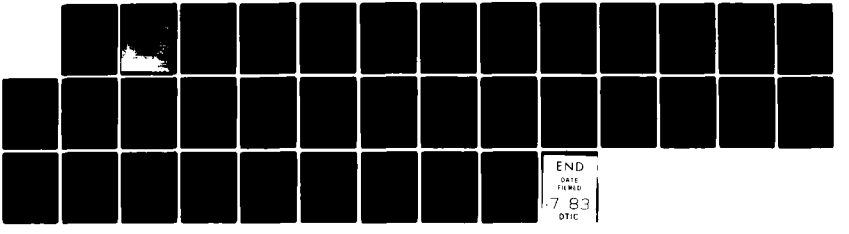
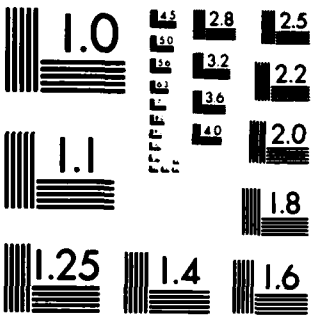
AD-A129 474 A NEW SYSTEM-LEVEL APPROACH TO DIAGNOSABILITY(U) JOHNS 1/1
HOPKINS UNIV BALTIMORE MD DEPT OF ELECTRICAL ENGINEERIN
.. B L HAVLICSEK ET AL. 01 DEC 82 JHU/EECS-82/6
UNCLASSIFIED N00014-80-C-0772 F/G 9/2 NL





The Johns Hopkins University

(12)

A NEW SYSTEM-LEVEL APPROACH TO DIAGNOSABILITY

B.L. Havlicsek and G.G.L. Meyer

Technical Report JHU/EECS-82/6

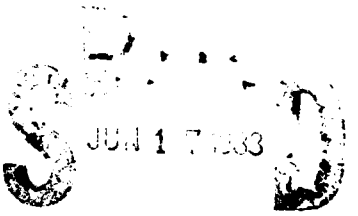
A NEW SYSTEM-LEVEL APPROACH TO DIAGNOSABILITY

B.L. Havlicsek and G.G.L. Meyer

Technical Report JHU/EECS-82/6

Electrical Engineering and Computer Science Department
The Johns Hopkins University
Baltimore, Maryland 21218

December 1, 1982



A

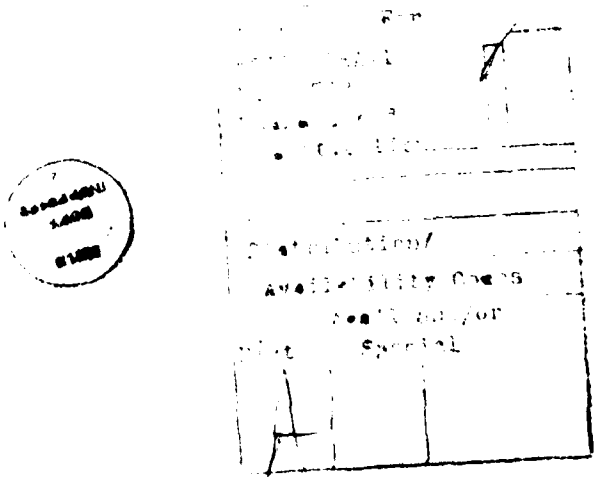
This work was supported in part by the Office of Naval Research under Contract N00014-80-C-0772 and in part by the Westinghouse Electric Corporation, Integrated Logistics Support Division, Hunt Valley, Maryland.

ABSTRACT

This paper presents a new approach to determine the conditions that ensure diagnosability properties in complex systems. In previous approaches, a fault-test relationship is assumed and all diagnosability conditions depend on both this relationship and the desired diagnosability property. In our approach, such assumptions are not required, so that diagnosability conditions depend only on the desired diagnosability property.

This method uses a new system-level fault model having both internal and observable test outcomes and allowing multiple test outcomes to be associated with each fault situation. By defining different sets of internal test outcomes, one can represent the desirable diagnostic properties of the model.

In this paper, diagnosability conditions for models possessing morphic properties are given. As an example, the conditions are applied to the fault model of Preparata, Metze and Chien. The results obtained demonstrate that 1) new diagnosability conditions can be determined and 2) the previous diagnosability conditions can be reconstructed and applied to a larger class of fault models.



1. INTRODUCTION

One of the most challenging problems currently facing the electronics industry is that of designing systems and tests for the detection and diagnosis of failures. There are two primary causes of this problem: 1) the increased complexity of systems has greatly increased the number of possible fault situations, and 2) the reduced accessibility of the circuit due to higher density components has reduced the availability of test results. Both causes increase the likelihood of multiple failures.

Previous approaches have addressed this system design and test generation problem by using a *system-level fault model* [FRI80] to describe the relationship between fault situations and test outcomes. Such models effectively reduce the number of fault situations by treating a large aggregation of failures as a single complex fault situation. Test results from these fault situations are compactly represented in order to reduce the volume of test data. These models are thus vehicles for examining the diagnosability of a system and improving the selection of tests.

This paper presents a new approach to determine the conditions that ensure diagnosability properties in complex systems. In previous approaches, a fault-test relationship is assumed and all diagnosability conditions depend on both this relationship and the desired diagnosability property. In our approach, such assumptions are not required, so that diagnosability conditions depend only on the desired diagnosability property. Since guidelines for system testability are derived from diagnosability conditions, the guidelines developed from this new approach are not limited by an assumed fault-test relationship.

The approach uses a new system-level fault model to represent relation-

ships between faults and test outcomes. By permitting multiple test outcomes to be associated with each fault situation, this model can represent a large aggregation of failures as a single system-level fault situation. Additional structure is introduced by using both internal and observable test outcomes. Internal test outcomes play a role analogous to that of state variables in linear system models by allowing the representation and analysis of properties that may not be directly observable. By defining different sets of internal test outcomes, one can represent the desirable diagnostic properties of the model.

The application of this new approach is demonstrated by determining diagnosability conditions for multiple fault diagnosis. Efficient analysis of multiple faults is provided by models possessing morphic properties. These properties allow one to determine multiple fault test outcomes from the outcomes of the single fault components. As an example, we apply the conditions to the fault model of Preparata, Metze and Chien [PRE67]. The results obtained demonstrate that 1) new diagnosability conditions can be determined and 2) the previous diagnosability conditions can be reconstructed and applied to a larger class of fault models.

2. FAULT MODEL DEFINITION

For a typical fault model, a set of fault situations is given and a set of observable syndromes representing the possible results of a testing procedure is defined. Thus, the typical fault model is described by the threetuple $(A, Y^p, \hat{G}(.))$, where A is a set of fault situations, Y^p is a set of observable syndromes and $\hat{G}(.)$ is a map from A into Y^p.

In contrast to the typical fault model, the model defined in this paper is described by the quintuple $(A, Z^p, Y^p, G(.), H(.))$, where A is a set of admissible fault situations, Z^p is a set of internal syndromes, Y^p is a set of observable syndromes, $G(.)$ is a map that relates fault situations and internal syndromes, and $H(.)$ is a map that relates internal syndromes and observable syndromes.

Clearly, all typical fault models may be represented by choosing $H(.)$ as the identity map, and letting $G(.) = \hat{G}(.)$. It is possible, however, to introduce additional structure into this model by using various sets of internal syndromes and maps $H(.)$. As a result, a specific model has multiple representations, some of which are more convenient for analyzing and deriving diagnosability conditions.

We will now define precisely the components of the fault model. To facilitate the definition of fault situations, we define a set of distinct elementary fault situations

$$E = \{f_1, f_2, \ldots, f_n\},$$

where the fault situations f_i, $i = 1,2, \ldots, n$ are elementary only in the sense that there is no need to isolate failures more precisely. As a result, an elementary fault situation may represent an aggregation of distinct failure modes, each of which may have a different effect on the overall operation of the system.

