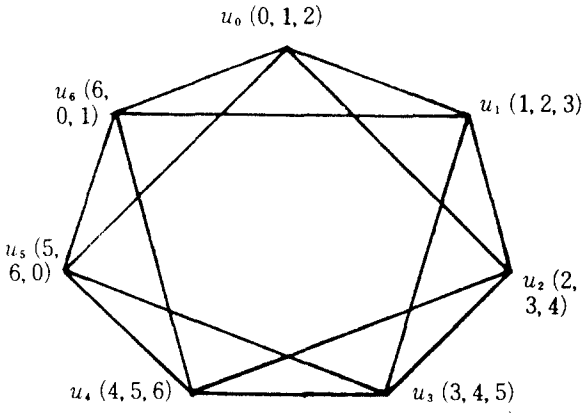

Fig. 4 A functional 2-redundant system with $n=7$

For optimal design, a function A of the system S is assumed to be divided into $2t+1$ subfunctions. If each subfunction is denoted by f_i $(i=0, 1, \cdots, n-1)$, a $R_{\sigma t}$ system is defined as follow.

Definition 2 : A system is a $R_{\sigma t}$ system if it is composed of $n=2t+1$ units, if each unit u_i can perform $t+1$ subfunctions f_i, $f(i+\delta) \bmod n, \cdots, f(i+\delta t) \bmod n$ and is connected with other t units $u(i+\delta) \bmod n$, $u(i+2\delta) \bmod n, \cdots, u(i+\delta t) \bmod n$.

Fig. 3 shows an example of R_{13} system. Each node denotes a unit which can perform anysubset of A and each edge denotes an access link be tween units.

Theorem 1 : A $R_{\sigma t}$ system is always t-FT.

Proof : Since a subfunction $f_i \in A$ is distributed in $t+1$ units, even if t unit (s) is (are) faulty, there is always one fault-free unit which can perform f_i. Thus a $R_{\sigma t}$ system is always t-fault tolerant.

Because each subfunction f_i is executed by $t+1$ units, a $R_{\sigma t}$ system is t-redundant. A general functional m-redundant system can be defined from the $R_{\sigma t}$ system as follow.

Definition 3 : When a system S of n units performs a function A, assume that A can be divided into n subfunctions f_i $(i=0, 1, \cdots, n-1)$. Then, for $m \leqq (n-1)/2$, the system S is a functional m-redundant system if each unit u_i can perform $m+1$ subfunctions f_i, $f(i+1) \bmod n, \cdots, f(i+m) \bmod n$ and is connected with other m units $u(i+1) \bmod n$, $u(i+2) \bmod n, \cdots, u(i+m) \bmod n$.

When $m=0$, the system is irredundant, and when n is odd and $m=(n-1)/2$, it is a R_{1t} system.

Corollary 1 : A functional m-redundant system is always m-fault tolerant.

Proof : It is apparent from the theorem 1.

Therefore, a t-FT system can be constructed with the structure of functional m-redundant system. Fig. 4 shows a functional 2-redundant system with $n=7$. It is a 2-FT system.

4. Fault Diagnosis in a Redundant Digital System

In the Preparata's diagnostic model, the syndrome of a system is obtained by test results. But in a redundant system, since a subfunction is executed by several units, the faults can be diagnosed by comparing their outcomes. Thus, diagnostic processing can be done on-line.

It is assumed that when unit $u_i(i, j)$ is faulty, none of two subfunctions f_i and f_j can be executed by $u_i(i, j)$. That is, when $u_i(i, j)$ is faulty, the outcomes of $u_i(i, j)$ for f_i and f_j are all incorrect. For diagnosis, there should be a comparing link between any two units which have one or more common subfunctions. Comparing result c_{ij} is 0 if unit u_i agrees with unit u_j for any subfunction f_k, and is 1 otherwise. It is apparent that $c_{ij}=c_{ji}$. The set of comparing results c_{ij} represents the syndrome of the system.

For given graph $G(V, E)$ of a system S and

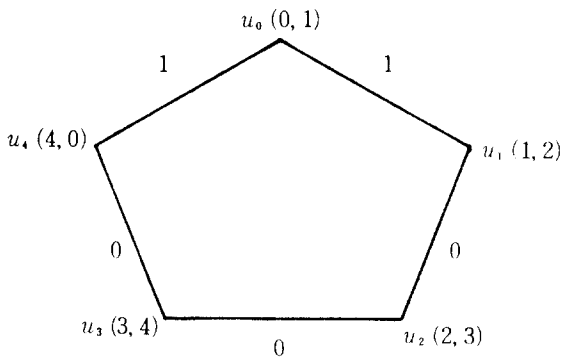

Fig. 5 An example of fault diagnosis in a functional 1-redundant system with $n=5$.

