SRC TR 86-81

System Level Fault Diagnosis: An Overview

by

J. Narasimhan and K. Nakajima

TR-86-81

System Level Fault Diagnosis: An Overview

by

Jagannathan Narasimhan
and
Kazuo Nakajima

System Level Fault Diagnosis: an Overview [1]

Jagannathan Narasimhan

Electrical Engineering Department,
and Systems Research Center
University of Maryland
College Park, MD 20742

and

Kazuo Nakajima

Electrical Engineering Department,
Institute for Advanced Computer Studies,
and Systems Research Center
University of Maryland
College Park, MD 20742

November 25, 1986

[1]This work was supported in part by National Science Foundation Grants DCI-84-51510 and CDR-85-00108, and in part by a grant from AT&T Information Systems

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Recent times have seen a rapid growth in the development of digital systems. The cost of the hardware has shown a remarkable decline allowing designers to build systems which are extremely complex. This in turn has resulted in these complex systems being used in applications which require a high degree of reliability. With the advent of a distributed processing environment a large number of quasi independent modules are now interconnected to form megasystems. The real time applications in which these systems are used require that their designers build into them efficient means of failure detection and in most cases correction mechanisms.

Circuit level fault diagnosis and correction techniques are used widely in building digital systems. However the complexity and the interconnections of the various modules involved in the structure of these systems require fault diagnosis at a system level too. The importance of system level diagnosis has been recognized by many in the recent past and has encouraged a lot of research which has now reached quite an advanced stage.

This report describes in fair detail some of the important developments that have taken place in system level fault diagnosis since interest was aroused in this field of research by Preparata, Metze and Chien [36] in 1967. It is organized in three parts each one dealing with a specific subfield in the area. Knowledge of fundamental graph theory is assumed. Wherever necessary references for specific topics in graph theory are provided.

1.1 Graph Theoretical Models of Fault Diagnosable Systems

A system could be perceived as an interconnection of a number of modules or units forming a network in the context of fault tolerant computing. A system of units which are interconnected is represented by a graph $G(V, E)$, where the

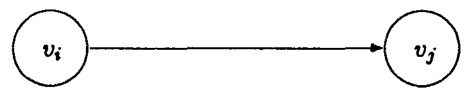


Figure 1.1: The digraph model

set V of vertices in the graph corresponds to the set of units in the system, and the set E of edges in the graph corresponds to the interconnections between the units.

Graph theoretic models may be divided into two classes, namely the digraph model and the undirected graph model depending on the nature of the testing mechanisms used to identify faulty units.

1.1.1 The Digraph Model

The **digraph model** is used to represent systems where each unit can evaluate a subset of the other units and can in turn be evaluated by a subset of the other units in the system. A directed edge from vertex v_i to vertex v_j indicates that the unit v_i is capable of testing the unit v_j. The outcome of this test is associated with a weight 0 or 1 depending on whether v_i evaluated v_j to be fault-free or faulty. Figure 1.1 shows such a model.

1.1.2 The Undirected Graph Model

The **undirected graph model** could be used to represent systems where the test measures and compares the responses of two different units in the system to external stimuli. The stimuli is input from an external device and the measurement and the comparison are also done by the external device. In such a test environment the test is not administered by either of the two systems. Figure 1.2 shows such a model.

1.1.3 Definitions

Some of the basic definitions used widely in the text of this report are listed below. Other definitions are introduced as and when they are required.

Diagnostic Graph: A *diagnostic graph* is a graph which represents the system as described in either section 1.1.1 or 1.1.2.

Figure 1.2: The undirected graph model

Diagnostic Test: A *diagnostic test* is a test which has a binary outcome (either a 0 or a 1) and is represented by a directed edge or an undirected edge depending on the type of test performed.

Test Invalidation Assumptions: *Test invalidation assumptions* are a set of assumptions made on the behavior of the modules in the system. These assumptions enable us to characterize the systems as will be seen later.

Syndrome: The set of all outcomes of the diagnostic tests performed on the system is called a *syndrome.*

t-diagnosability: A system is said to be *t-diagnosable* if, given a syndrome and the fact that the system contains no more than t faulty units, all the faulty units in the system can be identified.

Consistent Fault Set: A set of units $X \subseteq V$ is a *consistent fault set* only if it is consistent with the test results that X contains only faulty units and $V - X$ contains only fault-free units.

1.1.4 Notations

The notations used in the text of this report are described below.

$|X|$: For any set X, $|X|$ is defined to be the cardinality of the set X.

$\Gamma^-(x)$: For any given digraph $G(V, E)$ and a vertex $x \in V, \Gamma^-(x) = \{v \in V \mid (v, x) \in E\}$.

$\Gamma^+(x)$: For any given digraph $G(V, E)$ and a vertex $x \in V, \Gamma^+(x) = \{v \in V \mid (x, v) \in E\}$.

$\Gamma^-(X)$: For a given digraph $G(V, E)$ and a set $X \subseteq V, \Gamma^-(X) = \bigcup_{v \in X} \Gamma^-(v) - X$.

$\Gamma^+(X)$: For a given digraph $G(V, E)$ and a set $X \subseteq V, \Gamma^+(X) = \bigcup_{v \in X} \Gamma^+(v) - X$.

$\Gamma(X)$: For a given undirected graph $G(V, E)$ and a set $X \subseteq V$, $\Gamma(X) = \bigcup_{v \in X} \Gamma(v) - X$.

$\Gamma(x)$: For any given undirected $G(V, E)$ and a vertex $x \in V, \Gamma(x) = \{v \in V \mid (x, v) \in E\}$.

$d^-(v)$: For a vertex v in a given digraph $G(V, E)$, $|\Gamma^-(v)|$ is called the indegree of v and is denoted by $d^-(v)$.

$d(v)$: For a vertex v in a given undirected $G(V, E)$, $|\Gamma(v)|$ is called the degree of v and is denoted by $d(v)$.

1.1.5 Synthesis and Analysis of Fault Diagnosable Systems

The fundamental areas of research in fault diagnosable systems are characterization, synthesis and analysis of these systems. The following chapters in the report describe these areas specifically for different test invalidation assumptions. An brief description of the characterization, synthesis and analysis problems are provided below.

Characterization of t-diagnosable systems

The *characterization* of t-diagnosable systems refers to the problem of determining the necessary and sufficient conditions for the t-diagnosability of the systems under the assumptions on which they are based.

Synthesis of t-diagnosable systems

The *synthesis* problem involves determining a set of tests which would be sufficient to diagnose a system that is t-diagnosable. The aim of most researchers in this area has been to design a system which contains a minimum number of such tests and to develop efficient algorithms to analyze the results of these tests. Nakajima [29] provided the first adaptive algorithm for the system level diagnosis. This and other approaches used in the synthesis of fault diagnosable systems are discussed in detail later in this report.

Analysis of t-diagnosable systems

Analysis of t-diagnosable systems refers to the problem of determining the the maximum value of t for which a given system is t-diagnosable. Analysis in other words is the determination of properties of a predefined system like the maximum number of faulty units that the system can tolerate etc. Sullivan [39] has given the first polynomial time algorithm for the analysis of a system in the model proposed by Preparata, Metze and Chien [36]. The problem of analysis could in a sense be perceived as the opposite of the problem of synthesis.

Chapter 2

Characterization of t-Diagnosable Systems

A survey of different t-diagnosable systems along with their characterizations are presented in this part of the report. Various researchers have used different test invalidation assumptions to characterize their models. Each of the models can be justified for a some specific physical properties inherent to the system. Common to all the models however are some basic assumptions.

In systems which can be represented by the digraph model it is assumed that

(i) no unit tests itself,

(ii) each unit has the capability of testing another unit in the system solely by itself if a test connection is provided from the testing unit to the tested unit and,

(iii) for any pair of units v_1 and v_2, unit v_1 performs at most one diagnostic test on unit v_2. Note, however, that the diagnostic test itself may consist of may test stimuli but can have only a binary outcome.

In systems represented by the undirected graph model it is assumed that

(i) comparative tests are performed between pairs of units and

(ii) at most one diagnostic test is performed on a pair of units in the system.

Based on the test invalidation assumptions, t-diagnosable systems can be broadly classified into two categories. They are the *symmetric* and the *asymmetric* models. The symmetric model first proposed by Preparata et. al. [36] postulates that the result of a test performed by a fault-free unit is always reliable whereas the result of a test performed by a faulty unit is never reliable.

Testing unit	Tested unit	Test outcome(Edge weight)
Fault-free	Fault-free	0
Fault-free	Faulty	1
Faulty	Fault-free	0/1 unpredictable
Faulty	Faulty	0/1 unpredictable

Table 2.1: The PMC model

The **asymmetric** model first proposed by Barsi, Grandoni and Maestrini [2] postulates that it is very unlikely that two units in the system would fail precisely in the same way and hence a faulty unit will never find another faulty unit fault-free.

2.1 Symmetric Models

2.1.1 The PMC Model

The characterization of the PMC model first proposed by Preparata et. al. [36] was provided by Hakimi and Amin [13]. The model is referred to as the PMC model in this report. The proof of their characterization is provided based on a more elegant and generalised characterization theorem given by Allan, Kameda and Toida [1]. The PMC model is a digraph model whose test invalidation assumptions are shown in Table 2.1.

Theorem 2.1 (Hakimi and Amin) *Let S be a system of n units under the PMC model represented by a digraph $G(V,E)$. S is t-diagnosable $\Longleftrightarrow$ (i) $n > 2t+1$, (ii) $\forall v \in V, d^-(v) \geq t$ and (iii) $\forall q \in \{0,1,2,\ldots,t-1\}$ and $\forall X \subseteq V$ with $|X| = n-2t+q$, $|\Gamma^+(X)| > t-q+1$.*

An example of a 2-diagnosable PMC model is shown in Figure 2.1. The system consists of five units 1,2,3,4,5 represented by the vertices v_1, v_2, v_3, v_4 and v_5 and a connection assignment of ten tests. It can be easily seen from the figure that units 1,4 and 5 cannot be faulty. If 1 is faulty then 5 must be faulty and hence 4 must be faulty too. Hence there are at least 3 faulty units in the system. For the given syndrome, using similar arguments, it can be shown that there must be at least 3 faulty units if units 4 or 5 are faulty. We conclude that units 4 and 5 cannot be faulty. Units 2 and 3 must be faulty since unit 1 finds them faulty and unit 1 is fault-free.

Figure 2.2 shows a system which is not 2-diagnosable. For the connection of units there are two possible consistent fault sets, namely $\{v_2, v_3\}$ and $\{v_2, v_4\}$.