Let A_n be the family of all subsets of E. The empty subset represents the nonfaulty mode of the system and is denoted by F_0. All possible fault situations are represented by elements in A_n; however, in many cases it is desirable to restrict the analysis to a subset of the possible fault situations. Let $A \subseteq A_n$ be the set of admissible fault situations,--that is, it is assumed that only these fault situations may occur. Often, the admissible fault situations are defined as the subsets of E that have cardinality less than or equal to an integer τ, $1 \leqslant \tau \leqslant n$. In this case, denote $A_\tau \subseteq A_n$ as the set of fault situations defined by

$$A_\tau = \{ F \in A_n \mid \|F\| \leqslant \tau \}.$$

The union of two fault situations, $F_i \cup F_j$, represents the fault situation consisting of all elementary faults in F_i and F_j. Similarly, the intersection $F_i \cap F_j$ represents the fault situation consisting of only those elementary faults common to both F_i and F_j.

Associated with the system is a testing procedure consisting of a set of p tests,

$$T = \{t_1, t_2, \ldots, t_p\}.$$

The outcome of test t_j is denoted by a variable x_j that takes values in a set Z. We have assumed that Z is finite, therefore let Z be the set

$$Z = \{0, 1, 2, \ldots, q-1\}.$$

The test outcome '0' represents the behavior of each test in the presence of fault situation F_0. Clearly, in order for the model to provide useful information, it is necessary that $q \geqslant 2$. When $q = 2$, a test that produces outcome '0' is said to *pass*, and a test producing outcome '1' is said to *fail*.

The set of test outcomes for a single application of all p tests is represented by the p-tuple

$$x = (x_1, x_2, \ldots, x_p).$$

This vector of test outcomes is called an *internal syndrome* of the system and the space of all internal syndromes is denoted by Z^p.

Failures are assumed to be permanent and deterministic so that a given set of failures occurring simultaneously always produces a single unique syndrome. Yet, because of the complexity allowed in the definition of an elementary fault situation, more than one syndrome may be associated with a given admissible fault situation.

The fault model defined in this paper uses a point-to-set map to represent this uncertainty. Each choice of a set of admissible fault situations and a given testing procedure defines a unique *admissible fault situation - syndrome (AFSS) map* $G(.)$ from the domain A of admissible fault situations to collections of non-empty subsets in the range Z^p of all possible internal syndromes. The assumption that the sets E, T, and Z are finite implies that the AFSS map can be represented in a tabular form by an *AFSS table*.

Although the set Z may reflect some internal structure of a testing procedure, such knowledge may not be available if information is lost in the process of observing the syndromes. This occurs, for example, if different test outcome values representing internal properties of the model cannot be distinguished by an observer. In order to introduce this concept into the fault model, let

$$Y = \{0, 1, 2, \ldots, r-1\}$$

be the set of possible observations of test outcomes, and let the observation

process be represented by a map

$$H(.):Z \rightarrow Y.$$

In this paper we consider only those observation processes that can be decomposed into observations of individual test outcomes. The observation of a internal syndrome is thus represented by the map

$$H(x) = (H(x_1), H(x_2),..., H(x_p)),$$

where x is a syndrome in Z^p. In this manner, the primary structure of the model is described by the AFSS table. The map $H(.)$ may be either a point-to-point or a point-to-set map. In the latter case, it is possible to restrict the uncertainty associated with a fault situation to the observation map and produce a point-to-point AFSS table by choosing specific internal test outcomes.

Here we have assumed that the nonfaulty situation F_0 and each elementary fault situation are admissible. Thus, $A_1 = E \cup \{F_0\}$ is the greatest lower bound of A. Also, the internal test outcome '0', which represents the behavior of a test when the system is nonfaulty, is assumed to be uniquely observable as the observable outcome '0'. In order to remove trivial models, we have also assumed that at least one test and more than one internal and more than one external test outcome exist. Throughout this paper we have assumed the following basic hypothesis.

Hypothesis 2.1: Let $S = (A, Z^p, Y^p, G(.), H(.))$ be a fault model. Then,

(i) $n = |E| \geq 1$

(ii) $A_1 \subseteq A$

(iii) $p = |T| \geq 1$

(iv) $q = |Z| \geq 2$

(v) $r = |Y| \geq 2$

(vi) $G(F_0) = \{ (0,0,...,0) \}$

(vii) $H(0) = 0$.

The purpose of defining such a general structure for fault models is to allow flexibility in defining diagnosability properties and in deriving diagnosability conditions. This paper deals primarily with the one-step τ-fault diagnosability property [PRE67], in which all admissible fault situations of cardinality τ or less can be repaired by replacing all faulty and only faulty components after only one application of the testing procedure.

Definition 2.2: A fault model S is *one-step τ-fault diagnosable* if and only if τ is such that $1 \leqslant \tau \leqslant n$, and for every pair of fault situations F_a, F_b in $A \cap A_\tau$ such that $F_a \neq F_b$,

$$H(G(F_a)) \cap H(G(F_b)) = \phi.$$

3. MORPHIC FAULT MODELS

Without additional structure in the fault model, one cannot simplify the conditions for one-step τ-fault diagnosability beyond the definition. Under the basic hypothesis, the only inherent structure of the fault models exists in the set A_n by virtue of the union operation. For this set, the union operation is an associative and commutative binary operation, and the fault situation F_0 functions as the unique identity element. This inherent structure is of value when multiple faults (fault situations of cardinality greater than one) are admissible and the binary operation on A_n is in some manner "preserved" by the maps $G(.)$ and $H(.)$. This implies that multiple fault syndromes can be obtained from the syndromes of their elementary fault components. When this is possible, the model is said to possess a *morphic property* [HAV81].

Morphic properties are of great importance in reducing the complexity of fault models, since they imply that the analysis of a model's diagnosability and the development of diagnostic algorithms can be based solely on the knowledge of the elementary fault syndromes. The presence of a morphic property also reduces the complexity of determining and storing the AFSS table by several orders of magnitude. One should note that the existing graphical fault models [BAR76, HOL79, PRE67, RUS75a, SOG64] have reduced their complexity in exactly this way; the graph is actually a description of the elementary fault situation and syndrome association. Moreover, the complexity of determining the existence of diagnosability properties and deriving diagnostic algorithms is also reduced in these models. Evidence for this is found in the existence of system-level diagnostic algorithms [COR76, KAM75, MEY78, MEY79, MEY81, SMI79] that correspond only to models with morphic properties.

3.1 WEAKLY MORPHIC PROPERTY

The morphic properties we are considering occur when an associative and commutative binary operation between internal test outcomes exists, called a *morphic map.*

Definition 3.1.1: A *morphic map* is an associative and commutative binary operation $*$ on the set Z of internal test outcomes.

Let $a = (a_1, a_2, \ldots, a_p)$ and $b = (b_1, b_2, \ldots, b_p)$ be syndromes in Z^p; then $a*b$ is the syndrome defined by

$$a*b = (a_1*b_1, a_2*b_2, \ldots, a_p*b_p).$$

Let Q and R be subsets of syndromes in Z^p; then $Q*R$ is the subset of syndromes defined by

$$Q*R = \{ a*b \mid (a,b) \in Q \times R \}.$$

When all fault situations are admissible and all multiple fault syndromes can be calculated from the elementary fault syndromes using a morphic map, the model is said to be *weakly morphic.*

Definition 3.1.2: A fault model S is *weakly morphic* with respect to the morphic map $*$ if and only if

(i) $A = A_n$ and

(ii) for every F in A, such that $\|F\| > 1$,

$$G(F) = G(f_{i_1}) * G(f_{i_2}) * \ldots * G(f_{i_{|F|}})$$

where $f_{i_j} \in F$, $1 \leq j \leq \|F\|$ and $\bigcup_{j=1}^{|F|} f_{i_j} = F$.

Fault models that are not weakly morphic may possess a *weakly morphic approximation* from which diagnosability properties can be implied.