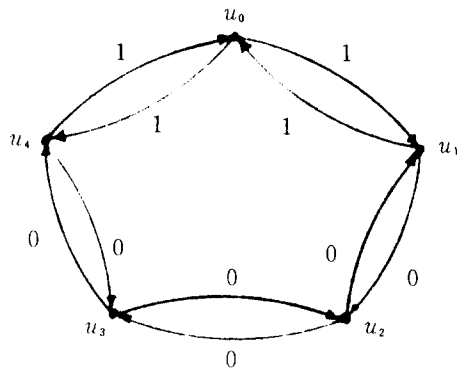

Fig.6 An equivalent preparata's diagnostic model of figure 5.

syndrome σ, if, for $V_f \subset V$, 1) $u_i, u_j \in V_f$ implies $c_{ij}=0$, and 2) $u_i \in V_f$ and $u_j \in V_f$ implies $c_{ij}=1$, then V_f is called Consistent Fault Set (CFS) of a system S for syndrome σ. If such V_f which $|V_f| \leq t$ can be identified by system's syndrome σ obtained from comparing, the system S is t-diagnosable.

Fig. 5 shows a diagnostic model for a functional 1-redundant system with $n=5$. The weight of each edge denotes comparing result when u_0 (0, 1) is assumed to be faulty. Since u_0 (0, 1) is faulty, c_{01} and c_{40} become 1. If it is assumed that the number of faulty unit does not exceed 2, it is always possible to find V_f which $|V_f| \leq 2$, that is, it is 2-diagnosable. This can be proved by the theorem (theorem 2) presented lately.

The diagnostic characteristics of a general redundant system can be analyzed by theorem 2 of (Ref. 2) if its diagnostic model can be converted into Preparata's modal.

Lemma 1 : It is always possible to interpret a comparing result c_{ij} of diagnostic model of a redundant system using two identical values $a_{ij}=a_{ji}$ of Preparata's model by the weight of c_{ij}.

Proof : a) When u_i and u_j are both fault free, $c_{ij}=0$ and $a_{ij}=a_{ji}=0$.

b) When any one unit (u_i) is faulty, $c_{ij}=1$ and $a_{ij}=x$, $a_{ji}=1$. Since a_{ij} is don't care term, it can be assumed to be 1.

c) When u_i and u_j are both faulty, $c_{ij}=x$ and a_{ij}, a_{ji} are both x. Therefore, these can be assumed to be any one of 1 and 0.

Therefore, in all cases, c_{ij} can be interpreted using two identical values $a_{ij}=a_{ji}$ by the weight of c_{ij}.

An equivalent Preparata's model of Fig. 5 is obtained as Fig. 6 using lemma 1.

From lemma 1, the following theorem is obtained.

Theorem 2 : If $n \geq 2t+1$ and $m=\lceil t/2 \rceil^*$, a functional m-redundant system composed of n units is always t-fault diagnosable.

Proof : By the lemma 1, the diagnostic model G of a functional m-redundant system S can be converted into an equivalent Preparata's model G', so it is sufficient to show that G' satisfies theorem 2 of (Ref. 2)

a) Since $n \geq 2t+1$, it satisfies theorem 2, 1) of (Ref. 2)

b) By the definition of a functional m-redundant system, for all $u \subset V$, $d_{in}(u)=2m$. Since $m=\lceil t/2 \rceil$, $2m \geq t$. Thus, $d_{in}(u)=2m \geq t$ and it satisfies theorem 2, 2) of (Ref. 2)

c) X which makes $|\Gamma X|$ minimum is a set of adjacent units. Let X be a set of $k (0<k<n-t)$ adjacent units, then $X=\{u_i, u(i+1) \bmod n, \cdots, u(i+k-1) \bmod n\}$. Since S is a functional m-redundant system, $u(i+k-1) \bmod n$ has $m+1$ subfunctions $f(i+k-1) \bmod n$, $f(i+k) \bmod n, \cdots$, $f(i+k+m-1) \bmod n$. Thus, $u(i+k-1) \bmod n$ of G' has test links to a set of m units $A=\{u_j | u_j \notin X, j=(i+k) \bmod n, (i+k+1) \bmod n, \cdots, (i$

