한국통신학회 1983년도 추계학술발표회 논문집 ( 1983· 10· 29 )

# Redundant 디지탈 시스템에서의 고장진단에 관한 연구

○김기섭 김정선
한국항공대학 전자과

# On the Fault-Diagnosis in a Redundant Digital System

○Gi Seop KIM, Jung Sun KIM
Hankuk Aviation College, Dept. of Avionics

## 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≥m) fault-diagnosable by comparing its unit's outcomes without additive test functions, and so, the system down for diagnosis is not needed. The diagnostic model for this system is presented and this effectively uses system's redundancy. 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 systems, the importance of self-diagnosable system also increases. Asystem which has the capability of finding out all the faulty subsystems in itself is called a self-diagnosable system.

According to Preparata's model[1](in this paper, we call it 'fault diagnosis in irredundant system'), a 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 fount, 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 system should be designed to perform its function normally against some faults, and fault diagnosis processing should be done on-line. Thus, the concept of fault-tolerant system has been emphasized.

The concept of fault-tolerant system, which has been being studied since the computer was originated, uses the redundancy and the study based on the graph-theory was firstly introduced by J.P.Hayes(4).

In this paper, a functional m-redundant system, which is m-fault tolerant system, is defined based on the graph-theory. This system is designed to be t( t≥ m) fault-diagnosable by comparing its unit's outcomes without additive test functions, and since the diagnosis method of this system is comparing each unit's outcomes, the system down for diagnosis is not needed.

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 diagnosis characteristics of this system is presented and it is analyzed by this method.

## 2. Fault Diagnosis in Irredundant System

### (1) A Graph-theoretical Method for Diagnosis

The fault diagnosable system is composed of several units, and each unit can test the other unit. If each unit can be represented as node, and each test link as edge, the fault diagnosable system S can be denoted by digraph $G(V,E)$ and $(u_i, u_j) \in E$ if and only if unit $u_i$ tests $u_j$ in S. 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 $a_{ij}=1$ if $u_i$ finds $u_j$ 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.

Definition 1 : 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.

### (2) One-step Fault Diagnosis

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

For a given digraph $G(V,E)$ and $u \in V$, let $\Gamma u=\{u_i \mid (u,u_i) \in E\}$ and $\Gamma X=\{\bigcup_{u \in X} \Gamma u-X\}$, $X \subset V$. Then the relation among the number of units n,t and test link is given as follow.

Theorem 1 : 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) $d_{in}(u) \geq t$, 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: Theorem 2. of (2).

For given integer and t, a system S of $n(n=2t+1)$ units is said to belong to a design $D_{\delta t}$ when a testing link from $u_i$ to $u_j$ exists if and only if $j-i=\delta m (\mathrm{mod}\ n)$ and m assumes the values 1,2,...,t.

Lemma 1 : If a system S employs design $D_{\delta t}$ such that $(\delta,n)=1$ then S is one-step t-fault diagnosable and $D_{\delta t}$ is an optimal design.

proof : Theorem 3. of (1).

So, an optimal one-step t-diagnosable system can be obtained by $D_{\delta t}$ design. Fig.1 shows example of $D_{\delta t}$ system for t=2 and $\delta=1$.

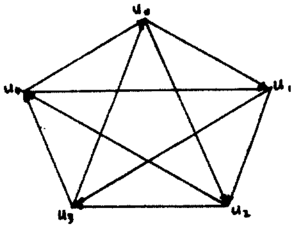

Fig.1. $D_{\delta t}$ system.

## 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(5). An operational fault is an unspecified(failure-induced) change in the value of one or more logic variable in the hardware of the system.

The fault tolerance can be achived by diagnostic processing and redundancy of system's structure or operation. For fault tolerance, a system can diagnose the presence of faults and its location, and it should have redundancy for compensating these faults.

### (1) t-FT System Model

J.P.Hayes(6) represented computing system as Facility graph $G_f$, of which node $x_i$ represents system's facilities 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 subfunction $f_i$. Then we can write $A=\{f_i|$ $i=0,1,\ldots,k$; k is any integer greater then zero$\}$. When unit $u_i$ performs subfunction $f_i, f_j$, we write $u_i(i,j)$. Then a system S can be represented as Graph G, in which each node denotes any subset of A, and it is interpreted as a unit which can perform several subfunctions.