Allan, Kameda and Toida [1] have presented the necessary and sufficient conditions for characterization of the PMC model in a slightly different manner. Their characterization is based on the properties of the partitions of the vertices

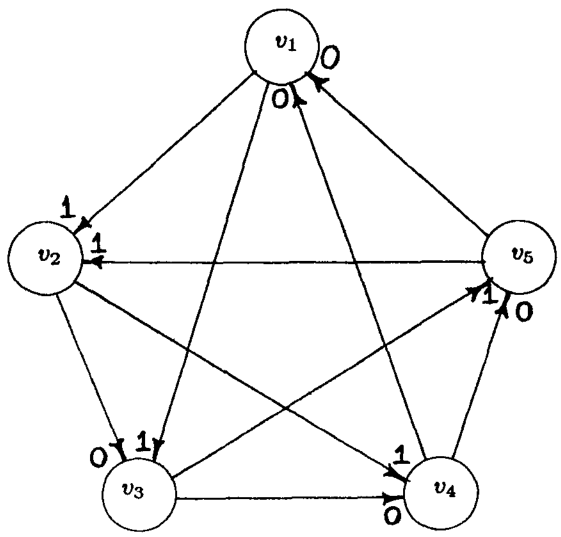


Figure 2.1: 2-diagnosable PMC system

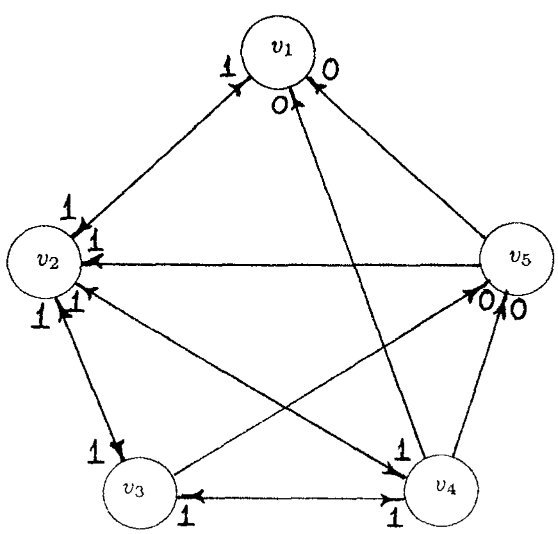


Figure 2.2: PMC system which is not 2-diagnosable

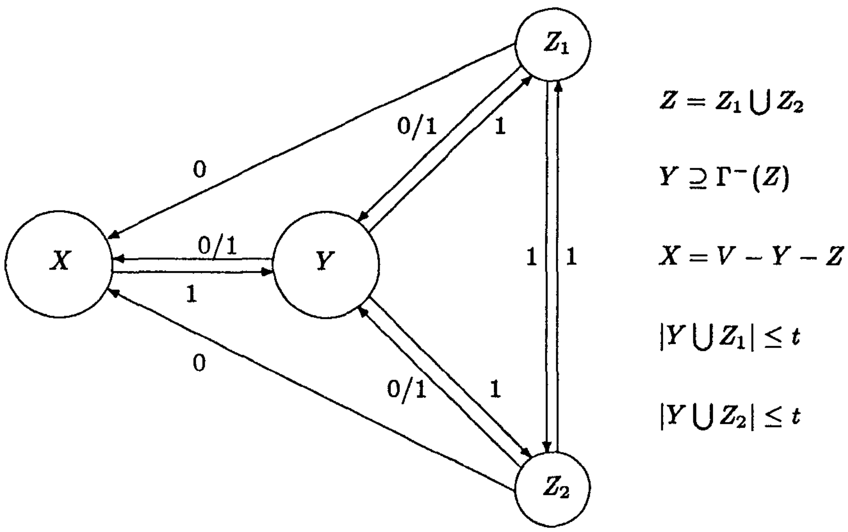


Figure 2.3: An AKT partition for proof of necessity

of the diagnostic graph. The partitions of t-diagnosable systems defined for their characterization are referred to as AKT partitions in this report.

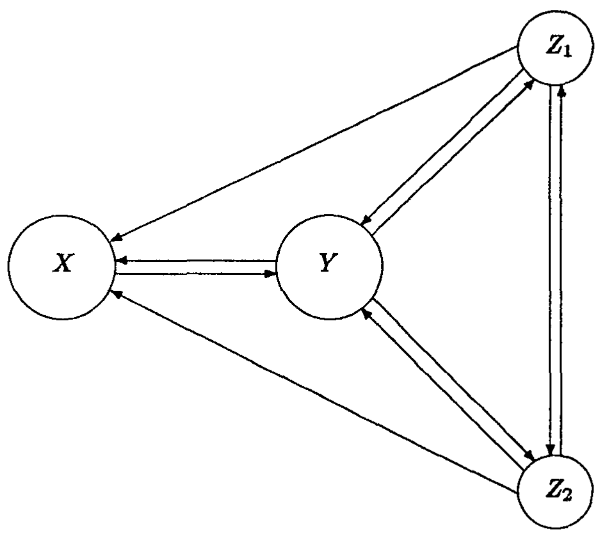
Theorem 2.2 (Allan, Kameda and Toida) *Let P be the set of partitions (X, Y, Z) of V of a digraph $G(V, E)$ defined with (i) $|Z| \geq 1$, and (ii) $\Gamma^-(Z) \subseteq Y$. Let $k(p)$ be defined as $k(p) = |Y| + \lceil \frac{|Z|}{2} \rceil$, where $\lceil r \rceil =$ the ceiling of r. The system S represented by the digraph $G(V, E)$ is t-diagnosable $\Longleftrightarrow \forall p \in P, k(p) > t$.*

Proof. The proof of this theorem is provided in two parts. The first part shows the necessity and the second part shows the sufficiency.

Necessity: Suppose there exists a partition $p = (X, Y, Z) \in P$ with $k(p) \leq t$. Partition the set Z of p into two sets Z_1 and Z_2 such that $|Z_1| + 1 \geq |Z_2|$. Then for the syndrome shown in Figure 2.3 figure both the sets $Y \bigcup Z_1$ and $Y \bigcup Z_2$ are consistent fault sets. Note that $|Y \bigcup Z_1|$ and $|Y \bigcup Z_2|$ are less than t. The system is thus not t-diagnosable.

Sufficiency: Suppose that a given PMC system is not t-diagnosable. This means that there exists a syndrome for which there are at least two possible consistent fault sets whose cardinalities do not exceed t. Let V_f and V_{f^1} be two such fault sets. Define the sets X, Y, Z, Z_1 and Z_2 as follows :

$$Y = V_f \bigcap V_{f^1}$$
$$Z_1 = V_f - Y$$
$$Z_2 = V_{f^1} - Y$$
$$Z = Z_1 \bigcup Z_2$$



$Y = V_f \bigcap V_{f^1}$

$Z_1 = V_f - Y$

$Z_2 = V_{f^1} - Y$

$Z = Z_1 \bigcup Z_2$

$X = V - (Y \bigcup Z)$

Figure 2.4: An AKT partition for proof of sufficiency

$$X = V - (Y \bigcup Z).$$

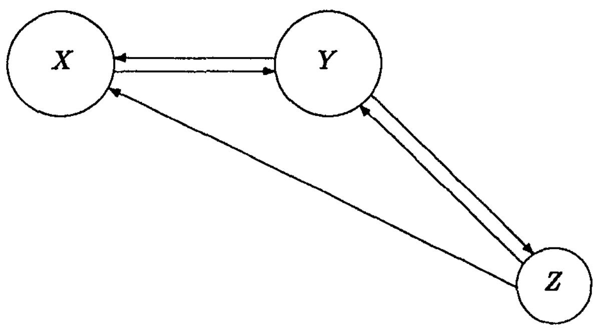
If V_f and V_{f^1} are distinct fault sets, then at least one of $|Z_1|$ or $|Z_2|$ is not equal to zero. The units in the set X are all fault-free. Since the diagnosis of a fault-free unit is always reliable, the units in X cannot test any unit in either Z_1 or Z_2, because then the unit tested would be positively identified as faulty and V_f and V_{f^1} will not be two distinct fault sets. Therefore $\Gamma^-(Z) \bigcap X = \phi$ and $\Gamma^-(Z) \subseteq Y$. Hence the partition $p = (X, Y, Z) \in P$. Such a partition is shown in Figure 2.4. From the definition of Y,Z_1 and Z_2 we see that $|V_f| = |Y| + |Z_1|$ and $|V_{f^1}| = |Y| + |Z_2|$. Since $|V_f| \leq t$ and $|V_{f^1}| \leq t$, we note that $k(p) \leq t$. Therefore there exists a partition p for which $k(p) \leq t$. This proves the sufficiency of the theorem. □

The conditions given by Hakimi and Amin [13] for a PMC system to be t-diagnosable can be easily derived from Theorem 2.2 as shown by Allan, Kameda and Toida [1]. In other words, the conditions imposed by Theorem 2.1 on the system can be shown to be properties of the partition p as defined by Theorem 2.2.

1. $p = (\phi, \phi, V) \in P$. Then $k(p) > t \Longrightarrow \lceil \frac{n}{2} \rceil > t$. Therefore $n > 2t + 1$.

2. Let $v \in V$ be a vertex such that $d^-(v) = d_{min}(G)$, where $d_{min}(G)$ is the minimum of the indegrees of the vertices in the graph. Let $Z = \{v\}$, $Y = \Gamma^-(v)$ and $X = V - (Y \bigcup Z)$. The partition $p = (X, Y, Z) \in P$. See Figure 2.5. Then $k(p) = d_{min}(G) + 1$. Since $k(p) > t$, $d_{min}(G) > t + 1$. Therefore $d_{min}(G) > t$.

3. To prove the third condition it is shown that the condition is both necessary and sufficient for the generalised characterization to be true. That is, if



$Z = \{v\}$

$Y = \Gamma^{-}(v)$

$X = V - (Y \bigcup Z)$

Figure 2.5: An AKT partition proving that $d_{min}(G) > t$

$k(p) > t, \forall p \in P$, then the condition is true and vice versa.

Necessity: If $k(p) \leq t, |Y| + \lceil \frac{|Z|}{2} \rceil \leq t$. Let $|Y| = q$. Thus $0 \leq q < t$, because $|z| \geq 1$. Hence $\lceil \frac{|Z|}{2} \rceil \leq t - q$. Therefore $|Z| \leq 2t - 2q$. Since $X = V - (Y \bigcup Z), |X| \geq n - 2t + q$. There is thus at least one X such that the condition (iii) of Theorem 2.1 is violated.

Sufficiency: If condition (iii) of Theorem 2.1 is violated, then $\exists$ an integer q with $0 \leq q < t$ and a set $X \subseteq V$ with $|X| = n - 2t + q$ such that $|\Gamma^{-}(X)| = r$, $r \leq q$. Let $p = (X_1, Y_1, Z_1)$ be defined as $X_1 = X$, $Y_1 = \Gamma^{-}(X)$ and $Z_1 = V - (X \bigcup Y)$. Then $|Z_1| = |V| - |X_1| - |Y_1| = n - (n - 2t + q) - r = 2t - q - r$. Since $0 \leq q \leq t$ and $r \leq q, |Z_1| \geq 2$. Furthermore $Y_1 = \Gamma^{+}(X_1)$,and hence $\Gamma^{-}(Z_1) \subseteq Y_1$. Therefore $p \in P$. Since $|Z_1| = 2t - q - r$ and $r \leq q, \lceil \frac{|Z|}{2} \rceil \leq t - r$. Then $k(p) = |Y_1| + \lceil \frac{|Z_1|}{2} \rceil \leq t - r + r = t$. Hence p is a partition with $k(p) \leq t$.