Definition 3.1.3: The fault model $S_* = (A_n, Z^p, Y^p, G_*(.), H(.))$ is the *weakly morphic approximation* of a fault model $S = (A, Z^p, Y^p, G(.), H(.))$ with respect to the morphic map $*$ if and only if (i) S_* is weakly morphic with respect to $*$, and (ii) $G(F) \subseteq G_*(F)$ for every F in A.

3.2 DETECTABLE SUBSETS

Our purpose is to determine those conditions of the fault model that ensure good diagnosability properties. By considering the class of weakly morphic fault models, we can reduce this task to that of finding those conditions of elementary fault syndromes and morphic maps that ensure diagnosability. It is particularly interesting to examine the consequences of assuming that the test outcome "0" functions as the identity element of the set Z with respect to the morphic map.

Definition 3.2.1: A fault model S satisfies the *Irredundancy Hypothesis* if and only if S is weakly morphic with respect to a morphic map $*$ such that $0 * a = a$ for every a in Z.

As a consequence of this hypothesis, not only do the diagnosability conditions of the fault model depend only on the elementary fault syndromes, but only on the nonzero outcomes of these syndromes. This is a characteristic of systems that are not redundant. In such systems, the presence of an elementary fault situation that always causes a certain test to have a "0" test outcome can never be detected by that test, even if combined with other fault situations. The Irredundancy Hypothesis thus represents a strong assumption on the nature of the fault model. One should note, however, that all system-level fault models referred to in this paper have representations satisfying this hypothesis.

The Irredundancy Hypothesis leads to an important concept related to diagnosability conditions for these models. This concept is that the syndromes of a fault situation can be divided into portions,--ie., subsets of tests,--such that the test outcomes in a given portion depend only on a subset of elementary faults in the fault situation. There is thus a "decoupling" between some elementary faults and some test outcomes that permits diagnosability conditions to be simplified. When the test outcomes in one portion of the syndromes ensure that all the syndromes of a given fault situation are nonzero, then the subset of elementary faults associated with that portion of the syndrome is called a *detectable subset* of the fault situation. We will show that a great deal of information--and in some cases, all information--about the diagnosability of a fault model can be ascertained by examining only detectable subsets.

Definition 3.2.2: Let S be a fault model and let F be an admissible fault situation. A set B of elementary faults is a *detectable subset* of F if and only if

(i) $B \neq \phi$

(ii) $B \subseteq F$

(iii) for every $a \in H(G(F))$ an index k exists, such that $1 \leqslant k \leqslant p$, where $a_k \neq 0$ and $G(f)_k = 0$ for every $f \in F - B$

(iv) the only subset of B satisfying (i), (ii) and (iii) is B itself.

The family of all detectable subsets associated with a fault situation characterizes the detectability of the fault situation. It is therefore convenient to introduce the concept of a *detectability map.*

Definition 3.2.3: The *detectability map* $\Lambda(.)$ of a fault model S is the point-to-set map from A to A_n defined for every F in A by

$$\Lambda(F) = \{ B \in A_n \mid B \text{ is a detectable subset of } F \}.$$

The term "detectable" in these definitions is appropriate since one can easily show that a fault situation F is always distinguishable from the nonfaulty situation if and only if $\Lambda(F) \neq \phi$. Thus, a necessary condition for a fault model to be one-step τ-fault diagnosable is that $\Lambda(F) \neq \phi$ for all F in $A \cap A_\tau$.

The importance of defining detectable subsets is that sufficient conditions for one-step τ-fault diagnosability for models satisfying the Irredundancy Hypothesis have been determined based on these subsets. Given in the following sections, these conditions make use of the fact that if B is a detectable subset of a fault situation F, then B is also a detectable subset of every fault situation $\hat{F}$ where $B \subseteq \hat{F} \subseteq F$. This fact justifies condition (iv) of Definition 3.2.2, in which only the smallest subsets satisfying conditions (i), (ii) and (iii) are included. One should also note that for a model satisfying the Irredundancy Hypothesis, if F is a fault situation and $B \in \Lambda(F)$, then a test k exists such that

$$G(F)_k - G(B)_k * G(F-B)_k - G(B)_k.$$

From the preceding comments, one would expect that determining the syndromes in $G(F)$ and deriving diagnosability conditions is easier when $\|B\| \ll \|F\|$, because this implies the maximum amount of "decoupling" between faults and test outcomes. It is therefore not surprising that fault models exist in which all detectable subsets consist of exactly one elementary fault situation [PRE67, RUS75a]. Such cases demonstrate that diagnosability conditions have been greatly simplified.

4. SUFFICIENT CONDITIONS FOR ONE-STEP τ-FAULT DIAGNOSABILITY

The model and properties defined in the preceding sections can be used to derive new conditions for one-step τ-fault diagnosability. In this section, sufficient conditions are derived for models satisfying the Irredundancy Hypothesis. Since all known system-level fault models have representations satisfying this hypothesis, these conditions have a wide application. As an example, the conditions are applied to the fault model of Preparata, Metze and Chien [PRE67] and, in particular, diagnosability conditions based on the Irredundancy Hypothesis are compared to those derived by Hakimi and Amin [HAK74]. (The proofs of theorems and lemmas in this section can be found in Section 6 of this paper.)

4.1 DIAGNOSABILITY THEOREMS

In the following results, we demonstrate that the Irredundancy Hypothesis relates conditions involving detectable subsets with one-step τ-fault diagnosability. We provide the basic conditions on the detectability map $\Lambda(.)$ that ensure one-step τ-fault diagnosability in Lemma 4.1.1. These conditions can be simplified using Lemma 4.1.2, and this result is given in Theorem 4.1.3. A special case of the map $\Lambda(.)$ that applies to existing fault models [PRE67, RUS75a] is given in Definition 4.1.4 and the resulting diagnosability conditions are given in Theorem 4.1.5.

The definition of one-step τ-fault diagnosability involves comparing the syndromes for each pair of fault situations in the set $P_1(\tau)$, where

$$P_1(\tau) = \{ \{F_a, F_b\} \mid F_a, F_b \in A_\tau,\ F_a \neq F_b \}$$

for every τ such that $1 \leqslant \tau \leqslant n$. The following lemma uses the pairs of fault

situations in $P_1(\tau)$ to relate conditions on the map $\Lambda(.)$ with one-step τ-fault diagnosability.

Lemma 4.1.1: Let S satisfy the Irredundancy Hypothesis and let τ be such that $1 \leqslant \tau \leqslant n$. If to every pair $\{F_a, F_b\}$ in $P_1(\tau)$ there corresponds a set B in $\Lambda(F_a \cup F_b)$ such that either $B \cap F_a = \phi$ or $B \cap F_b = \phi$, then S is one-step τ-fault diagnosable.

Instead of using the set $P_1(\tau)$, one may use a smaller set $P_2(\tau)$ where

$$P_2(\tau) = \{ \{F_a, F_b\} \mid F_a, F_b \in A_\tau, \|F_a \cup F_b\| \geqslant \tau, \|F_a \cap F_b\| = \min(\|F_a \cup F_b\| - 1, 2\tau - \|F_a \cup F_b\|) \}$$

for every τ such that $1 \leqslant \tau \leqslant n$.

Clearly, $P_2(\tau)$ is always a subset of $P_1(\tau)$. If, for example, $n = 5$, then $\|P_2(1)\| = \|P_1(1)\| = 15$; however, $\|P_2(2)\| = 65$ is less than $\|P_1(2)\| = 120$ and $\|P_2(3)\| = 75$ is less than $\|P_1(3)\| = 325$. The following lemma shows that the conditions of Lemma 4.1.1 can be verified by examining only pairs of fault situations in $P_2(\tau)$.