Definition 2 : 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 units is A.

(2) Design of t-FT System

If any subfunction is performed by several units, a t-FT system can be implimented. Since the effective t-FT system should be t-diagnosable, it is desirable to be designed whit this consideration.

Since a system should be composed of minimum 2t+1 units when the units which have no self-diagnosing capability are used, the t-FT system should be composed of minimum 2t+1 units. For optimal design, a function A of the system is assumed to be divided into 2t+1 subfunctions. If each subfunction is denoted by $f_i(i=0,1,\ldots,n-1)$, a $R_{\delta t}$ system is defined as follow.

Definition 3 : A system is a $R_{\delta t}$ system if it is composed of n=2t+1 units, and if each unit $u_i$ can perform t+1 subfunctions $f_i$, $f_{(i+\delta)\text{mod } n}$, ..., $f_{(i+\delta t)\text{mod } n}$ and is connected with other t units $u_{(i+\delta)\text{mod } n}$, ..., $u_{(i+\delta t)\text{mod } n}$.

Fig.2 shows an example of $R_{13}$ system. Each node denotes a unit which can perform any subset of A and each edge denotes an access link between units.

Theorem 2 : A $R_{\delta t}$ system is always t-FT.

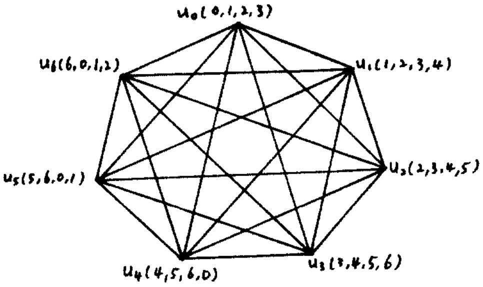

Fig.2. $R_{13}$ system

proof : Since a subfunction $f_i \in A$ is distributed in t+1 units, even if t unit(s) is(are) faulty, there is(are) always more then or equal to one unit. So, a $R_{\delta t}$ system is always t-FT.

A general functional m-redundant system can be defined from $R_{\delta t}$ system.

Definition 3 : When a system S of n units has a function A, assume that A can be divided into n subfunctions $f_i(i=0,1,\ldots,n-1)$. then, for $m\leq(n-1)/2$, the system S is a functional m-redundant system if each unit $u_i$ can perform m+1 subfunctions $f_i$, $f_{(i+1)\text{mod } n}$, ..., $f_{(i+m)\text{mod } n}$ and is connected with other m units $u_{(i+1)\text{mod } n}$, $u_{(i+2)\text{mod } n}$, ..., $u_{(i+m)\text{mod } n}$.

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

proof : It is apparent from theorem 2.

## 4. Fault Diagnosis in a Redundant 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 performed by several units, the faults can be diagnosed by comparing their outcomes. So, for diagnosis, any two units which have same subfunctions should have a comparing link. A comparing result $C_{ij}$ is 0 if $u_i$ agrees with $u_j$ for any subfunction $f_k$, and is 1 otherwise.($C_{ij}=C_{ji}$)

Fig.3 shows a diagnostic model for a functional 1-redundant system with n=5. The weight of each edge represents comparing outcomes when $u_0(0,1)$ is assumed to be faulty. Since $u_0(0,1)$ is faulty, $C_{01}$, $C_{40}$ become 1. If it is assumed that the number of faulty unit does not exceed 2, this system can diagnose upto 2 faults.

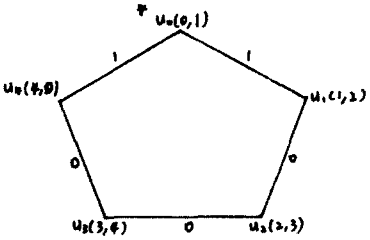

Fig.3 Example of fault diagnosis in a functional 1-redundant system(n=5).