If p_{min} is a partition with the minimum value of $k(p)$, then $\tau(G) = k(p_{min}) - 1$, is called the **diagnosability number** of the system. $k(p_{min})$ is also referred to as $k_{min}(G)$.

2.1.2 Symmetric Undirected Graph Models

The motivation for the undirected graph models arose from the attempt to compare the performance of fault tolerant computing systems based on modularly redundant systems and t-diagnosable systems. Chwa and Hakimi [4] proposed an undirected version of the PMC model in an application of the theory of t-diagnosable systems to fault tolerant computing. Table 2.2 shows their test

First unit	Second unit	Test outcome(Edge weight)
Fault-free	Fault-free	0
Fault-free	Faulty	1
Faulty	Faulty	0/1 unpredictable

Table 2.2: The Chwa-Hakimi Model

invalidation assumptions. They then showed that the throughput and the reliability of fault tolerant systems are better in t-diagnosable systems than in modularly redundant systems.

Theorem 2.3 (Chwa and Hakimi) *Let S be a system of n units under the Chwa-Hakimi model represented by an undirected $G(V, E)$. S is t-diagnosable $\iff$ (i) $n > 2t+1$, (ii) $d(v) \geq t, \forall v \in V$ and (iii) $\forall q \in \{0, 1, 2, \ldots, t-1\}$ and $\forall X \subseteq V$ with $|X| = n - 2t + q$, $|\Gamma(X)| > t - q + 1$.*

This system can also be characterized by using a generalised approach as in Theorem 2.2. applied to the PMC model. Refer to Narasimhan [33] for the characterization.

2.2 Asymmetric Models

The PMC model presented in Section 2.1.1 presumes that the outcome of a test performed by a faulty unit is unpredictable. It is very unlikely that two faulty units one of which is testing the other will fail precisely in a manner that would provide an outcome 0 for the test if the test contained a very large number of stimuli. Then it is not unreasonable to assume that a faulty unit will never find another faulty unit fault-free. Barsi, Grandoni and Maestrini [2] considered the t-diagnosability of systems based on these assumptions. This model is referred to as the *BGM model* in this report. Such a model will be particularly useful when systems contain very few similar modules. They have given the necessary and sufficient conditions for the t-diagnosability of this model.

The test invalidation assumptions are shown in Table 2.3. From the table it may be observed that if the outcome of a test is 0, then the tested unit is necessarily fault-free. Further, since tests may not be complete, it is not possible to predict the outcome of a test performed by a faulty unit on a fault-free unit.

Figure 2.6 shows a 2-diagnosable system in the BGM model. According to the syndrome shown, units 1 and 4 are necessarily fault-free. Units 2 and 3 are therefore faulty. A system which is not 2-diagnosable in the BGM model is shown in Figure 2.7. The only differences between the systems shown in Figure 2.6 and Figure 2.7 are that unit 4 tests unit 2 instead of unit 3 and unit 1 tests unit 3 instead of unit 2 in the latter system. For the system shown in

Testing unit	Tested unit	Test outcome(Edge weight)
Fault-free	Fault-free	0
Fault-free	Faulty	1
Faulty	Fault-free	0/1 unpredictable
Faulty	Faulty	1

Table 2.3: The BGM model

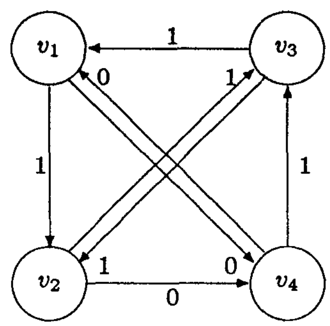


Figure 2.6: A 2-diagnosable BGM system

Figure 2.7, it is not possible to decide whether the consistent fault set is $\{1, 2\}$ or $\{3, 4\}$.

Theorem 2.4 (Barsi,Grandoni and Maestrini) *Let S be a system of n units in the BGM model represented by a digraph $G(V, E)$. S is t-diagnosable $\Longleftrightarrow$ (i) $n > 2$, (ii) $d^-(v) \geq t$, $\forall v \in V$ and (iii) $\forall v, v' \in V$ with $d^-(v) = d^-(v') = t$ and $v' \in \Gamma^-(v) \bigcap \Gamma^-(v'), \exists$ at least one unit $u \in \Gamma^-(v) - \Gamma^+(v')$ and $\Gamma^-(u) \neq \Gamma^-(v')$ or $u \in \Gamma^-(v') - \Gamma^+(v)$ and $\Gamma^-(u) \neq \Gamma^-(v)$.*

Though Theorem 2.4 fully characterizes a system under the BGM model, it is quite convenient to characterize the system using a generalized approach to study some of its properties. The following theorem is similar to Theorem 2.2 for the PMC model.

Theorem 2.5 (Narasimhan and Nakajima) *Let P be the set of partitions (X, Y, Z_1, Z_2) of V of a digraph $G(V, E)$ defined with (i) $|Z_1 \bigcup Z_2| \geq 1$, (ii) $\Gamma^-(Z_1 \bigcup Z_2) \subseteq Y$, and (iii) Z_1 and Z_2 are independent sets. Let $k(p)$ be defined as a function mapping the set of partitions P to the set of non-negative integers I given by $k(p) = |Y| + max\{|Z_1|, |Z|_2\}$. The system is t-diagnosable $\Longleftrightarrow \forall p \in P, k(p) > t$.*

Proof This theorem like Theorem 2.2 is proved by first showing the necessity and then the sufficiency.

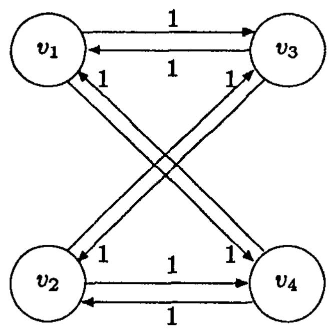


Figure 2.7: BGM system which is not 2-diagnosable

Necessity: Suppose that there exists a partition $p = (X, Y, Z_1, Z_2)$ of V such that $\Gamma^+(X) \subseteq Y, Z_1 \bigcup Z_2 \neq \phi, Z_1$ and Z_2 are independent sets and $k(p) = max\{|Z_1|, |Z_2|\} \leq t$. Note that $|Y \bigcup Z_i| \leq t$ for $i = 1, 2$. Then there is a syndrome shown in Figure 2.8 for which there are two consistent fault sets. Therefore the system is not t-diagnosable.

Sufficiency: Suppose that the system is not t-diagnosable. Then there are two distinct fault sets V_f and V_{f^1} such that $|V_f| \leq t$ and $|V_{f^1}| \leq t$. Let $Y = V_f \bigcap V_{f^1}, Z_1 = V_f - Y, Z_2 = V_{f^1} - Y$ and $X = V - Y - Z_1 - Z_2$. Since $V_f \neq V_{f^1}$ it can be easily seen that $Z_1 \neq Z_2$. Furthermore Z_1 and Z_2 are independent sets. To prove this, suppose otherwise, say $\exists u_i, u_j \in Z_1, (u_i, u_j) \in E$. Since V_f is a consistent fault set, $w(u_i, u_j) = 1$. However, since V_{f^1} is a consistent fault set and $u_i, u_j \in V_f$ we see that $w(u_i, u_j) = 0$, a contradiction. Therefore (u_i, u_j) cannot belong to E. Therefore Z_1 is an independent set. Likewise Z_2 must also be an independent set. Since V_f and V_{f^1} are distinct fault sets, no unit in X can test units in either of Z_1 or Z_2. Thus $\Gamma^+(X) \subseteq Y$. Therefore $p \in P$. This partition is shown in Figure 2.9. Further, since $V_f \leq t$ and $V_{f^1} \leq t$, we see that $k(p) = |Y| + max\{|Z_1|, |Z_2|\} \leq t$. For details about the properties of the minimum partitions, the reader is referred to Narasimhan and Nakajima [35].

If $d_{min}(G)$ is the minimum indegree of G, $c(G)$ the connectivity of the graph G and $\tau(G)$ the diagnosability number of the system, then

1. $\tau(G) \leq d_{min}(G)$.
2. $\tau(G) \geq d_{min}(G) - 1$.
3. $\tau(G) \leq n - 2$.
4. $\tau(G) \geq \min\{c(G), n - 2\}$.
5. If no two units in the system test each other, then $\tau(G) = d_{min}(G)$.

The three conditions stated in Theorem 2.4 characterizing a system in the BGM model can be derived form the above theorem and vice versa.

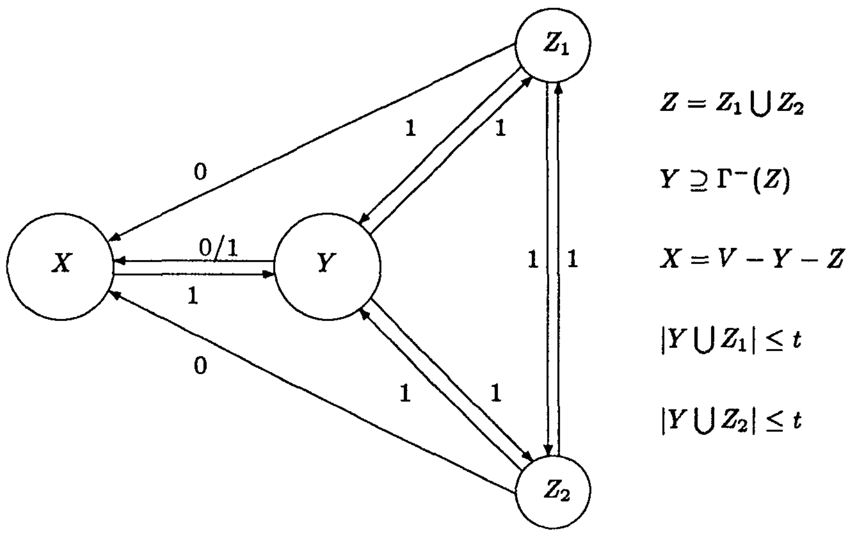


Figure 2.8: A partition for proof of the necessity for the BGM characterization theorem

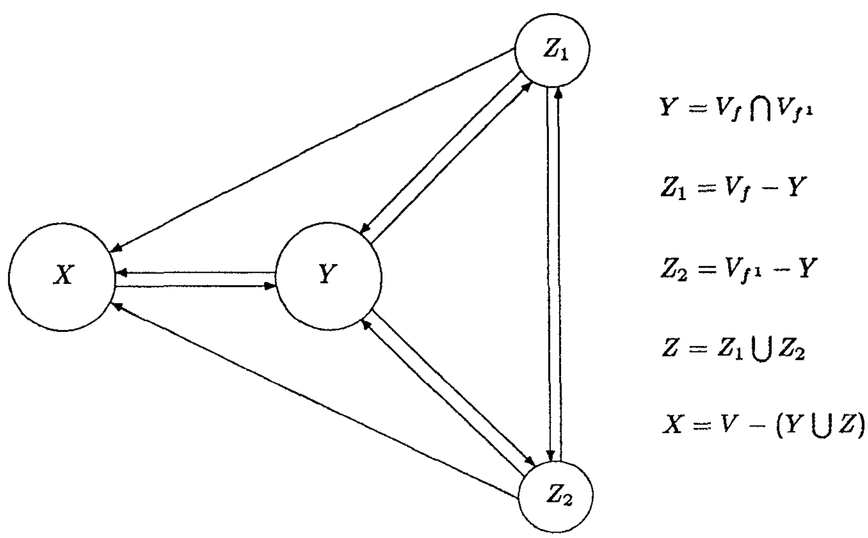


Figure 2.9: A partition for the proof of sufficiency for the BGM characterization theorem

First unit	Second unit	Test outcome(Edge weight)
Fault-free	Fault-free	0
Fault-free	Faulty	1
Faulty	Faulty	1

Table 2.4: The Malek Model

2.2.1 Asymmetric Undirected Graph Models

Malek [26] proposed an undirected graph model corresponding to the BGM system. The motivation for such a model could be seen to be a combination of the motivations for the BGM system and the Chwa-Hakimi undirected graph model. Table 2.4 shows the test invalidation assumptions. The characterization theorem for such a system was given by Dal Cin [5].