Lemma 4.1.2: If to every pair $\{\hat{F}_a, \hat{F}_b\}$ in $P_2(\tau)$ there corresponds a set $\hat{B}$ in $\Lambda(\hat{F}_a \cup \hat{F}_b)$ such that either $\hat{B} \cap \hat{F}_a = \phi$ or $\hat{B} \cap \hat{F}_b = \phi$, then to every pair $\{F_a, F_b\}$ in $P_1(\tau)$ there corresponds a set B in $\Lambda(F_a \cup F_b)$ such that either $B \cap F_a = \phi$ or $B \cap F_b = \phi$.

Lemmas 4.1.1 and 4.1.2 immediately imply the following theorem.

Theorem 4.1.3: Let S satisfy the Irredundancy Hypothesis and let τ be such that $1 \leqslant \tau \leqslant n$. If to every pair $\{F_a, F_b\}$ in $P_2(\tau)$ there corresponds a set B in $\Lambda(F_a \cup F_b)$ such that either $B \cap F_a = \phi$ or $B \cap F_b = \phi$, then S is one-step τ-fault diagnosable.

It is interesting to examine the consequences of assuming that all detectable subsets in $\Lambda(F)$ contain one and only one elementary fault situation.

Definition 4.1.4: A map $\Lambda(.)A \rightarrow A_n$ satisfies the *Cardinality Condition* if and only if $\|B\|=1$ for every $B \in \Lambda(F)$ and every $F \in A$.

As a consequence of $\Lambda(.)$ satisfying the Cardinality Condition, the conditions ensuring one-step τ-fault diagnosability reduce to that of considering only the cardinality of $\Lambda(F)$.

Theorem 4.1.5: Let S satisfy the Irredundancy Hypothesis, let $\Lambda(.)$ satisfy the Cardinality Condition and let τ be such that $1 \leqslant \tau \leqslant n$. If

$$\|\Lambda(F)\| > \min(\|F\|-1, 2\tau-\|F\|)$$

for every $F \in A_n$ such that $\tau \leqslant \|F\| \leqslant 2\tau$; then S is one-step τ-fault diagnosable.

4.2 APPLICATION TO THE PMC FAULT MODEL

In this section, we will consider the following representation of the Preparata, Metze and Chien (PMC) [PRE67] model based on the graphical description given in [HAK74].

Definition 4.2.1: Let $G(V,C)$ be the graphical description of a PMC fault model. $S = (A_n, \{0,1,2\}^p, \{0,1\}^p, G(.), H(.))$ is a *type 1* representation of this PMC model if and only if

(i) $n = \|V\|$

(ii) $p = \|C\|$

(iii) for every $(v_i,v_j) \in C$, $1 \leqslant k \leqslant p$ exists such that for every $F \in A_n$

$$G(F)_k = \begin{cases} 2, & f_i \in F \\ 1, & f_i \notin F,\ f_j \in F, \\ 0, & \text{otherwise} \end{cases}$$

(iv) $H(0)=0$, $H(1)=1$ and $H(2)=\{0,1\}$.

This representation of a PMC fault model implies a one-to-one correspondence between units (vertices) in V and elementary fault situations in E, and between edges in C and tests in T. This representation is meaningful since a subset of faulty units in V corresponds to every $F \in A_n$, and $H(G(F))$ is equal to the syndromes for this set of faulty units. The following lemmas show that a type 1 representation of a PMC model satisfies the Irredundancy Hypothesis and $\Lambda(.)$ satisfies the Cardinality Condition.

Lemma 4.2.2: If S is a type 1 representation of a PMC fault model, then S is weakly morphic with respect to a morphic map $*$, where $0*0=0$, $0*1=1*0=1$ and $0*2=1*2=2*0=2*1=2$. (The values $1*1$ and $2*2$ are not used in this representation.)

Corollary 4.2.3: If S is a type 1 representation of a PMC fault model, then S satisfies the Irredundancy Hypothesis.

Lemma 4.2.4: If S is a type 1 representation of a PMC fault model, then for every $F \in A_n$,

$$\Lambda(F) = \{ f \in F \mid 1 \leq k \leq p \text{ exists where } G(f)_k = 1 \text{ and } G(\hat{f})_k = 0, \text{ for all } \hat{f} \in F - \{f\} \}.$$

Corollary 4.2.5: If S is a type 1 representation of a PMC fault model, then $\Lambda(.)$ satisfies the Cardinality Condition.

The preceding corollaries and Theorem 4.1.5 immediately imply the following theorem.

Theorem 4.2.6: Let S be a type 1 representation of a PMC fault model, and let τ be such that $1 \leq \tau \leq n$. If

$$\|\Lambda(F)\| > \min(\|F\|-1, 2\tau-\|F\|)$$

for every $F \in A_n$ such that $\tau \leqslant \|F\| \leqslant 2\tau$, then S is one-step τ-fault diagnosable.

Using Theorem 4.2.6, one can reconstruct the diagnosability conditions derived by Hakimi and Amin [HAK74] and show that condition 1 of Theorem 2 [HAK74], that is, $n > 2\tau$, is actually implied by the other conditions of that theorem.

Lemma 4.2.7: Let S be a type 1 representation of a PMC fault model, and let τ be such that $1 \leqslant \tau \leqslant n$. Every unit in the PMC model is tested by τ others (condition 2 [HAK74]) if and only if $\|\Lambda(F)\| \geq \tau$ for every $F \in A_n$, $\|F\| \geq \tau$.

Lemma 4.2.8: Let S be a type 1 representation of a PMC fault model, and let τ be such that $1 \leqslant \tau \leqslant n$. For every r such that $0 \leqslant r < \tau$, and every $X \subset V$ such that $\|X\| = n-2\tau+r$, $\|\Gamma X\| > r$ (condition 3 [HAK74]) if and only if $\|\Lambda(F)\| > 2\tau-\|F\|$ for every $F \in A_n$, $\tau < \|F\| \leqslant 2\tau$.

Theorem 4.1.5 and Lemmas 4.2.7 and 4.2.8 immediately imply the following theorem and show that conditions 2 and 3 [HAK74, Theorem 2] alone are sufficient for one-step τ-fault diagnosability.

Theorem 4.2.9: Let S be a type 1 representation of a PMC fault model, and let τ be such that $1 \leqslant \tau \leqslant n$. If every unit in the PMC model is tested by τ others (condition 2 [HAK74]), and for every r such that $0 \leqslant r < \tau$, and every $X \subset V$ such that $\|X\| = n-2\tau+r$, $\|\Gamma X\| > r$ (condition 3 [HAK74]), then S is one-step τ-fault diagnosable.

The following lemma shows that $n > 2\tau$ (condition 1 [HAK74]) is implied by the conditions of Theorem 4.2.6.

Lemma 4.2.10: Let S be a type 1 representation of a PMC fault model, and let τ be such that $1 \leqslant \tau \leqslant n$. If

$$\|\Lambda(F)\| > \min(\|F\|-1, 2\tau-\|F\|)$$

for every $F \in A_n$ such that $\tau \leqslant \|F\| \leqslant 2\tau$, then $n > 2\tau$.

In the special case of the PMC fault model in which no two units test each other, the diagnosability conditions of Theorem 4.2.6 can be further simplified.

Lemma 4.2.11: Let S be a type 1 representation of a PMC fault model in which no two units test each other, and let τ be such that $1 \leqslant \tau \leqslant n$, then

$$\|\Lambda(F)\| > \min(\|F\|-1, 2\tau-\|F\|)$$

for every $F \in A_n$ such that $\tau \leqslant \|F\| \leqslant 2\tau$ if and only if $\|\Lambda(F)\| = \tau$ for every $F \in A_n$ such that $\|F\| = \tau$.

Theorem 4.2.6 and Lemmas 4.2.7 and 4.2.11 immediately imply the following theorem, which is equivalent to Theorem 1 of [HAK74].

Theorem 4.2.12: Let S be a type 1 representation of a PMC fault model in which no two units test each other, and let τ be such that $1 \leqslant \tau \leqslant n$. If every unit is tested by τ other units, then S is one-step τ-fault diagnosable.