The diagnostic characteristics of general redundant system can be analyzed by Theorem 1 if its diagnostic model can be converted into an irredundant system model.

Lemma 2 : A comparing result $C_{ij}$ of a redundant system is interpreted as two test results $a_{ij}$, $a_{ji}$ of an irredundant system.

proof : There are three comparable cases as follow;

a) both $u_i$, $u_j$ are fault free : then, $C_{ij}=0$ and $a_{ij}=a_{ji}=0$. Therefore, $C_{ij}$ can be interpreted using two identical value $a_{ij}=a_{ji}$ by the weight of $C_{ij}$.

b) any one unit($u_i$) is faulty ; then $C_{ij}=1$ and $a_{ij}=x$, $a_{ji}=1$. Since $a_{ij}$ is don't care , it can be assumed to be 1. Therefore, $C_{ij}$ can be interpreted using two identical value $a_{ij}=a_{ji}$ by the weight of $C_{ij}$.

c) both $u_i$, $u_j$ are faulty ; then, $C_{ij}=x$ and $a_{ij}$, $a_{ji}$ are both x. Therefore, $C_{ij}$ can be interpreted using two identical values $a_{ij}=a_{ji}$ by the weight of $C_{ij}$.

Fig.4 shows an equivalent irredundant system model for a that of Fig.3.

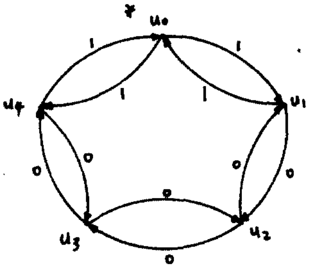

Fig.4. An equivalent diagnostic model of Fig.3.

From lemma 2, the following theorem is obtained.

Theorem 3 : 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 lemma 2, a functional m-redundant system model S can be converted into an equivalent irredundant system model S', so, it is sufficient to show that S' satisfies theorem 1.

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

b). By definition of a functional m-redundant system, for all $u \in V$, $d_{in}(u)=2m$. Since $m=\lceil t/2 \rceil$, $2m \geq t$. Thus, $d_{in}(u)=2m \geq t$ and it satisfies theorem 1, 2).

c). X, which makes $|\Gamma X|$ minimum, is a set of ajacent units. Let X be a set of k ajacent units, then $X=\{u_i, u_{(i+1)\bmod n}, \ldots, u_{(i+k-1)\bmod n}\}$. Since S is a functional m-redundant system, $u_{(i+k-1)\bmod n}$ of S' has m+1 subfunctions $f_{(i+k-1)\bmod n}$, $f_{(i+k)\bmod n}$, ..., $f_{(i+k+m)\bmod n}$. Thus, $u_{(i+k-1)\bmod n}$ has

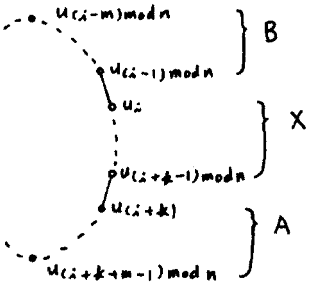

Fig.5. Proof of theorem 3, c).