Theorem 2.6 (Dal Cin) *Let S be a system of n units in the Malek model represented by an undirected graph $G(V, E)$. S is t-diagnosable $\Longleftrightarrow$ (i) $n > t + 2$, (ii) $d(v) \geq t$, $\forall v \in V$ and (iii) $\forall v, v' \in V$ with $d(v) = d(v') = t$ and $v' \in \Gamma(v) \bigcap \Gamma(v'), \exists$ at least one unit $u \in \Gamma(v) - \Gamma(v')$ and $\Gamma(u) \neq \Gamma(v')$ or $u \in \Gamma(v') - \Gamma(v)$ and $\Gamma(u) \neq \Gamma(v)$.*

This system can also be characterized by using an approach similar to the generalised method of characterization used for the BGM system. The reader is referred to Narasimhan and Nakajima [34] for more details.

2.3 Kreutzer-Hakimi Directed Graph Models

Kreutzer and Hakimi [20] have suggested two other models which are basically digraph models for whose characterization the undirected graph models of Sections 2.1.2 and 2.2.1 could be easily adapted. Their first model assumes that due to a large number of stimuli a faulty unit will never find a fault-free unit faulty. However in a system containing a large number of modules it is not impossible that two systems fail in exactly the same way. Such an assumption gives rise to a digraph model with test invalidation assumptions as shown in Table 2.5. As can be seen the table, though it represents a digraph model, is very much similar to Table 2.2 in Section 2.1.2. It can be easily shown that Theorem 2.3 can be used to characterize such a system. Their next model is a directed graph model which assumes that a faulty unit will alway obtain an outcome 1 for any test it performs. Like the first model, one can observe that the test invalidation assumptions in Table 2.6 are very much similar to those in Table 2.4 for the undirected graph of Section 2.2.1. Theorem 2.4 could thus be used to characterize a system in such a model.

Testing unit	Tested unit	Test outcome(Edge weight)
Fault-free	Fault-free	0
Fault-free	Faulty	1
Faulty	Fault-free	1
Faulty	Faulty	0/1 unpredictable

Table 2.5: Kreutzer-Hakimi Model-I

Testing unit	Tested unit	Test outcome(Edge weight)
Fault-free	Fault-free	0
Fault-free	Faulty	1
Faulty	Fault-free	1
Faulty	Faulty	1

Table 2.6: Kreutzer-Hakimi Model-II

Chapter 3

Synthesis of t-Diagnosable Systems

The theory of t-diagnosable systems as can be seen from the discussion in previous chapters has reached an advanced stage. One of the main areas of interest in t-diagnosable systems is that of designing systems which require the minimum number of diagnostic tests and that of developing efficient algorithms to analyze the results of these tests. The process of synthesis could be explained as one which first chooses a set of tests, then seeks the results of the tests and finally proceeds to use the test results to identify the faulty units in the system assuming that the number of faulty units does not exceed t.

Dahbura and Masson [6] have provided an $O(n^{2.5})$ algorithm that isolates all the faulty units for any syndrome in a digraph representing a t-diagnosable system in the PMC model. Their technique uses some special properties of a diagnostic graph relative to their vertex cover sets and maximum matchings for a system in the PMC model. For specific classes of t-diagnosable systems, however, the diagnosis procedure could be done faster. It should be noted that Dahbura and Masson's algorithm is applicable to any diagnostic graph of a PMC system.

Algorithms have been developed by various researchers to analyze certain classes of t-diagnosable systems. Nakajima [29] proposed the first adaptive diagnosis algorithm for these systems. The adaptive diagnosis procedure as applied to systems under the digraph model first determines a fault-free unit. This unit is then used to identify all other faulty units in the system.

For a system in which each unit is capable of testing all the remaining units, Nakajima [29] showed that one can identify a fault-free unit in $t(t+1)$ tests. Using this fault-free unit, it is then possible to determine all the faulty units for such a system using exactly $n-1$ tests. Therefore, for a fully connected system the total number of tests required is at most $n-1+t(t+1)$ tests. Hakimi and

Nakajima [15] advanced the adaptive diagnosis technique further and showed that for the system described above at most $2t - 1$ tests are required to identify a fault-free unit. Thus $n + 2t - 2$ tests are required to identify all faulty units. By using a different adaptive procedure Blecher [3] showed that all the faulty units could be identified in at most $n + t - 1$ tests and that $n + t - 1$ is the lower bound on the number of tests required to find all faulty units in such a system.

Hakimi and Schmeichel [16] provided an algorithm which identifies a fault-free unit in any system of $2t + 1$ units where no two units test each other. The algorithm is referred to as the HS algorithm in this report. Preparata et al. [36] proposed a second class of systems. This class of systems is known as $D_{\delta t}$. This system is explained in greater detail in Section 3.1.3. Hakimi and Nakajima [15] showed that their adaptive algorithm identifies faulty units in the $D_{\delta t}$ system. Chwa and Hakimi [4] proposed another class of systems known as the $D(n, t, X)$. Nakajima and Krothapalli [31] have shown that a variation of the HS algorithm is applicable to a subset of the $D(n, t, X)$ class of systems known as $D^*(n, t, X)$. The HS algorithm identifies a fault-free unit in at most $2t - B_1(t)$ tests, where $B_1(t)$ is the number of ones in the binary representation of t.

Some of the major classes of systems along with efficient adaptive diagnosis algorithms are given in the sections that follow in this chapter. A detailed proof showing the validity and complexity of each of the algorithms is beyond the scope of this report and is therefore omitted. Diagnosis algorithms are provided for t-diagnosable systems under the PMC and BGM models. Since all these algorithms are also applicable to the undirected graph models with in some cases minor modifications, no separate discussion of algorithms for the undirected graph models are presented. Finally, a brief discussion on distributed diagnosis algorithms is presented.

3.1 Synthesis of Symmetric Systems

This section presents some of the important adaptive diagnosis algorithms developed to diagnose systems in the PMC model. Systems under the PMC models are classified according to the types of interconnection. The applicability of the algorithms to the different classes is discussed.

3.1.1 Fully Connected Systems

The simplest of the classes of t-diagnosable systems under the PMC model would be a system consisting of $2t + 1$ units, where each unit tests every other unit. In this case since every unit tests every other unit, once a fault-free unit has been located, all the faulty units can be located in exactly $n - 1$ tests.

Algorithm 3.1 (Hakimi and Nakajima)

1. *Initialization.* V is the set of units, $V_1 \longleftarrow \phi, |V_1| \longleftarrow 0, L \longleftarrow \phi, |L| \longleftarrow 0, E \longleftarrow \phi$, and t is a given positive integer.

2. If $|L| = 0$ select an arbitrary member $v_1 \in V$, place v_1 at the end of list L, and set $|L| \longleftarrow |L| + 1$ and $V \longleftarrow V - \{v_1\}$.

3. If $|L| + \frac{1}{2}|V_1| < t + 1$,let u be the last element of L and $v \in V$. Seek the result of the test $t_k = (v, u)$ denoted by $R(v, u)$, set $V \longleftarrow V - \{v\}$, and $E \longleftarrow E \bigcup \{(v, u)\}$.

  (a) If $R(v, u) = 0$,place v at the end of L and set $|L| \longleftarrow |L| + 1$, Return to 2.

  (b) If $R(u, v) = 1$, remove u from the end of L and set $|L| \longleftarrow |L| - 1$ and set $V_1 \longleftarrow V_1 \bigcup \{u, v\}$ and $|V_1| \longleftarrow |V_1| + 2$, return to 2.

4. If $|L| + \frac{1}{2}|V_1| = t + 1$, **stop**; the first element of list L is fault-free.

In the process of determining a fault-free unit Algorithm 3.1 also constructs a directed weighted forest $G(U, E)$ where $U = L_u \bigcup V_1$ and L_u denotes the set of units in L. The number of roots of this forest is the number of times Step 1 of the algorithm is used to select an arbitrary member of V. It is easy to see that the algorithm terminates in at most $2t - 1$ tests. The reader is referred to Hakimi and Nakajima [15] for proof of the validity of this algorithm.

Example 3.1 Figure 3.1 shows a 2-diagnosable system. The steps used by Algorithm 3.1 to identify a fault-free unit for the syndrome shown in the figure are outlined below. For this example $t = 2$. Figure 3.1 also shows the forest with 3 roots generated by Algorithm 3.1 when determining a fault-free unit.

1. The first pass through the algorithm isolates the pair of units $\{v_1, v_2\}$. Since $R(v_1, v_2) = 1$, at least one of the two units must be faulty. $|V_1| = 2$ and $|L| = 0$.

2. The second pass through the algorithm isolates the pair of units $\{v_3, v_4\}$. Since $R(v_3, v_4) = 1$, at least one of the two units must be faulty. $|V_1| = 4$ and $|L| = 0$.

3. The third pass concludes that v_5 is fault-free since at least 2 of $\{v_1, v_2, v_3, v_4\}$ are faulty. At this stage it may be noted that v_5 has been included in L. $|L| = 1$ and $|V_1| = 4$, and therefore $|L| + \frac{1}{2}|V_1| > 2$. The last element of L, namely, v_5 is thus fault-free.