5. CONCLUSION

Our research presents a new approach for determining diagnosability conditions by using a new fault model having flexible features. We have shown that without initially assuming conditions on the fault-test relationship, diagnostic conditions can be determined that have a wide application and which should lead to new testability design guidelines.

The results given in this paper were limited to sufficient conditions for one-step τ-fault diagnosability. It can be shown, however, that the approach is applicable to other types of diagnosability properties and leads to necessary conditions as well. We are currently engaged in research efforts to extend this approach to transient fault situations.

6. PROOFS

This section contains the proofs of theorems and lemmas in Sections 4.1 and 4.2. Lemmas 6.1 and 7.3 are used to simplify these proofs.

Lemma 6.1: Let S be a fault model and let $F \in A$, then (i) for every $b \in G(F)$ an index k exists such that $1 \leqslant k \leqslant p$, where $0 \notin H(b_k)$ if and only if
(ii) for every $a \in H(G(F))$ an index k exists such that $1 \leqslant k \leqslant p$, where $a_k \neq 0$.

PROOF: (i)→(ii). Let $a \in H(G(F))$. This implies that $b \in G(F)$ exists such that $a \in H(b)$. Therefore, by (i), an index k exists such that $1 \leqslant k \leqslant p$, where $0 \notin H(b_k)$, which implies $a_k \neq 0$.

(ii)→(i). Let $b \in G(F)$. Since $H(b) \subseteq H(G(F))$, by (ii), for every $a \in H(b)$ an index j exists such that $1 \leqslant j \leqslant p$, where $a_j \neq 0$. Therefore, $a \neq (0, \ldots, 0)$ for every $a \in H(b)$. Then, since $H(b) = H(b_1) \times H(b_2) \times \ldots \times H(b_p)$, this implies that an index k exists such that $1 \leqslant k \leqslant p$, where $0 \notin H(b_k)$. □

Lemma 6.1 and Definition 3.2.2 immediately imply an alternative definition for detectable subsets. This definition is used in the proofs of Lemmas 6.3, 4.1.1 and 4.2.4.

Corollary 6.2: Let S be a fault model and let F be an admissible fault situation. A set B of elementary faults is a *detectable subset* of F if and only if
(i) $B \neq \phi$
(ii) $B \subseteq F$
(iii) for every $b \in G(F)$ an index k exists such that $1 \leqslant k \leqslant p$, where $0 \notin H(b_k)$ and $G(f)_k = 0$ for every $f \in F - B$
(iv) the only subset of B satisfying (i), (ii) and (iii) is B itself.

The following lemma verifies a statement made at the end of Section 3.2 and is

used in the proof of Lemma 4.1.2.

Lemma 6.3: Let S satisfy the Irredundancy Hypothesis, let $F \in A$ such that $\Lambda(F) \neq \phi$, and let $B \in \Lambda(F)$. If $\hat{F} \in A$ such that $B \subseteq \hat{F} \subseteq F$, then $B \in \Lambda(\hat{F})$.

PROOF: If $\hat{F} = F$, then immediately, $\Lambda(F) = \Lambda(\hat{F})$. Assume that $\hat{F} \subset F$. Let $a \in G(\hat{F})$. By the weakly morphic property, $a * G(F - \hat{F}) \subseteq G(F)$. Let $b \in a * G(F - \hat{F})$. This implies that $b \in G(F)$. Since $B \in \Lambda(F)$, by Corollary 6.2 an index k exists such that $1 \leq k \leq p$, where $0 \notin H(b_k)$ and $G(f)_k = 0$ for all $f \in F - B$. Since $F - \hat{F} \subseteq F - B$, $G(F - \hat{F})_k = 0$ and, by the Irredundancy Hypothesis, $b_k = a_k * 0 = a_k$. Then, since $\hat{F} - B \subseteq F - B$, an index k exists such that $1 \leq k \leq p$, where $0 \notin H(a_k)$ and $G(f)_k = 0$ for every $f \in \hat{F} - B$. Hence, $B \in \Lambda(\hat{F})$. □

The remainder of this section consists of the proofs of theorems and lemmas in Sections 4.1 and 4.2.

Lemma 4.1.1: Let S satisfy the Irredundancy Hypothesis and let τ be such that $1 \leq \tau \leq n$. If to every pair $\{F_a, F_b\}$ in $P_1(\tau)$ there corresponds a set B in $\Lambda(F_a \cup F_b)$ such that either $B \cap F_a = \phi$ or $B \cap F_b = \phi$, then S is one-step τ-fault diagnosable.

PROOF: Let $\{F_a, F_b\} \in P_1(\tau)$ and assume without loss of generality that $F_a \neq F_0$ and that $B \in \Lambda(F_a \cup F_b)$ exists such that $B \cap F_b = \phi$. Hence, $B \subseteq F_a \subseteq F_a \cup F_b$. Let $a \in G(F_a)$.

Case (1): $F_a = F_a \cup F_b$. In this case, $\Lambda(F_a) = \Lambda(F_a \cup F_b)$, and by Corollary 6.2, an index k exists such that $1 \leq k \leq p$, where $0 \notin H(a_k)$ and $G(f)_k = 0$ for every $f \in F_a - B$. Then, since $F_b \subseteq F_a - B$, by the Irredundancy Hypothesis $G(F_b)_k = 0$.

Case (2): $F_a \subset F_a \cup F_b$. In this case, by the weakly morphic property, $a * G(\{F_a \cup F_b\} - F_a) \subseteq G(F_a \cup F_b)$. Let $b \in a * G(\{F_a \cup F_b\} - F_a)$; then $b \in G(F_a \cup F_b)$. Since $B \in \Lambda(F_a \cup F_b)$, by Corollary 6.2 an index k exists such that $1 \leqslant k \leqslant p$, where $0 \notin H(b_k)$ and $G(f)_k = 0$ for every $f \in \{F_a \cup F_b\} - B$. Then, by the Irredundancy Hypothesis, $F_b \subseteq \{F_a \cup F_b\} - B$ implies $G(F_b)_k = 0$ and $\{F_a \cup F_b\} - F_a \subseteq \{F_a \cup F_b\} - B$ implies $G(\{F_a \cup F_b\} - F_a)_k = 0$. Therefore, $b_k = a_k$, which implies $0 \notin H(a_k)$.

Hence, in both cases (1) and (2) an index k exists such that $1 \leqslant k \leqslant p$, where $H(a_k) \cap H(G(F_b)_k) = \phi$, which implies $H(a) \cap H(G(F_b)) = \phi$. Accordingly, since $a \in G(F_a)$ is arbitrary, $H(G(F_a)) \cap H(G(F_b)) = \phi$. Since this is true for any pair in $P_1(\tau)$, S is one-step τ-fault diagnosable. □

Lemma 4.1.2: If to every pair $\{\hat{F}_a, \hat{F}_b\}$ in $P_2(\tau)$ there corresponds a set $\hat{B}$ in $\Lambda(\hat{F}_a \cup \hat{F}_b)$ such that either $\hat{B} \cap \hat{F}_a = \phi$ or $\hat{B} \cap \hat{F}_b = \phi$, then to every pair $\{F_a, F_b\}$ in $P_1(\tau)$ there corresponds a set B in $\Lambda(F_a \cup F_b)$ such that either $B \cap F_a = \phi$ or $B \cap F_b = \phi$.

PROOF: We shall prove the contrapositive of this lemma; that is, we will assume that there $\{F_a, F_b\} \in P_1(\tau)$ exists such that for every $B \in \Lambda(F_a \cup F_b)$, $B \cap F_a \neq \phi$ *and* $B \cap F_b \neq \phi$, and then construct $\{\hat{F}_a, \hat{F}_b\} \in P_2(\tau)$ such that for every $\hat{B} \in \Lambda(\hat{F}_a \cup \hat{F}_b)$, $\hat{B} \cap \hat{F}_a \neq \phi$ *and* $\hat{B} \cap \hat{F}_b \neq \phi$.