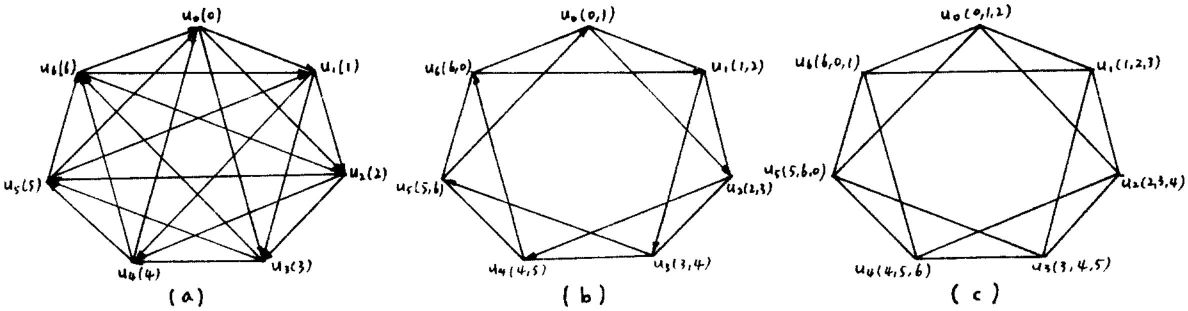

**Fig.6.** Examples of 3-fault diagnosable systems.

test links to a set of m units $A=\{u_j \mid u_j \notin X,\ j=(i+k)\bmod n, (i+k+1)\bmod n, \ldots, (i+k+m-1)\bmod n\}$. And since m units $u_{(i-1)\bmod n}$, $u_{(i-2)\bmod n}, \ldots$ and $u_{(i-m)\bmod n}$ have $f_i$, $u_i$ has test links to a set of m units $B=\{u_j \mid u_j \notin X,\ j=(i-m)\bmod n, (i-m+1)\bmod n, \ldots, (i-1)\bmod n\}$. Then, $X \subset V$, $A \subset V$, $B \subset V$ and $\Gamma X \subset V$. Since $X \cap \Gamma X = \emptyset$, we have $|X| + |\Gamma X| \leq |V|$. And $|V| \geq 2t+1$, $|X| \leq t$, $|A| = |B| = m$ and $\Gamma X = A \cup B$.

i) when t is even, $m=t/2$. Thus, $|X| + |\Gamma X| = |X| + |A \cup B| = |X| + |A| + |B| - |A \cap B| \leq t + 2m - |A \cap B|$. Since $|V| > 2t$, we have $A \cap B = \emptyset$ from Fig.5. Therefore, $|\Gamma X| = |A| + |B| = 2m = t$. Since $p = t-1$, we have $|\Gamma X| > p$.

ii) when t is odd, $m=t/2+\frac{1}{2}$. Thus, $|X| + |\Gamma X| = |X| + |A \cup B| = |X| + |A| + |B| - |A \cap B| \leq t+2m- |A \cap B| = 2t + 1 - |A \cap B|$. Since $|V| \geq 2t + 1$, we have $A \cap B = \emptyset$ from Fig.5. Therefore, $|\Gamma X| = |A| + |B| = 2m = t + 1$. Since $p = t - 1$, we have $|\Gamma X| > p$.

In all cases, we have $|\Gamma X| > p$, so, it satisfies theorem 1. 3).

From above theorem, it is seen that a $R_{1t}$ system is always t-fault diagnosable. According to theorem 3, it is possible to construct a fault-diagnosable system only using comparing links.

Fig.6 shows various examples of various 3-fault diagnosable system with n=7. a) indi indicates Preparata's $D_{13}$ system with no redundancy. b) shows a system with m=1, which has additive test links since it is not 3-fault diagnosable only with comparing links. This system is not only 3-diagnosable, but also 1-FT. c) shows a 2-FT system with m=2, In this case, this system has no test link since it is 3-fault diagnosable only with comparing links.

## 5. Conclusion

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

The diagnosis method using redundancy finds out the fault by comparing each output, therefore there's no need of system down for diagnosis. And in $R_t$ 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 t.

This study can especially be applied to a distributed computer system.

In this paper, the indirect method which is used to analyze the diagnostic characteristics of a redundant system by converting its model into an irredundant one' was presented, but it is needed to study about the direct method which can be used to analyze that from its own model.

## References

(1) F.P.Preparata, G.Metze, and R.T.Chien, "On the Connection Assignment Problem of Diagnosable System," IEEE Trans. Electron Computer, 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, Jun. 1974.

(3) A.D.Friedman and L.Simoncini, "System-Level Fault Diagnosis," Computer, pp. 47-53, March 1980.

(4) J.P.Hayes," A Graph Model for Fault-Tolerant Computing Systems," IEEE Trans. Computers, Vol. C-25, pp.875-884, Sep. 1976.

(5) A.Avizienis, "Fault-Tolerant System," IEEE Trans. Computers, Vol. C-25, pp.1304-1312, Dec. 1976.

(6) J.P.Hayes, "Computer Architecture and Organization," McGraw-Hill, 1978.