4. Tracing from v_5 it is now easy to conclude that the consistent fault set is $\{v_2, v_4\}$.

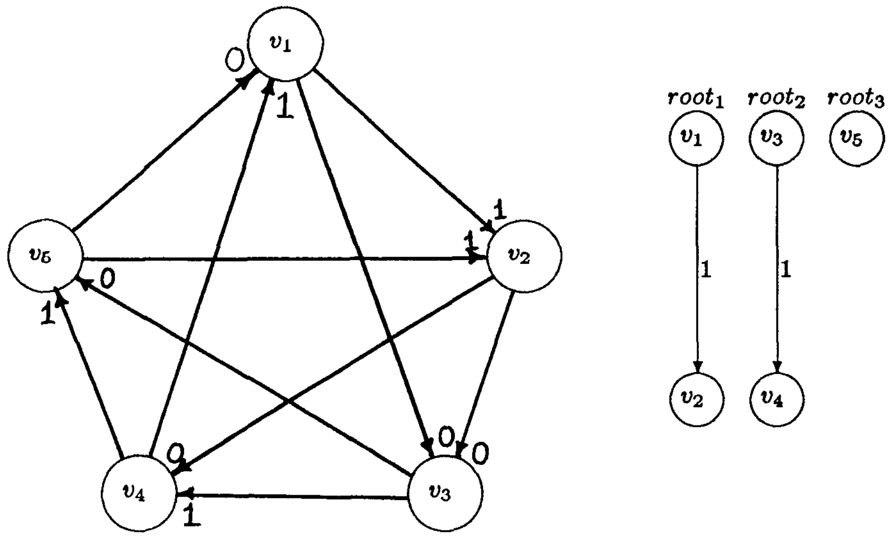


Figure 3.1: A syndrome and the forest generated by an adaptive algorithm for a complete graph

3.1.2 Systems with $n = 2t + 1$ and no Mutual Testing

A system with $n = 2t+1$ and where there is no mutual testing of units is clearly an optimal system. For as per the characterization provided for systems in the symmetric digraph model, each unit must be tested by at least t other units. In this system each unit is tested by exactly t other units and the system is t-diagnosable. Hakimi and Scheimechel [16] developed an adaptive algorithm which identifies a fault-free unit in such a system. It is presented in this section as Algorithm 3.2. This algorithm also makes use of the fact that if the outcome of a test $R(v_i, v_j) = 0$ and v_j is faulty, then there are 2 faulty units in the system, and if $R(v_i, v_j) = 1$, then the pair contains at least one faulty unit.

Algorithm 3.2 (Hakimi and Schmeichel)

1. Let V' be a subset of V with $|V'| = 2t + 1$. For each $u \in V'$ set $f(u) \longleftarrow 1$. Construct a list of the pairs $L = \{(f(u), u)\}$ for all $u \in V'$ in an arbitrary order. Set $L' \longleftarrow \phi$ and $F \longleftarrow 0$.

2. while $|L| > 1$ **do**
Pick the first two members, say $(f(u), u)$ and $(f(v), v)$, and remove them from L and seek the result of the test (u, v) denoted by $R(u, v)$.

(a) If $R(u, v) = 0$, then set $f(v) \longleftarrow f(v) + f(u)$ and create a pair $(f(v), v)$ and place it at the beginning of the list L'. If $f(v) + F > t$, then stop, v is fault-free.

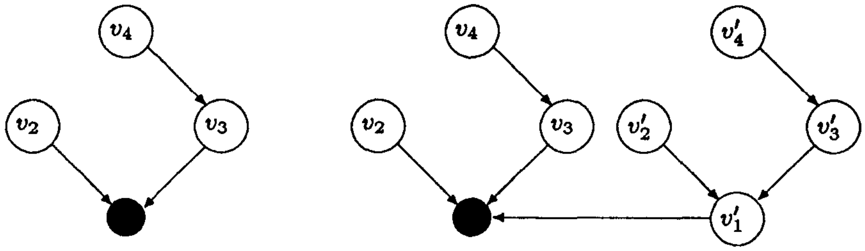


Figure 3.2: Binomial trees of order 2 and 3

(b) If $R(u,v) = 1$, then set $F \longleftarrow F + f(v)$. Let $(f(w), w)$ be the first member of L'. If $L' = \phi$, then let $(f(w), w)$ be the first member of L. If $F + f(w) > t$, then w is fault-free. **Stop.**

end while

3. Let $(f(z), z)$ be the first member of L. Set $L \longleftarrow L'$ followed by $(f(z), z)$. Set $L' \longleftarrow \phi$ and **go to** step 2.

Algorithm 3.2 always identifies a fault-free unit in at most $2t - B_1(t)$ tests, where $B_1(t)$ is the number of ones in the binary representation of t. It is quite useful to note at this point that despite the fact that the algorithm identifies a fault-free unit, it may be impossible to determine all faulty units using just this fault-free unit. Nakajima and Krothapalli [31] have provided an example to show that locating one fault-free unit may be insufficient to locate all the faulty units in the system. The essence of the algorithm is in constructing binomial trees which have the property that if the root is faulty, then all the units in the tree are faulty. Two such trees of the same order could be combined by connecting the roots of the two trees to create a binomial tree, of a higher order with the same property. If there are 2^n nodes in a binomial tree then n is the order of the tree. Figure 3.3 shows a binomial tree of order 2 and a combination of two such trees generating a binomial tree of order 3.

Example 3.2 Figure 3.3 shows a 2-diagnosable system where $n = 2t + 1$ and there is no mutual testing. The steps used by Algorithm 3.2 to identify a fault-free unit for the syndrome shown in Figure 3.3 are outlined below. For this example $t = 2$.

1. Initially $L = \{(1, v_1), (1, v_2), (1, v_3), (1, v_4), (1, v_5)\}$
2. The first time through step 2 of the algorithm, 2(b) is executed and F is set to 1 since $R(v_1, v_2) = 1$ implying that at least one of them must be faulty.
3. The second time through step 2 the algorithm executes 2(a). $f(v_4)$ is set to 2 at this point indicating that if v_4 is faulty, then at least 2 units in the system, namely, v_4 and v_3 are faulty. At this point the

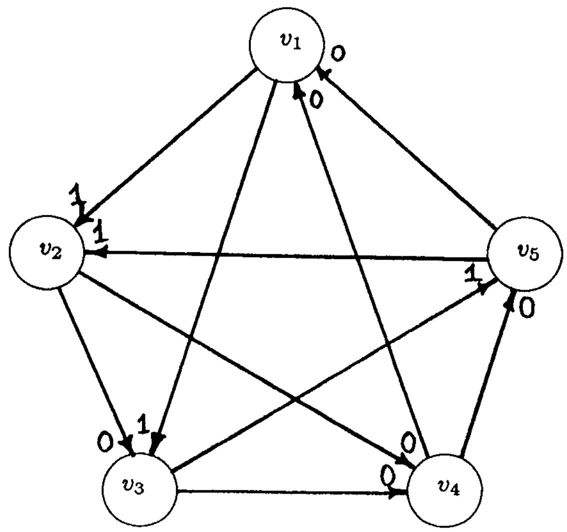


Figure 3.3: Syndrome for example illustrating the Hakimi-Schmeichel algorithm

algorithm notes that $F + f(v_4) > t$ and concludes that v_4 must be fault-free since otherwise there would be 3 faulty units in the system.

If the algorithm were applied to Example 3.1, then it would have executed step 2(b) twice and concluded that v_5 is fault-free.

3.1.3 $D_{\delta t}$ Systems

Let $V = \{v_0, v_1, \ldots, v_{n-1}\}$. Let $G(V, E)$ be a digraph representing an interconnected system. The system is a $D_{\delta t}$ system if $(v_i, v_j) \in E \Longleftrightarrow j - i = \delta k (\mathrm{mod} n), \forall k \in \{1, 2, \ldots, t\}$. Note that the system used in Example 3.2 is a D_{12} system. When δ and n are relatively prime it has been shown that the $D_{\delta t}$ system is t-diagnosable by Preparata, Metze and Chien [36]. The same authors have also shown that by appropriately renaming the units any $D_{\delta t}$ system is equivalent to a D_{1t} system. Krothapalli [22] has shown that a variation of Algorithm 3.2 identifies a fault-free unit in a $D_{\delta t}$ system.

Algorithm 3.3 (Nakajima and Krothapalli)

1. Construct a list L of pairs $\{(f(u), u)\}$ in the following manner. **for** each $i = 0, 1, \ldots, t-1$ **do** Set $f(u) \longleftarrow 1$ and $f(u_{i+t}) \longleftarrow 1$. Insert the pairs $(f(u_i), u_i)$ and $(f(u_{i+t}), u_{i+t})$ at the end of list L in this order.

end for.

Set $f(u_{n-1}) \longleftarrow 1$ and insert $(f(u_{n-1}), u_{n-1})$ at the end of L. Note that since $n > 2t+1$, we can always find the unit u_{n-1}. Set $L' \longleftarrow \phi$ and $F \longleftarrow 0$.

2. while $|L| > 1$ **do** Pick the first two members, say $(f(u), u)$ and $(f(v), v)$, and remove them from L and seek the result of the test $R(u, v)$.

(a) If $R(u, v) = 0$, then set $f(v) \longleftarrow f(v) + f(u)$ and create a pair $(f(v), v)$ and place it at the end of list L'. If $f(v) + F > t$, then v is fault-free. **Stop.**

(b) If $R(u, v) = 1$, then set $F \longleftarrow F + f(v)$. Let $(f(w), w)$ be the first member of L'. If $L' = \phi$, then let $(f(w), w)$ be the first member of L. If $F + f(w) > t$, then w is fault-free. **Stop.**

end while

3. Let $(f(z), z)$ be the first member of L. Set $L \longleftarrow L'$ followed by $(f(z), z)$. Set $L' \longleftarrow \phi$ and **go to** step 2.

In $D_{\delta t}$ systems it may be noted that once a fault-free unit is located, it can be used to locate a set of faulty units or to locate a fault-free unit unidentified thus far. The new fault-free unit may now be used recursively to locate more faulty units and fault-free units until all the faulty units are identified. Algorithm 3.4 shows a method to locate faulty units in a $D_{\delta t}$ system.

Algorithm 3.4 (Nakajima and Krothapalli)

1. Let v_i be a fault-free unit. Set $F \longleftarrow 0, V \longleftarrow V - \{v_i\}, U \longleftarrow \phi$ and $W \longleftarrow \phi$.

2. for each unit $v_i \in \Gamma^+(v_i) \bigcap V$ **do** Set $V \longleftarrow V - \Gamma^+(v_i)$ and seek the result of the test $R(v_i, v_j)$.

(a) If $R(v_i, v_j) = 0$, then set $U \longleftarrow U \bigcup \{v_j\}$.

(b) If $R(v_i, v_j) = 1$, then set $F \longleftarrow F + 1$ and $W \longleftarrow W \bigcup \{u_j\}$.

end for

3. If $F = t$, then all units in $V \bigcup U$ are fault-free and all units in W are faulty. **Stop.** If $F \neq t$, then let v_k be the unit such that $v_k \in \Gamma^+(v_i)$ and $(i - k) \bmod n$ has the highest value among all units in $\Gamma^+(v_i) \bigcap U$. If $U = \phi$, all the units in w are faulty. **Stop.** Otherwise set $i \longleftarrow k$ and **go to** step 1.

In the D_{12} system as Example3.2, once v_4 has been identified as fault-free, v_5 is immediately identified as faulty. v_1 is included in the set U. The next pass through the algorithm enables v_1 to identify v_2 as faulty.

3.1.4 $D^*(n,t,X)$ Systems.

The class of t-diagnosable systems, denoted by $D^*(n,t,X)$, consists of n units $\{v_1, v_2, \ldots, v_{n-1}\}$ and has exactly nt links. If $X = \{x_1, x_2, \ldots, x_t\}$ with $1 \leq x_1 \leq x_2 \leq \ldots \leq x_t \leq \lfloor \frac{n-1}{2} \rfloor$ and $a_1 = x_1$ and $a_i = x_i - x_{i-1}$ for $1 < i \leq t$, then a system of n units, represented by a digraph $G(V,E)$, is said to be in the $D^*(n,t,X)$ system if:

$(v_i, v_j) \in E \Longleftrightarrow (i-j) \bmod n \in X$, and

$a_i > a_{i-1}$ for $1 \leq i \leq t-1$.