Case (1): $\| F_a \cup F_b \| \leqslant \tau$. Without loss of generality, let $f_a \in F_a$ such that $f_a \notin F_b$. Let $V = F_a \cup F_b$ and $W = V - \{f_a\}$. Since $\tau \leqslant n$, $X \subseteq E - F_a \cup F_b$ exists such that $\| X \| = \tau - \| F_a \cup F_b \|$. Let $\hat{F}_a = X \cup V$ and $\hat{F}_b = X \cup W$; then $\{\hat{F}_a, \hat{F}_b\} \in P_2(\tau)$ and $F_a \cup F_b \subseteq \hat{F}_a \cup \hat{F}_b$. By assumption, $\{f_a\} \notin \Lambda(F_a \cup F_b)$. Therefore, by Lemma 6.3, $\{f_a\} \notin \Lambda(\hat{F}_a \cup \hat{F}_b)$. Consequently, since

$\{f_a\}-\hat{F}_a \cup \hat{F}_b - \hat{F}_a \cap \hat{F}_b$, for every $\hat{B} \in \Lambda(\hat{F}_a \cup \hat{F}_b)$, $\hat{B} \cap (\hat{F}_a \cap \hat{F}_b) \neq \phi$. This implies that $\hat{B} \cap \hat{F}_a \neq \phi$ and $\hat{B} \cap \hat{F}_b \neq \phi$.

Case (2): $\|F_a \cup F_b\| > \tau$. In this case, $\|\{F_a \cup F_b\} - F_a\| > \tau - \|F_a\| \geq 0$; thus, $V \subseteq \{F_a \cup F_b\} - F_a$ exists such that $\|V\| = \tau - \|F_a\|$. Let $\hat{F}_a = V \cup F_a$. Similarly, $W \subseteq \{F_a \cup F_b\} - F_b$ exists such that $\|W\| = \tau - \|F_b\|$. Let $\hat{F}_b = W \cup F_b$. Consequently, $\{\hat{F}_a, \hat{F}_b\} \in P_2(\tau)$ and $F_a \cup F_b = \hat{F}_a \cup \hat{F}_b$. Hence, $\Lambda(F_a \cup F_b) = \Lambda(\hat{F}_a \cup \hat{F}_b)$. Therefore, if $\hat{B} \in \Lambda(\hat{F}_a \cup \hat{F}_b)$ exists, then $\hat{B} \in \Lambda(F_a \cup F_b)$. By assumption, then, $\hat{B} \cap F_a \neq \phi$, which implies $\hat{B} \cap \hat{F}_a \neq \phi$ and $\hat{B} \cap F_b \neq \phi$, which implies $\hat{B} \cap \hat{F}_b \neq \phi$. □

Theorem 4.1.5: Let S satisfy the Irredundancy Hypothesis, let $\Lambda(.)$ satisfy the Cardinality Condition and let τ be such that $1 \leq \tau \leq n$. If

$$\|\Lambda(F)\| > \min(\|F\| - 1, 2\tau - \|F\|)$$

for every $F \in A_n$ such that $\tau \leq \|F\| \leq 2\tau$, then S is one-step τ-fault diagnosable.

PROOF: Assume that $\|\Lambda(F)\| > \min(\|F\| - 1, 2\tau - \|F\|)$ for every $F \in A_n$ such that $\tau \leq \|F\| \leq 2\tau$. Let $\{F_a, F_b\} \in P_2(\tau)$; then $\tau \leq \|F_a \cup F_b\| \leq 2\tau$ and $\|F_b \cup F_b\| = \min(\|F_a \cup F_b\| - 1, 2\tau - \|F_a \cup F_b\|)$. Let $V = \bigcup_{B \in \Lambda(F_a \cup F_b)} B$. Then $\|B\| = 1$ for all $B \in \Lambda(F_a \cup F_b)$ and $\|\Lambda(F_a \cup F_b)\| > \min(\|F_a \cup F_b\| - 1, 2\tau - \|F_a \cup F_b\|)$ imply that $\|V\| > \min(\|F_a \cup F_b\| - 1, 2\tau - \|F_a \cup F_b\|) - \|F_a \cap F_b\|$. Hence, $f \in V$ exists such that $f \notin F_a \cap F_b$. Since $f \in V$ if and only if $\{f\} \in \Lambda(F_a \cup F_b)$, this implies $\{f\} \in \Lambda(F_a \cup F_b)$ exists such that either $\{f\} \cap F_a = \phi$ or $\{f\} \cap F_b = \phi$. Therefore, by Theorem 4.1.3, S is one-step τ-fault diagnosable. □

Lemma 4.2.2: If S is a type 1 representation of a PMC fault model, then S is

weakly morphic with respect to a morphic map $*$, where $0*0=0$, $0*1=1*0=1$ and $0*2=1*2=2*0=2*1=2$. (The values $1*1$ and $2*2$ are not used in this representation.)

PROOF: Definition 4.2.1 satisfies Definition 3.1.2(i). Let $F \in A$ such that $|F|>1$ and let $1 \leqslant k \leqslant p$. Definition 4.2.1(iii) implies that f_i, $f_j \in E$ exist such that for every $f \in E$,

$$G(f)_k = \begin{cases} 2, & f=f_i \\ 1, & f=f_j \\ 0, & \text{otherwise} \end{cases} .$$

Let $*$ be the morphic map given in this lemma and let

$$G_*(F) = G(f_{i_1}) * G(f_{i_2}) * \ldots * G(f_{i_{|F|}}),$$

where $f_{i_j} \in F$, $1 \leqslant j \leqslant |F|$ and $\bigcup_{j=1}^{|F|} f_{i_j} = F$. Then, $G_*(F)_k=2$ if and only if $f_i \in F$, $G_*(F)_k=1$ if and only if $f_i \notin F$, $f_j \in F$ and $G_*(F)_k=0$ if and only if $f_i \notin F$, $f_j \notin F$. Thus, $G_*(F) = G(F)$ for every $F \in A$. Hence, Definition 4.2.1 satisfies Definition 3.1.2(ii) and therefore, S is weakly morphic with respect to $*$. □

Lemma 4.2.4: If S is a type 1 representation of a PMC fault model, then for every $F \in A_n$

$$\Lambda(F) = \{ f \in F \mid 1 \leqslant k \leqslant p \text{ exists where } G(f)_k=1 \text{ and } G(\hat{f})_k=0, \text{ for all } \hat{f} \in F-\{f\} \}.$$

PROOF: Let $F \in A_n$ and let

$$Q(F) = \{ f \in F \mid 1 \leqslant k \leqslant p \text{ exists where } G(f)_k = 1 \text{ and } G(\hat{f})_k = 0, \text{ for all } \hat{f} \in F - \{f\} \}.$$

Let $\Lambda(F)$ be defined according to Definition 3.2.2.

Case (1): $\Lambda(F) = \phi$. Definition 3.2.2(iii) implies that $a \in H(G(F))$ exists such that $a = (0,0,\ldots,0)$. Definition 4.2.1(iv) implies that $G(F)_k \neq 1$ for every index k such that $1 \leqslant k \leqslant p$. Therefore, by Definition 4.2.1(iii), for each index k either $G(f)_k = 0$ for every $f \in F$ or $f_{i_k} \in F$ exists such that $G(f_{i_k})_k = 2$. Hence, $Q(F) = \phi$, and consequently, $\Lambda(F) = Q(F) = \phi$.