*$\lceil X \rceil$: "Ceiling of X": the least integer $\geq x$

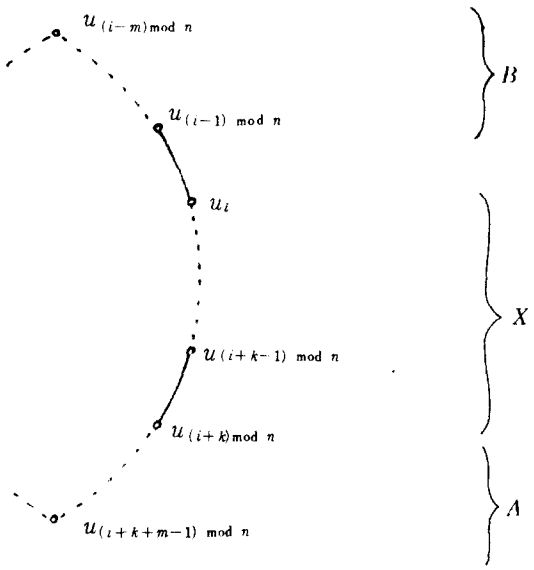

Fig.7 Proof of theorem 2.

$+k+m-1) \bmod n\}$. And since m units $u(i-1) \bmod n$, $u(i-2) \bmod n, \cdots$, and $u(i-m) \bmod n$ have f_i, u_i has test links to a set of m units $B=\{u_j \mid u_j \notin X,\ j=(i-m) \bmod n,\ (i-m+1) \bmod n, \cdots,\ (i-1) \bmod n\}$.

Then, $X \subset V$, $A \subset V$, $B \subset V$, $\Gamma X \subset V$ and $\Gamma X = A \cup B$. And $|V|=n$, $|X|<n-t$ and $|A|=|B|=m$.

i) When t is even, $m=t/2$. Thus, $|X|+|A|+|B| \leq n-t+2m=n-t+t=n$. Then, we have $A \cap B=\phi$ from Fig. 7. Therefore, $|\Gamma X|=|A \cup B| = |A|+|B|-|A \cap B|=2m=t$. and since $p \leq t-1$, we have $|\Gamma X|>p$ for all X.

ii) When t is odd, $m=t2+1$. Thus, $|X|+|A|+|B| \leq n-t+2m=n-t+t+1=n+1$. Then, we have $A \cap B=\phi$ from Fig. 7. Therefore, $|\Gamma X|=A \cup B|=|A|+|B|-|A \cap B|=2m=t+1$, and since $p \leq t-1$, we have $|\Gamma X|>p$ for all X.

In both cases, we have $|\Gamma X|>p$, so, it satisfies theorem 2, 3) of (2).

Since G' satisfies theorem 2 of (Ref. 2), it is always t-fault diagnosable.

From above theorem, it is shown that a R_{1t} system is always t-fault diagnosable. According to theorem 2, it is possible to construct a fault-