As an example a $D^*(7,2,\{1,3\})$ system is shown in Figure 3.4 If the condition (b) in the above definition is omitted, then the class of systems is referred to as the $D(n,t,X)$ first introduced by Chwa and Hakimi [4].

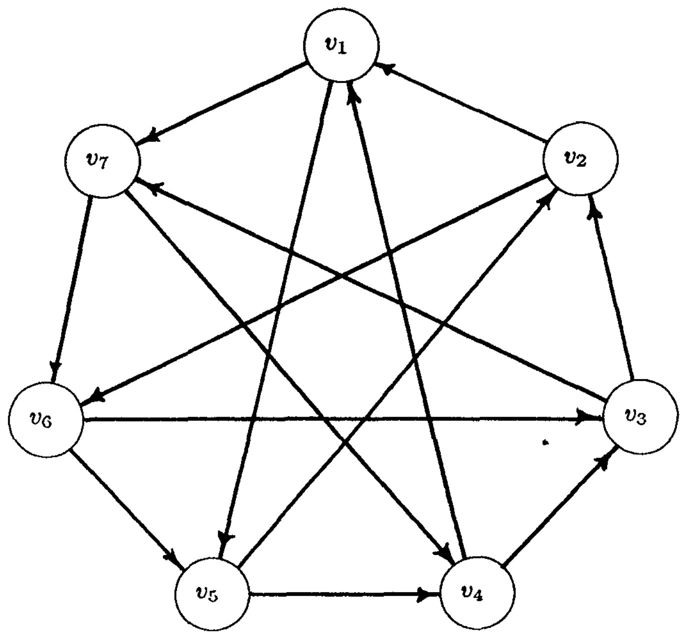
Nakajima and Krothapalli [31] have shown that a variation of Algorithm 3.2 correctly identifies a fault-free unit in the $D^*(n,t,X)$ system. They have also shown that if a fault-free unit is identified, then all the faulty units in the system can be easily located for such a system. Since the algorithms follow a nearly similar pattern to Algorithms 3.2 and 3.4, they have not been ellaborated upon here.

3.2 Synthesis of Asymmetric Systems

All the discussion thus far has been on adaptive algorithms for systems based on symmetric models, that is, systems based on the PMC test invalidation assumptions. In this section the focus is on an adaptive algorithm for asymmetric models based on the BGM test invalidation assumptions. Only one algorithm is presented here. Hakimi and Nakajima [15] first developed this algorithm and showed that it is optimal. That is, the number of tests used by their algorithm is the smallest number needed by any algorithm. Algorithm 3.5 locates a fault-free unit in a BGM system.

To determine a fault-free unit in a system under the BGM model one merely has to locate a test with outcome 0. Once such a test is located, the tested unit is definitely fault-free. See the test invalidation assumptions in Table 2.3. For $n = 2t+1$ it is easy to see that by picking distinct $u_i' s$ and $v_j' s$ and examining the outcome of the tests $(u_i, v_j)' s$, it is quite easy to locate a fault-free unit in t steps. The algorithm outlined below describes a method which is applicable to systems where $t \leq n+2$.

For a system represented by a digraph $G(V,E)$ with a set of n units in V and an integer t with $n \geq t+2$, let $m = n-t-1$ and $q = \lfloor \frac{n-1}{m} \rfloor$. $\lfloor r \rfloor$ is the largest integer smaller than r. Let $V^- = V - \{v_n\}$ with $v_n \in V$. Define $V_1, V_2, \ldots V_m$ to be a partition of V^- such that their cardinalities differ by at most 1. $|V_i| = q$ for $i = n - qm, \ldots, m$ and $|V_i| = q+1$ for $i = 1, 2, \ldots, (n-1-qm)$. Let $V_i = \{v_{i1}, v_{i2}, \ldots, v_{ix_i}\}$ with $q \leq x_i \leq q+1$ for $i = 1, 2, 3, \ldots, m$.



$n = 7$

$t = 3$

$X = \{1, 3\}$

Figure 3.4: A $D^*(n, t, X)$ system

Algorithm 3.5 (Hakimi and Nakajima)

1. *Initialization.* Set $E \longleftarrow \phi$ and let V_i and x_i as defined earlier for $i = 1, 2, \ldots, m$
2. Seek the results of the tests $R(v_{ik}, v_{il})$ for $i = 1, 2, 3, \ldots, m$ and $k < l$ with $1 \leq k < l \leq x_i$. If $R(v_{ik}, v_{il}) = 0$, then v_{il} is fault-free. **Stop.** Otherwise set $E \longleftarrow E \bigcup \{(v_{ik}, v_{il})\}$ and continue.
3. u_n is fault-free. **End.**

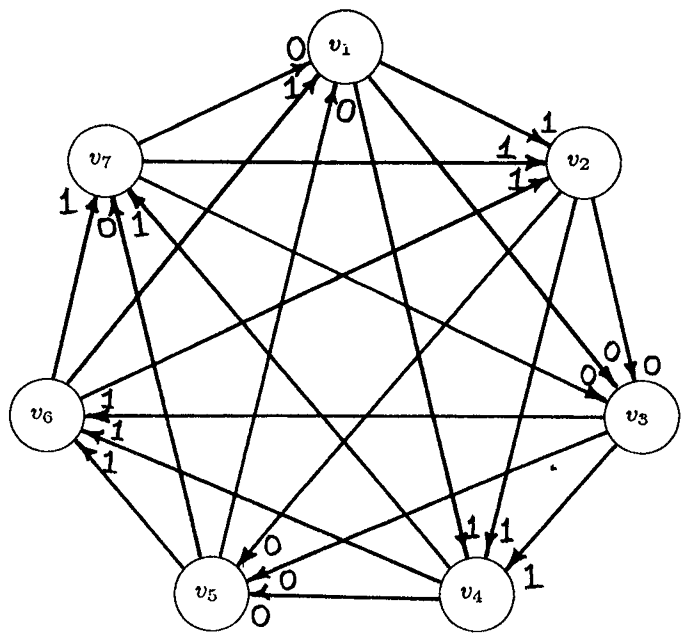
Algorithm 3.5 always identifies a fault-free unit in no more than $(2n - 2 - mq - m)\frac{q}{2}$ tests. For a proof that this is the upper bound on the number of tests required by the algorithm to identify a fault-free unit and that this is also the lowest bound possible, the reader is referred to Hakimi and Nakajima [15].

Example 3.3 In Figure 3.5 the various elements of the partition are shown along with the values of n, t, m and q. If v_2, v_4 and v_6 are faulty, then Algorithm 3.5 determines that there are 3 faulty units in the set $\{v_1, v_2, v_3, v_4, v_5, v_6\}$ and concludes that v_7 is fault-free.

3.3 Distributed Diagnosis

With advances in LSI technology interest in investigating the possibilities of constructing large distributed processing systems has increased considerably. A distributed processing system could be conceived as an interconnection of a large number of smaller units. As the number of such elements increases it is very likely that their reliability will decrease substantially. If a single such element fails and is allowed to operate unchecked, it could act in a manner which could cause a faulty functioning of the entire system. This could happen because unsuspecting elements could be led totally off track when they accept a result from the faulty element and continue to process incorrect data. In such a scenario it will not be long before enough corruption has occurred to make the entire system unreliable. It is necessary therefore to incorporate some method of diagnosing and possibly removing or correcting the faulty element. The system should be built so that it is self diagnosing in this distributed environment. In this section algorithms to diagnose faulty elements in such a distributed system are presented.

The fault model and the algorithms developed by Kuhl and Reddy [23] are presented in this section. The fault models used to devise the distributed diagnosis algorithms are based on the test invalidation assumptions for the PMC model given in Table 2.1.



$n = 7$

$t = 3$

$m = n - t - 1 = 7 - 3 - 1 = 3$

$q = \lfloor \frac{n-1}{m} \rfloor = \lfloor \frac{7-1}{3} \rfloor = 2$

Partition set $= \{(v_1, v_2), (v_3, v_4), (v_5, v_6)\}$
of $V - \{v_n\}$

Figure 3.5: A syndrome for example of an adaptive diagnosis algorithm for a BGM system

3.3.1 The Distributed Fault Model

Every distributed fault model consists of units $\{v_1, v_2, \ldots, v_n\}$ and a set of communication links through which these elements can communicate. It is assumed that no more than t units in the system can be faulty simultaneously. It is assumed that these units are capable of testing a subset of the units with which they have a direct communication link. Further these units are assumed to exchange diagnostic information about their evaluation of the other elements in the system periodically. Distributed diagnosis algorithms should be able to decide rationally which of the units in the system are faulty based on this exchange of information. The test invalidation assumptions for this model are the same as those of the PMC model discussed earlier. The system will thus be associated with a diagnostic graph like systems under the PMC model.

Algorithm 3.6 (Kuhl and Reddy)
Messages for the purpose of exchanging diagnostic information are assumed to be of the form $D_0; D_1$ where each of D_0 and D_1 is a set of integers in the range of $1, \ldots, n$. Each unit computes a fault vector $F_i = f_i^1, f_i^2, \ldots, f_i^n$ where $f_i^j = 1$ if v_i concludes that v_j is faulty and $f_i^j = 0$ if v_i concludes that v_j is fault-free. It is worth noting at this point that information about same unit v_k might not have reached v_i and the entry $f_i^k = u$ in such a case is said to be unspecified. The fault vector F_i for unit v_i is said to be completely specified if F_i contains only ones and zeros or if F_i consists of t ones. Let a_i^r be the outcome of the test performed by v_i on v_r. a_i^r can either be 0 if v_i finds v_r fault-free or 1 otherwise.

1. *Initialization.* Set $D_0 \longleftarrow \phi, D_1 \longleftarrow \phi, f_i^i = 0$ and $F_i^j = u$ for $j \neq i$. (u indicates unspecified.)

2. for each $v_r \in \Gamma^+(v_i)$ **do**

Let $f_i^r = a_i^r$.
if $a_i^r = 0$ **then**

$D_0 \longleftarrow D_0 \bigcup \{r\}$

else

$D_1 \longleftarrow D_1 \bigcup \{r\}$.

end for.