Case (2): $\Lambda(F) \neq \phi$. Let $B \in \Lambda(F)$. Let $a = G(F)$; then by Corollary 6.2, an index k exists such that $1 \leqslant k \leqslant p$, where $0 \notin H(a_k)$ and $G(\hat{f})_k = 0$ for every $\hat{f} \in F - B$. Definition 4.2.1(iv) implies that $a_k = 1$. Definition 4.2.1(iii) implies that $f_i \in F$ exists such that $G(f_i)_k = 1$ and $G(\hat{f})_k = 0$ for every $\hat{f} \in F - \{f_i\}$. Therefore, by Definition 3.2.2(iv), $B = \{f_i\}$ and $B \in Q(F)$. Hence, $\Lambda(F) \subseteq Q(F)$.

Let $\{f_i\} \in Q(F)$, then $f_i \in F$, and an index k exists such that $1 \leqslant k \leqslant p$, where $G(f_i)_k = 1$ and $G(\hat{f})_k = 0$ for every $\hat{f} \in F - \{f_i\}$. Definition 4.2.1(iv) implies that for every $a \in H(G(F))$, $a_k \neq 0$ and $G(\hat{f})_k = 0$ for every $\hat{f} \in F - \{f_i\}$. Hence, $\{f_i\} \in \Lambda(F)$, and thus, $Q(F) \subseteq \Lambda(F)$. Therefore, $\Lambda(F) = Q(F)$. □

Lemma 4.2.7: Let S be a type 1 representation of a PMC fault model, and let τ be such that $1 \leqslant \tau \leqslant n$. Every unit in the PMC model is tested by τ others (condition 2 [HAK74]) if and only if $\| \Lambda(F) \| = \tau$ for every $F \in A_n$, $\| F \| = \tau$.

PROOF: Let $f_j \in E$ and define $T(f_j) = \{f_i \in E \mid (v_i, v_j) \in C, i \neq j\}$. Then, each unit in the PMC model that tests unit v_j corresponds to a elementary fault in $T(f_j)$.

First, assume every unit in the PMC model is tested by at least τ others. Then, for every $f \in E$, $|T(f)| \geq \tau$. Let $F \in A_n$ such that $|F| = \tau$, and let $f_j \in F$. Since $f_j \notin T(f_j)$ and $|T(f_j)| \geq \tau$, $f_i \in T(f_j)$ exists such that $f_i \notin F$. Therefore, by Definition 4.2.1(iii) an index k exists such that $1 \leq k \leq p$, where $G(f_i)_k = 2$ and $G(f_j)_k = 1$. Hence, $f_j \in \Lambda(F)$. Since this is true for any $f \in F$, $\Lambda(F) = F$ and therefore, $|\Lambda(F)| = |F| = \tau$.

Second, assume that a unit in the PMC model exists that is tested by fewer than τ others. Then $f_j \in E$ exists such that $|T(f_j)| < \tau$. Let $W \subseteq E - \{f_j\} \cup T(f_j)$ such that $|W| = \tau - 1 - |T(f_j)|$. Let $F = \{f_j\} \cup T(f_j) \cup W$; then, $|F| = \tau$. By definition 4.2.1(iii), for every index k such that $1 \leq k \leq p$ and $G(f_j)_k = 1$, $f_i \in T(f_j)$ exists such that $G(f_i)_k = 2$. Thus, $f_i \in F$ implies that $f_j \notin \Lambda(F)$. Hence, $|\Lambda(F)| < |F| = \tau$. □

Lemma 4.2.8: Let S be a type 1 representation of a PMC fault model, and let τ be such that $1 \leq \tau \leq n$. For every r such that $0 \leq r < \tau$ and every $X \subset V$ such that $|X| = n - 2\tau + r$, $|\Gamma X| > r$ (condition 3 [HAK74]) if and only if $|\Lambda(F)| > 2\tau - |F|$ for every $F \in A_n$, $\tau < |F| \leq 2\tau$.

PROOF: Let $X \subseteq V$. Then let $F \in A_n$ be defined such that $f_i \in F$ if and only if $v_i \notin X$. Then F is the set of elementary faults corresponding to the vertices in the complement of X. By definition [HAK74], $\Gamma X = \{v_j \notin X \mid (v_i, v_j) \in C, v_i \in X\}$. By Definition 4.2.1(iii), $(v_i, v_j) \in C$ if and only if an index k exists such that $1 \leq k \leq p$, where $G(f_i)_k = 2$ and $G(f_j)_k = 1$. Hence, $v_j \in \Gamma X$ if and only if $f_j \in \Lambda(F)$. Therefore, $|\Gamma X| = |\Lambda(F)|$.

First, assume for every r such that $0 \leq r < \tau$, and for every $X \subseteq V$ such that $|X| = n - 2\tau + r$, that $|\Gamma X| > r$. Let $F \in A_n$ such that $\tau < |F| \leq 2\tau$. Let $r = 2\tau - |F|$; then $0 \leq r < \tau$ and $|X| = n - |F| = n - 2\tau + r$.

Then, $|\Lambda(F)|-|\Gamma X|>r-2\tau-|F|$.

Second, assume that $|\Lambda(F)|>2\tau-|F|$ for every $F\in A_n$ such that $\tau<|F|\leqslant 2\tau$. Let $X\subseteq V$ and let $0\leqslant r<\tau$ such that $|X|=n-2\tau+r$. Then, $|F|=n-|X|=2\tau-r$ and $\tau<|F|\leqslant 2\tau$. Hence, $|\Gamma X|-|\Lambda(F)|>2\tau-|F|-r$. □

Lemma 4.2.10: Let S be a type 1 representation of a PMC fault model, and let τ be such that $1\leqslant\tau\leqslant n$. If

$$|\Lambda(F)| > \min(|F|-1, 2\tau-|F|)$$

for every $F\in A_n$ such that $\tau\leqslant|F|\leqslant 2\tau$, then $n>2\tau$.

PROOF: Note that for a type 1 representation of a PMC model, $|\Lambda(E)|=0$. Assume that $|\Lambda(F)|>\min(|F|-1, 2\tau-|F|)$ for every $F\in A_n$ such that $\tau\leqslant|F|\leqslant 2\tau$, and assume that n is such that $\tau\leqslant n\leqslant 2\tau$.

If $n=\tau$, then $|\Lambda(E)|=0\leqslant\min(n-1, 2n-n)=n-1$ is a contradiction. If $\tau<n\leqslant 2\tau$, then $|\Lambda(E)|=0\leqslant\min(n-1, 2\tau-n)=2\tau-n$ is a contradiction. Therefore, $n>2\tau$. □

Lemma 4.2.11: Let S be a type 1 representation of a PMC fault model in which no two units test each other, and let τ be such that $1\leqslant\tau\leqslant n$, then,

$$|\Lambda(F)| > \min(|F|-1, 2\tau-|F|)$$

for every $F\in A_n$ such that $\tau\leqslant|F|\leqslant 2\tau$ if and only if $|\Lambda(F)|=\tau$ for every $F\in A_n$ such that $|F|=\tau$.

PROOF: Assumption (1): $|\Lambda(F)|=\tau$ for every $F\in A_n$ such that $|F|=\tau$. Assumption (2): $F_a\in A_n$ exists such that $\tau<|F_a|\leqslant 2\tau$ and $|\Lambda(F_a)|\leqslant 2\tau-|F_a|$. From assumptions (1) and (2) we derive a

contradiction, thus proving that if assumption (1) holds, assumption (2) cannot hold.

Let $f_j \in E$ and define $T(f_j) = \{f_i \in E \mid (v_i, v_j) \in C,\ i \neq j\}$. Then, each unit in the PMC model that tests unit v_j corresponds to a elementary fault in $T(f_j)$. By Lemma 4.2.7, assumption (1) implies that $|T(f)| \geq \tau$ for every $f \in E$.