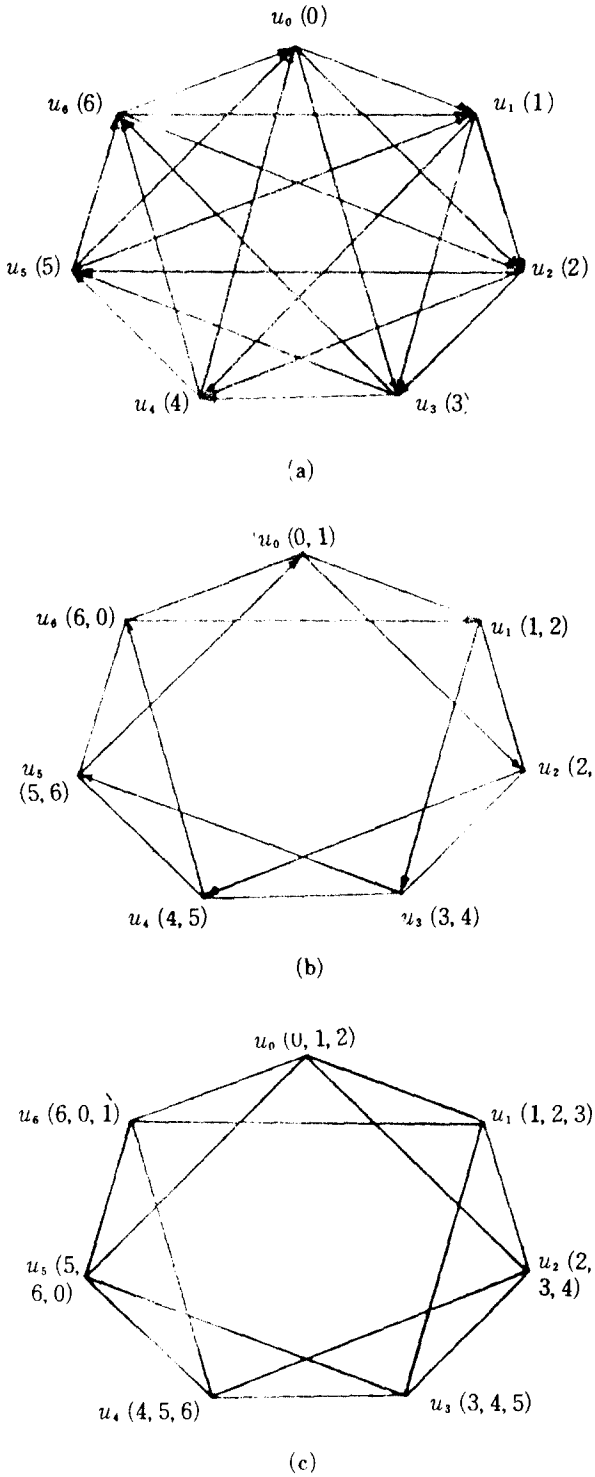

Fig. 8 Examples of 3-fault diagnosable system

diagnosable system using only comparing links.

When a high reliable and available system is needed, it is necessary to use some redundancies. In this case, these redundancies can be effectively used to improve the diagnosability of a system by adapting the strategy presented in this paper.

Fig. 8 shows examples of various 3-fault diagnosable system with $n=7$. a) indicates a D_{13} system with no redundancy. b) shows a system with $m=1$, that is, 1-FT. The diagnosability of this system achieved by comparing links is 2. With $m=1$, additive test links are required to obtain the diagnosability of more then 2. c) shows a 2-FT system with $m=2$, and this has no test link since it is 3-fault diagnosable only with comparing links.

5. Conclusions

Up to now, we considered the method of implementing a high reliable and available digital system. The main concept of fault-tolerant system is to avail the redundancy. In this paper, using the redundancy effectively, a m-fault tolerant system is implemented to be $t(t \geq m)$-diagnosable without additive fault diagnostic functions. And such a system could be analyzed by the diagnostic model proposed by Preparata et al..

Since the diagnostic method using redundancy is finding out the fault by comparing each outcome, there is no need of system down for diagnosis. In the functional m-redundant system, the fault can be immediately diagnosed and this system can perform its functions correctly without degradation until the number of faulty units does not exceed m. And it is possible to improve the diagnosability of the system up to $2m$ provided the number of units and subfunctions is greater then $4m+1$.

When the redundancy is inevitable, the redundancy can be most effectively used by adapting the strategy presented in this paper.

REFERENCES

(1) F. P. Preparata, G. Metze, and R. T. Chien, "On the connection assignment problem of diagnosable systems," IEEE Trans. Electron Computers, vol. EC-16 pp. 848-854, Dec. 1967.

(2) S. L. Hakimi, and A. T. Amin, "Characterization of connection assignment of diagnosable systems," IEEE Trans. Computers, vol. C-23, pp. 86-88, June 1974.

(3) J. D. Russell, and C. R. Kime, "System fault diagnosis: Closure and diagnosability with repair," IEEE Trans. Computers, vol. C-24, pp. 1078-1089, Nov. 1975.

(4) C. Manber, "System diagnosis with repair," IEEE Trans. Computers, vol. C-29, pp. 934-937, Oct. 1980.

(5) S. Karunanithi, and A. D. Friedman, "Analysis of digital systems using a new measure of system diagnosis," IEEE Trans. Computers, vol. C-28, pp. 121-133, Feb. 1979.

(6) A. D. Friedman, and L. Simoncini, "System level fault diagnosis," Computer, pp. 47-53, Mar. 1980.

(7) J. P. Hayes, "A Graph model for fault-tolerant computing systems," IEEE Trans. Computers, vol. C-25, pp. 875-884, Sep. 1976.

(8) A. Avizienis, "Fault-tolerant systems," IEEE Trans. Computers, vol. C-25, pp. 1304-1312, Dec. 1976.

(9) J. P. Hayes, "Computer architecture and organization," McGraw-hill, 1978.

(10) D. P. Siewiorek, and R. S. Swarz, "The theory and practice of reliable system design," Digital Press, 1982.

(11) J. A. Bondy, and U. S. Murty, "Graph theory with applications," American Elsevier Publishing Co., 1976.

金 己 燮 (Gi Seop KIM) 正會員

1960年 4月 2日生

1982年 2月：韓國航空大學電子工學科卒業

1984年 2月：韓國航空大學大學院電子工學科(工學碩士)

1984年 2月～現在：三星電子 Computer 事業部開發部研究員

金 正 善 (Gung Sun KIM) 正會員

1941年 5月 5日生

1965年：韓國航空大學電子工學科卒業

1972年：淸州大學校大學院(電子工學)修了

1965年～現在：韓國航空大學副敎授, 學科長, 本學會編輯委員會編輯委員