3. Broadcast message $D_0; D_1$ to all $v_r \in \Gamma^-(v_i)$.

4. for each message $D_0'; D_1'$ received from a neighbour v_j where $v_j \in \Gamma^+(v_i)$ and $a_i^j = 0$, until F_i is completed **do**

$D_0 \longleftarrow \phi, D_1 \longleftarrow \phi$.

for each $k \in D_0' \bigcup D_1'$ such that f_i^k is not yet specified **do**

if $k \in D_0'$ **then**

$D_0 \longleftarrow D_0 \bigcup \{k\}$

$f_i^k = 0$

else

$D_1 \longleftarrow D_1 \bigcup \{k\}$

$f_i^k = 1$

end for

if $D_0 \bigcup D_1 \neq \phi$ **then**

broadcast message to all units v_t such that $v_t \in \Gamma^-(v_i) - \{v_j\}$ and $a_i^t \neq 1$.

end for

5. Let any still unspecified positions of F_i be set to 0.

Example 3.4 The example used to illustrate the mechanism of Algorithm 3.6 is based on the D_{12} system of Figure 3.3. For the syndrome shown, after the first round of testing is completed, the fault vectors are $F_1 = 010uu, F_2 = u000u, F_3 = uu001, F_4 = 0uu01, F_5 = 01uu0$. v_1 now receives messages $\{4\};\{5\}$ from v_3 and $\{3,4\};\phi$ from v_2. F_1 will get updated to 01001. v_3 receives messages $\{1\};\{5\}$ from v_4 and $\{1\};\{2\}$ from v_5 and updates F_3 to $0u001$ and subsequently to 01001. F_4 is updated to 01001 when v_4 receives $\{3\};\{2\}$ from v_1 and $\{1\};\{2\}$ from v_5. Note that when F_1, F_3 and F_4 are completed, they identify $\{2,5\}$ as the consistent fault set. In all cases messages from v_2 and v_5 are ignored when generating the fault vectors for units v_1, v_3 and v_4.

One major drawback of the model outlined above is that it is impossible for the units to synchronize themselves so that they are certain about the state of the sender at the instant when the message was sent. Therefore their analysis may not be accurate. It is quite reasonable to assume that each unit performs its tests and broadcasts messages quite independently of the others. The fault vector cannot be viewed as an entity that is calculated at discrete intervals of time, but rather as one which is continuously evolving in time. Due to the time difference between evaluation and sending the messages it is impossible for the units to maintain an accurate picture of the system at all times. The diagnosis of a unit may be outdated. However, it is necessary to ensure that incorrect diagnosis is not made based on the incorrect information received by a unit. One method of ensuring this is to test the sender of the message before using the information already received from the sending unit. Algorithm 3.7 ensures that such an error does not occur. To accomplish this, the scenario is changed slightly. Firstly it is assumed that at some initial startup time all the fault vectors are all set to zero. Subsequently whenever a unit v_i finds a unit v_d faulty, then it broadcasts a message containing a single integer $"d"$ to all units v_k such that $v_k \in \Gamma^-(v_i)$.

Algorithm 3.7 (Kuhl and Reddy)

1. Perform the test of v_j and obtain a_i^j.

2. if $a_i^j = 1$ **then**

$f_i^j \longleftarrow 1$

broadcast message $''j''$ to all $v_k \in \Gamma^-(v_i)$ and $f_i^k = 0$.

Each time v_i receives a diagnostic message $''d''$ from a neighbour v_j, v_i should perform the following:

1. if $f_i^j = 0$ and $v_j \in \Gamma^+(v_i)$ and $f_i^d = 0$ **then**

Test v_j and obtain a_i^j.

if $a_i^j = 0$ **then**

set $f_i^d = 1$

broadcast message $''d''$ to all $v_k \in \Gamma^-(v_i) - \{v_j\}$ whose $f_i^k = 0$.

else

set $f_i^j = 1$ and broadcast message $''j''$ to all $v_k \in \Gamma^+(v_i)$ whose $f_i^k = 0$.

end if

Example 3.5 Consider the same connection assignment of Figure 3.3. Assume that at time t_0 all units were fault-free and all f_i^j were initialized to 0. If at time t_1 the unit v_1 fails and proceeds to diagnose v_3 as faulty, v_1 may initiate messages to v_4 and v_5 indicating that v_3 has failed. On receipt of this message v_4 and v_5 will proceed to test v_1. Finding that v_1 has failed the test, they will set f_4^1 and f_5^1 to 1. v_4 will broadcast the message $''1''$ to v_2 and v_3. v_5 will broadcast the message $''1''$ to v_3 and v_4. Depending on which message was received first, v_2 and v_3 will test v_4 and v_5 and set f_2^1 and f_3^1 to 1.

Kuhl and Reddy [24] have explored the effects of communication link failure and provided another distributed fault diagnosis algorithm to identify faulty units under these circumstances. Hosseini, Kuhl and Reddy [18] have extended this work further and have published a much more comprehensive algorithm to diagnose systems with dynamic failure in a distributed environment.

Chapter 4

Analysis of t-Diagnosable Systems

The research survey on t-diagnosable systems presented thus far has been in the area of designing and diagnosing these systems. Various interconnection schemes which have been introduced in the previous chapters are essentially different approaches to designing t-diagnosable systems and the algorithms presented earlier are means of using these designs effectively to locate faulty units in the system.

In the context of t-diagnosability it must be noted that the configuration of these systems could change with time. That is, the t-diagnosability itself could change. This could happen because of various reasons like introduction of new links, removal of faulty units, removal of links and addition of new units to the system. With reconfiguration of this nature, the properties of the system could get altered very much. For the algorithms presented earlier to function correctly, the properties of the reconfigured system need to be ascertained. This branch of research into t-diagnosable systems is termed **analysis**.

4.1 Analysis of Symmetric Systems

The first polynomial time algorithm for systems under the PMC model was provided by Sullivan [39]. This section gives a brief summary of his technique for analyzing systems under the PMC model. Sullivan [39] has shown that the analysis of these systems is equivalent to the maximal flow problem for a network generated from the diagnostic graph.

For a system under the PMC model let $G(V, E)$ be the diagnostic graph. Its corresponding flow graph $G'(V', E')$ is defined as follows:

$V' = V \bigcup \{s\}$ and

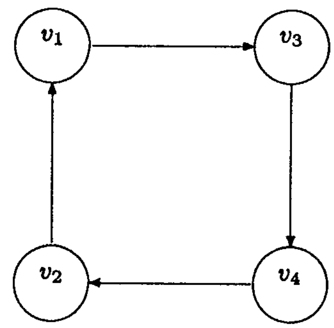


Figure 4.1: PMC digraph

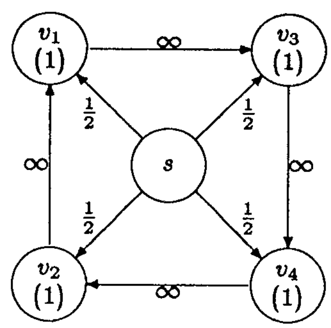


Figure 4.2: Flow graph

$E' = E \bigcup \{s \longrightarrow v, \forall v \in V\}$.

s is a new node introduced into G' termed as the **source** node. Let c' be a capacity function on $E' \bigcup V'$ defined as follows:

$\forall e \in \{s \longrightarrow v | v \in V\}, c'(e) = \frac{1}{2}$,

$\forall e \in E, c'(e) = \infty$ and

$\forall v \in V, c'(e) = 1$.

Theorem 4.1 (Sullivan) *A system in the PMC model represented by the digraph $G(V, E)$ is t-diagnosable $\Longleftrightarrow$ $\forall v \in V$ the maximal flow in the graph $G'(V', E')$ from $s \longrightarrow v > t$.*

To prove Theorem 4.1 Sullivan has made use of the characterization of systems under the PMC model given by Theorem 2.2. Figure 4.1 and Figure 4.2 show a PMC digraph and its corresponding flow graph.

To reduce the order of computation of the maximal flow problem, it becomes useful to redefine the flow graph as shown below. For the digraph $G(V, E)$ let the flow graph $G''(V'', E'')$ be defined as follows:

$V'' = \{s\} \bigcup \{v_{0i}, v_{1i}, v_{2i}, i = 1, 2, \ldots, n\}$, where $V = \{v_1, v_2, \ldots, v_n\}$,

$E'' = \{s \longrightarrow v_{0i}, v_{0i} \longrightarrow v_{1i}, v_{1i} \longrightarrow v_{2i}, i = 1, 2, \ldots, n\} \bigcup \{v_{1i} \longrightarrow v_{1j}, v_{1i} \longrightarrow v_{2j}, v_{2i} \longrightarrow v_{1j}, v_{2i} \longrightarrow v_{2j}, \forall v_i \longrightarrow v_j \in E\}$.

The capacity function for $G''(V'', E'')$ is defined as follows :

$\forall e \in E'', c''(e) = \infty$ and
$\forall v \in V'', c''(e) = 1$.

Theorem 4.2 (Sullivan) *The maximum flow in the network $G'(V', E')$ from $s \longrightarrow v' = F, \forall v' \in V' \Longleftrightarrow$ the maximal flow in the graph $G''(V'', E'')$ from $s'' \longrightarrow v'' = 2F, \forall v'' \in V''$.*

Even and Tarjan [9] have shown that Dinic's algorithm for finding the maximal flow in a network with all edge capacities $= \infty$ and all node capacities $= 1$ from a source to any vertex has a time complexity $O(|E||V|^{\frac{1}{2}})$. Sullivan's algorithm involves solving $|V|$ such maximal flow problems and thus determines the diagnosability of a system in the PMC model in $O(|E||V|^{\frac{3}{2}})$.

4.2 Analysis of Asymmetric Systems

The analysis of asymmetric systems appears to be a much simpler problem. If one is to find an approximate solution, it is readily available as $t \geq d_{min}(G) - 1$ and $t \leq d_{min}(G)$ where $d_{min}(G)$ is the minimum indegree of the graph G. If one is content with an approximate value for the diagnosability, one could stop here. The authors [35] provided the first polynomial time algorithm for a system in the BGM model using the generalized characterization of these systems presented earlier. Recently Kreutzer and Hakimi [21] have used a different approach to determine the diagnosability of an asymmetric system in polynomial time. Nakajima [30] has shown that these two algorithms algorithms compute the diagnosability in $O(nd_{min}^2(G))$ time. Algorithm 4.1 determines the diagnosability of a system in the BGM model. For further details about the algorithm the reader is referred to Narasimhan and Nakajima [35].

Algorithm 4.1 (Narasimhan and Nakajima)

comment: d will be set to be equal to the **diagnosability number** when the algorithm is completed.

$d \longleftarrow n - 1$; $U \longleftarrow \phi$;

```
for each v ∈ V
    if d > d⁻(v) then d ⟵ d⁻(v);
for each v ∈ V
    if d⁻(v) = d then U ⟵ U ⋃ {v};
for each v ∈ U do
    Y ⟵ Γ⁻(v);
    Y1 ⟵ Γ⁺(v) ⋂ Y ⋂ U;
    if |Y1| ≠ 0 then do
        for each y ∈ Y1
            if Γ⁻(y) = {v} ⋃ (Y − {y}) then
              d ⟵ d − 1,
              Stop;
        X' ⟵ V − Y − {v};
        X2 ⟵ φ;
        for each y ∈ Y1 do
            X1' ⟵ X' ⋂ Γ⁻(y);
            for each x ∈ X1'
              if Γ⁻(x) = Γ⁻(v) then X2 ⟵ X2 ⋃ {x};
            if X2 = φ then do
              Z2 ⟵ {y};
              Y2 ⟵ Y1 − {y};
              for each y' ∈ Y2
                if Γ⁻(y') = Γ⁻(y) then Z2 ⟵ Z2 ⋃ {y'};
              if |Z2| = |X2| + 1 then
                d = d − 1,
                Stop;
            end if
        end for
    end if
end for
```

Chapter 5

Conclusion

This report is an introduction to system level fault diagnosis using basic models where two single units are involved in each test. It has dealt with the problems of t-fault diagnosability for interconnected systems. Some of the fundamental characterization theorems for t-diagnosability of these interconnection networks have been presented. Algorithms for identifying faulty units in some classes of these systems have been provided. Distributed diagnosis has been introduced. Finally the problem of analysis of t-diagnosable systems has been mentioned.