Assumption (2) implies that $|F_a - \Lambda(F_a)| \geq 2$. Lemma 4.2.4 and Definition 4.2.1(iii) imply that for every $f \in F_a - \Lambda(F_a)$, $T(f) \subseteq F_a$. Let $T_a(f) = T(f) \cap \{F_a - \Lambda(F_a)\} = T(f) - \{\Lambda(F_a) \cap T(f)\}$. Then $|T_a(f)| \geq \tau - |\Lambda(F_a)|$. Consequently,

$$\sum_{f \in F_a - \Lambda(F_a)} |T_a(f)| \geq (|F_a - \Lambda(F_a)|)(\tau - |\Lambda(F_a)|).$$

(The quantity $\sum_{f \in F_a - \Lambda(F_a)} |T_a(f)|$ represents the number of distinct tests $t_k \in T$ such that $f \in F_a - \Lambda(F_a)$ and $\hat{f} \in F_a$ exist where $G(f)_k = 1$ and $G(\hat{f})_k = 2$.)

If no two units test each other, then $f_i \in T(f)$ implies that $f \notin T(f_i)$. Therefore, $f_i \in T_a(f)$ implies that $f \notin T_a(f_i)$. Consequently,

$$\sum_{f \in F_a - \Lambda(F_a)} |T_a(f)| \leq \frac{(|F_a - \Lambda(F_a)|)(|F_a - \Lambda(F_a)| - 1)}{2}$$

Combining these bounds yields,

$$\frac{(|F_a - \Lambda(F_a)|)(|F_a - \Lambda(F_a)| - 1)}{2} \geq (|F_a - \Lambda(F_a)|)(\tau - |\Lambda(F_a)|);$$

or equivalently, since $|F_a - \Lambda(F_a)| = |F_a| - |\Lambda(F_a)|$,

$$|\Lambda(F_a)| \geq 2\tau - |F_a| + 1,$$

which contradicts assumption (2).

Therefore, whenever no two units in the PMC model test each other, the

condition $|\Lambda(F)| = \tau$ for every $F \in A_n$ such that $|F| = \tau$ implies that $|\Lambda(F)| > \min(|F| - 1, 2\tau - |F|)$ for every $F \in A_n$ such that $\tau \leq |F| \leq 2\tau$.

The converse is immediate. □

REFERENCES

[BAR76] Barsi, F., Grandoni, F. and Maestrini, P., A Theory of Diagnosability of Digital Systems, IEEE Transactions on Computers, Vol. C-25 , June 1976, pp. 585-593.

[COR76] Corluhan, A.M. and Hakimi, S.L., On an Algorithm for Identifying Faults in a T-Diagnosable System, Proceedings of the 1976 Conference on Information Science and Systems, The Johns Hopkins University, Baltimore, 1976, pp. 370-375.

[FRI80] Friedman, A.D. and Simoncini, L., System-Level Fault Diagnosis, Computer, March 1980, pp. 47-53.

[HAK74] Hakimi, S.L. and Amin, A.T., Characterization of Connection Assignment of Diagnosable Systems, IEEE Transactions on Computers, Vol. C-23 , January 1974, pp. 86-88.

[HAV81] Havlicsek, B.L. and Meyer, G.G.L., Totally Morphic HM Fault Model, The Johns Hopkins University, Department of Electrical Engineering and Computer Science, Technical Report JHU-EE-81-15, 1981.

[HAV82] Havlicsek, B.L. and Meyer, G.G.L., A New System-level Approach to Diagnosability, The Johns Hopkins University, Department of Electrical Engineering and Computer Science, Technical Report JHU-EECS-82-6, 1982.

[HOL79] Holt, C.S. and Smith, J.E., Diagnosis of Systems with Asymmetric Invalidation, 17th Annual Allerton Conference, October 1979, pp. 354-363.

[KAM75] Kameda, T., Toida, S. and Allan, F.J., A Diagnosing Algorithm for Networks, Information and Control, Vol. 29 (1975), pp. 141-148.

[MEY78] Meyer, G.G.L. and Masson, G.M., An Efficient Fault Diagnosis Algorithm for Symmetric Multiple Processor Architectures, IEEE Transactions on Computers, Vol. C-27, No. 11, November 1978, pp. 1059-1063.

[MEY79] Meyer, G.G.L., Fault Diagnosis Algorithms for Asymmetric Modular Architectures, 17th Annual Allerton Conference, October 1979, pp. 350-353.

[MEY81] Meyer, G.G.L., Fault Diagnosis Algorithms for Asymmetric Modular Architectures, IEEE Transactions on Computers, Vol. C-30, No. 1, January 1981, pp. 81-83.

[PRE67] Preparata, F.P., Metze, G. and Chien, R.T., On the Connection Assignment Problem of Diagnosable Systems, IEEE Transactions on Electronic Computers, Vol. EC-16 , December 1967, pp. 848-854.

[RUS75a] Russell, J.D. and Kime, C.R., System Fault Diagnosis: Closure and Diagnosability with Repair, IEEE Transactions on Computers, Vol. C-24, November 1975, pp. 1078-1089.

[SMI79] Smith, J.E., Universal System Diagnosis Algorithms, IEEE Transactions on Computers, Vol. C-28, No. 5, May 1979, pp. 374-378.

[SOG64] Sogomonyan, E.S., Monitoring Operability and Finding Failures in Functionally Connected Systems, Automatic and Remote Control, Vol. 25, No. 6, June 1964, pp. 874-882.

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER: JHU/EECS-82/6	2. GOVT ACCESSION NO.: AD A129474
3. RECIPIENT'S CATALOG NUMBER:	
4. TITLE (and Subtitle): A New System-Level Approach to Diagnosability.	5. TYPE OF REPORT & PERIOD COVERED: Technical
	6. PERFORMING ORG. REPORT NUMBER:
7. AUTHOR(s): B. L. Havlicsek, G. G. L. Meyer	8. CONTRACT OR GRANT NUMBER(s): N00014-80-C-0772
9. PERFORMING ORGANIZATION NAME AND ADDRESS: The Johns Hopkins University, Baltimore, MD 21218	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS:
11. CONTROLLING OFFICE NAME AND ADDRESS: Office of Naval Research, Arlington, VA 22217	12. REPORT DATE: December 1, 1982
	13. NUMBER OF PAGES: 33
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office):	15. SECURITY CLASS. (of this report): unclassified
	15a. DECLASSIFICATION/DOWNGRADING SCHEDULE:

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release, distribution unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

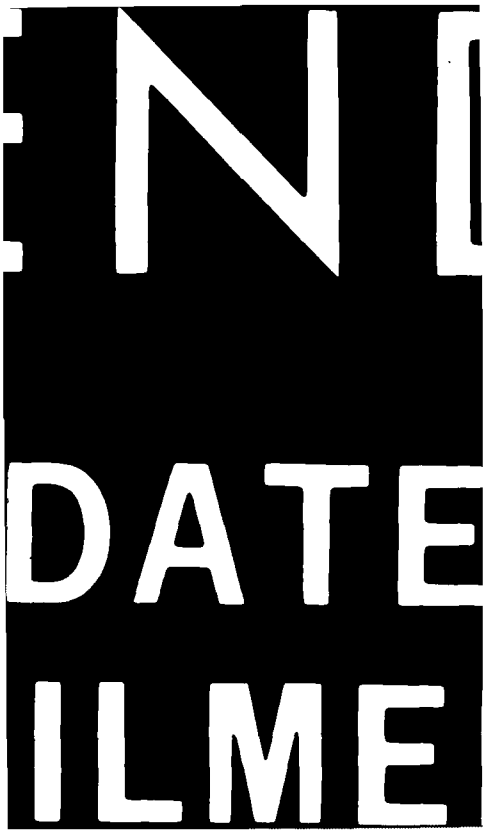
fault, fault model, fault diagnosis

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

This paper presents a new approach to determine the conditions that ensure diagnosability properties in complex systems. The approach uses a new system-level fault model having both internal and observable test outcomes. The results obtained demonstrate that previous diagnosability conditions can be reconstructed and that new diagnosability conditions can be determined.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE
S/N 0102-LF-014-6601

Unclassified
SECURITY CLASSIFICATION OF THIS PAGE (When Data Enter


N
DATE
ILME