In the time span covering the introduction of system level fault diagnosis by Preparata, Metze and Chien [36] in 1967 and the present, numerous researchers have worked in this area and have developed on the field extensively. It can be expected that with the rapid expansion in the use of computer networks, the theories developed in this field will be used very widely. The practicalities of the applicability of system level fault diagnosis and repair both in the area of hardware and that of software would be worth investigating. In one form of generalization of the PMC model provided by Russel and Kime [37] [38], a group of units test another group of units or a single unit. Such variants of the main theme of t-diagnosability would be worth investigating with an eye towards implementation. With regard to asymmetric invalidation assumptions Holt and Smith [17] have investigated these systems further. It is conceivable that the diagnosis algorithms could be speeded up considerably if approximate solutions are sufficient for certain applications. These solutions, however, should never be incorrect. The solutions may isolate a set of units to be faulty, in which case this contains all the faulty units and possibly some fault-free units but its complement should strictly consist of only fault-free units. Imposing conditions of this nature could simplify the diagnosis procedures considerably at the expense of losing some information which could probably be lived with. In this respect the notion of t/k-diagnosability has been introduced by Friedman [10] and some interesting results have been obtained by Karunanithi and Friedman [19], Chwa and Hakimi [4] and Yang, Masson and Leonetti [42].

The effect of intermittently faulty units in a system has been explored by Mallela and Masson [28]. The same authors [27] have presented an analysis of hybrid fault systems in another of their research endeavours. Their efforts have exposed many new topics of research in the area of intermittently faulty systems. A new characterization for intermittent fault systems was obtained by Nakajima and Narasimhan [32]. Dahbura and Masson [7] have also provided a detailed analysis of these systems. Dahbura and Masson [8] have introduced a class of systems known as self implicating systems. The concept of redundancy, introduced in these systems by Toida [40], has also opened new areas for research.

Procedures for testing units in a t-diagnosable system are still not very clearly specified. If a complete test of a unit is not performed by another, then it is not impossible for a fault-free unit to find a faulty unit fault-free in some cases. Maheshwari and Hakimi [25] and later Fujiwara and Kinoshita [11] [12] have provided an analysis of probabilistically diagnosable systems. Effects of introducing probabilities into t-diagnosable systems would be well worth investigating further. Application of t-diagnosability to analog systems have been investigated by Wu, Nakajima, Wey and Saeks [41] and could be of interest in a number of applications. A theory of t-diagnosable analog systems has been established by Hakimi and Nakajima [14].

Bibliography

[1] Allan F.J, Kameda T., and Toida S. An approach to the diagnosability analysis of a system. *IEEE Trans. on Computers*, C-24:1040–1042, Aug 1975.

[2] Barsi F., Grandoni F., and Maestrini P. A theory of diagnosability without repair. *IEEE Trans. on Computers*, C-25:558–593, Jun 1976.

[3] Blecher P.M. On a logical problem. *Discrete Math.*, 43:107–110, 1983.

[4] Chwa K.Y. and Hakimi S.L. On fault identification in diagnosable systems. *IEEE Trans. on Computers*, C-30:414–422, Jun 1981.

[5] Cin Dal M. A diagnostic device for large multiprocessor systems. In *Dig. 12^{th} Int. Symp. on fault tolerant computation*, pp. .357–360, Santa Monica, CA, Jun 1982.

[6] Dahbura A.T. and Mason G.M. An $o(n^{2.5})$ fault identification algorithm for diagnosable systems. *IEEE Trans. on Computers*, C-33:486–492, Jun 1984.

[7] Dahbura A.T. and Mason G.M. Greedy diagnosis as the basis of an intermittent fault/transient-upset tolerant system design. *IEEE Trans. on Computers*, C-32:953–957, Oct 1983.

[8] Dahbura A.T., Mason G.M. and Yang C.-L. Self-implicating structures for diagnosable systems. *IEEE Trans. on Computers*, C-34:718–723, Aug 1985.

[9] Even S. and Tarjan J.E. Network flow and testing graph connectivity. *SIAM J. Computing*, 5:507–518, Aug 1983.

[10] Friedman A.D. A new measure of digital system diagnosis. In *Dig. 1975 Int. Symp. on fault tolerant computation*, pp. .167–169, Jun 1975.

[11] Fujiwara H. and Kinoshita K. Connection assignment for probabilistically diagnosable systems. *IEEE Trans. on Computers*, C-27:280–283, Mar 1978.

[12] Fujiwara H. and Kinoshita K. Some existance theorems for probabilistically diagnosable systems. *IEEE Trans. on Computers*, C-27:379–384, Apr 1978.

[13] Hakimi S.L. and Amin A.T. Characterization of connection assignment of diagnosable systems. *IEEE Trans. on Computers*, C-23:86–92, Jan 1974.

[14] Hakimi S.L. and Nakajima K. On a theory of t-fault diagnosable analog systems. *IEEE Trans. on Computers*, CAS-31:946–951, Nov 1984.

[15] Hakimi S.L. and Nakajima K. On adaptive diagnosis. *IEEE Trans. on Computers*, 234–240, Mar 1984.

[16] Hakimi S.L. and Schmeichel E.F. An improved adaptive algorithm for system level diagnosis. *Journal of Algorithms*, vol. 5, No. 4:234–240, Dec 1984.

[17] Holt C.S. and Smith J.E. Diagnosis of systems with assymmetric invalidation. *IEEE Trans. on Computers*, C-30:679–690, Sep 1981.

[18] Hosseini S.H., Kuhl J.G., and Reddy S.M. A diagnosis algorithm for distributed computing systems with dynamic failure repair. *IEEE Trans. on Computers*, C-33:223–233, Mar 1984.

[19] Karunanithi S. and Friedman A.D. Analysis of digital systems using a new measure of system diagnosis. *IEEE Trans. on Computers*, C-28:121–133, Feb 1979.

[20] Kreutzer S.E. and Hakimi S.L. Adaptive fault identification in two new diagnostic models. In *Proc. of the* 21^{st} *Ann. Allerton Conf. on Comm., Cont. and Comput.*, pp. .353–362, Univ. of Illinois, Urbana Champaign, Oct 1983.

[21] Kreutzer S.E. and Hakimi S.L. Determining fault diagnosability. Unpublished Notes, Dept. EE & Comp.Sci., Northwestern Univ., Evanston, IL. 1985.

[22] Krothapalli P.V. *On fault identification in certain diagnosable systems.* Master's Thesis, Dept. of Elec. Engg., Texas Tech University, Lubbock, Texas, Aug 1983.

[23] Kuhl J.G. and Reddy S.M. Distributed fault tolerance in large multiprocessors. In *Proc. of the* 7^{th} *Ann. Symp. on Comput. Arch.*, pp. .23–30, May 1980.

[24] Kuhl J.G. and Reddy S.M. Fault diagnosis in fully distributed systems. In *Dig.* 11^{th} *Int. Symp. on Fault Tolerant computing*, pp. .100–105, Jun 1981.

[25] Maheshwari S.N. and Hakimi S.L. On models for diagnosable systems and probabilistic fault diagnosis. *IEEE Trans. on Computers*, C-25:228–236, Mar 1976.

[26] Malek M. A comparison connection assignment for diagnosis of multiprocessor systems. In *Proc. of the 7^{th} Symp. on Computer Architecture*, pp. .31–36, May 1980.

[27] Mallela S. and Mason G.M. Diagnosable systems with intermittent faults. *IEEE Trans. on Computers*, C-27:560–566, Jun 1978.

[28] Mallela S. and Mason G.M. Diagnosis without repair for hybrid fault situations. *IEEE Trans. on Computers*, C-29:461–470, Jun 1980.

[29] Nakajima K. A new approach to system diagnosis. In *Proc. of the 19^{th} Ann. Allerton Conf. on Comm., Cont. and Comput.*, pp. .697–706, Univ. of Illinois, Urbana Champaign, Sep 1981.

[30] Nakajima K. On an improvement of diagnosability algorithms for the BGM system level fault model. In *Proc. of the 29^{th} Midwest Symp. on Circuits and Systems*, Lincoln NE, Aug 1986.

[31] Nakajima K. and Krothapalli V.P. On adaptive fault diagnosis in optimal systems. In *Proc. of the 21^{st} Ann. Allerton Conf. on Comm., Cont. and Comput.*, pp. .373–382, Univ. of Illinois, Urbana Champaign, Oct 1983.

[32] Nakajima K. and Narasimhan J. A new characterisation of diagnosable systems for intermittent faults. In *Proc. of the 28^{th} Midwest Symp. on Circuits and Systems*, pp. .558–560, Louisville KY, Aug 1985.

[33] Narasimhan J. *A unified approach to fault diagnosability of systems.* Master's Thesis, Dept. of Elec. Engg. and Comp. Sc., Texas Tech University, Lubbock, Texas, Aug 1984.

[34] Narasimhan J. and Nakajima K. A polynomial time algorithm for fault diagnosability of a system using comparison tests. In *Proc. of the 28^{th} Midwest Symp. on Circuits and Systems*, pp. .554–557, Louisville KY, Aug 1985.

[35] Narasimhan J. and Nakajima K. An algorithm to determine the fault diagnosability of a system. *IEEE Trans. on Computers*, C-35:1004–1008, Nov 1986.

[36] Preparata F.P., Metze G., and Chien R.T. On the connection assignment problem for diagnosable systems. *IEEE Trans. on Electronic Computers*, EC-16:848–854, Dec 1967.

[37] Russel J.D. and Kime C.R. System fault diagnosis: closure and diagnosis with repair. *IEEE Trans. on Computers*, C-24:1078–1089, Nov 1975.

[38] Russel J.D. and Kime C.R. System fault diagnosis: masking, exposure and diagnosability without repair. *IEEE Trans. on Computers*, C-24:1155–1161, Dec 1975.

[39] Sullivan G. A polynomial time algorithm for fault diagnosability. In *Proc. 25^{th} IEEE Symp. Foundations Comput. Sc.*, pp. .148–156, West Palm Beach, FL, Oct 1984.

[40] Toida S. System diagnosis and redundant tests. *IEEE Trans. on Computers*, C-25:1167–1170, Nov 1976.

[41] Wu C.C., Nakajima K., Wey C.L., and Saeks R. Analog fault diagnosis with failure bounds. *IEEE Trans. on Circuits and Systems*, CAS-29:277–284, May 1982.

[42] Yang C.-L., Masson G.M. and Leonetti Richard A. On fault isolation and identification in t_1/t_1-diagnosable systems. *IEEE Trans. on Computers*, C-35:639–643, Jul 1986.