Journal of Circuits, Systems, and Computers, Vol. 1, No. 4 (1991) 353–371

DIAGNOSIS OF *t/s*-DIAGNOSABLE SYSTEMS*

A. DAS
Département d'informatique et de recherche operationnelle, Université de Montréal, Canada

K. THULASIRAMAN
Department of Electrical and Computer Engineering, Concordia University, Canada

V. K. AGARWAL
Department of Electrical Engineering, McGill University, Canada

Received 10 May 1991
Accepted 4 September 1991

A t/s-diagnosable system permits diagnosis of faulty units within a set of s units provided the number of faulty units does not exceed t. A characterization of t/s-diagnosable systems is presented. This characterization is then used to develop an efficient algorithm for diagnosis of t/s-diagnosable systems. It is noted that a useful modification of the algorithm can be used for fault diagnosis of sequentially t-diagnosable systems.

1. Introduction

Several models have been proposed in the literature for diagnosable system design. Of these, the now well-known PMC model introduced by Preparata, Metze, and Chien[1] has been extensively studied. In this model, each processor tests some of the other processors and produces test results, which are unreliable if the testing processor is itself faulty. The collection of all test results over the entire system is referred to as a **syndrome**. The classical constraint used in the study of diagnosable systems is to assume that the number of faulty processors in the entire system is upper bounded by an integer t. A system is then said to be ***t*-diagnosable** if given a syndrome, all processors can be correctly identified as faulty or fault-free, provided that the number of faulty processors present in the system does not exceed t. Three problems of interest in this context are: the ***t*-characterization problem** to determine the necessary and sufficient conditions for the system test assignment to be t-diagnosable, the ***t*-diagnosability problem** to determine the largest value of t for which a given system is t-diagnosable, and finally the ***t*-diagnosis problem** to locate the faulty units present in a t-diagnosable system, using a given syndrome.

Hakimi and Amin[2] gave a solution to the t-characterization problem. An $O(|E|n^{3/2})$ algorithm for the t-diagnosability problem was presented by Sullivan.[3] Dahbura and

* This paper was recommended by Associate Editor T. Murata.

Masson[4] published an $O(n^{2.5})$ algorithm for the t-diagnosis problem; a t-diagnosis algorithm with complexity $O(|E| + t^3)$ was presented by Sullivan.[5] A generalized theory for system-level diagnosis was proposed by Somani, Davis, and Agarwal in Ref. 6. This paper presented a generalized characterization theorem which provides the necessary and sufficient conditions for unique diagnosis of fault sets of any cardinality under different fault models.

The requirement that all the faulty processors in a multiprocessor system be identified exactly is rather restrictive. Friedman[7] introduced the concept of t/s-**diagnosability** which allowed the possible replacement of fault-free processors, whereas in t-diagnosability only the replacement of faulty processors in considered. A multiprocessor system S is said to be t/s-**diagnosable**, if given a syndrome, the set of faulty processors can be isolated to within a set of at most s processors provided that the number of faulty processors does not exceed t. Allowing some fault-free processors to be possibly identified as faulty permits the system to have far fewer tests. It has been shown that t/t-diagnosable systems with $n*[(t + 1)/2]$ tests can be constructed.[8] t/t-diagnosable systems have been studied extensively in the literature. Chwa and Hakimi[9] gave a characterization of t/t-diagnosable systems, Sullivan[3] presented a polynomial time algorithm for the t/t-diagnosability problem, and Yang *et al.*[10] presented an $O(n^{2.5})$ algorithm for the t/t-diagnosis problem. Sullivan also presented, in Ref. 11, a $t/t + k$-diagnosability algorithm which runs in polynomial time for each fixed integer k. This diagnosability algorithm is based on a characterization of $t/t + k$-diagnosable systems also developed in Ref. 11. In Ref. 12, Raghavan has developed, among other things, a characterization of t/s-diagnosable systems. He has also given improved algorithms for the t-diagnosability problem.

A system is **sequentially** t-diagnosable if at least one faulty unit can be identified provided the number of faulty processors in the system does not exceed t. Equivalently, a system is sequentially t-diagnosable if and only if given any syndrome there exists a unit v which is present in every allowable fault set of cardinality at most t.[12]

The objective of this work is to develop diagnosis algorithms for t/s-diagnosable systems. The paper is organized as follows. First in Sec. 2, we present certain basic definitions, notations and results. We present in Sec. 3 the t/s-characterization theorem of Ref. 13. With the objective of determining an efficient test for a vertex v to be in an allowable fault set of cardinality at most t, we establish in Sec. 4 several properties of allowable fault sets. Using these properties and the t/s-characterization, we develop in Sec. 5 a $t/t + k$ diagnosis algorithm which runs in polynomial time for each fixed integer k. In this section we also show how this algorithm can be modified to determine the set of all units which lie in every allowable fault set of cardinality at most t. These units can be correctly identified as faulty. This modified algorithm can thus be used for diagnosis of a sequentially t-diagnosable system.

2. Preliminaries

A multiprocessor system S consists of n units or processors, denoted by the set $U = \{u_1, u_2, \ldots, u_n\}$. Each unit is assigned a subset of other units for testing. Thus the

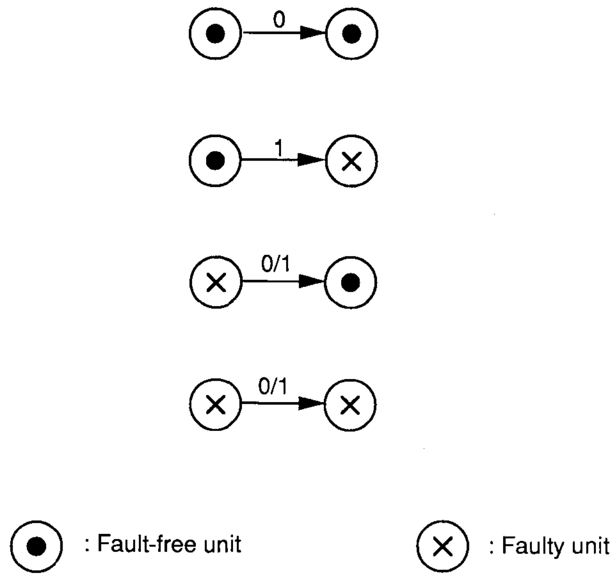


Fig. 1. Test outcomes under the PMC model.

test inter-connection can be modeled as a directed graph $G = (U, E)$. The **test outcome** a_{ij}, which results when unit u_i tests unit u_j, has value 1 (0) if u_i evaluates unit u_j to be faulty (fault-free). Since all faults considered are permanent, the test outcome a_{ij} is reliable if and only unit u_i is fault-free. The collection of all test results over the entire system is referred to as a **syndrome**. Test outcomes under the PMC model are shown in Fig. 1. A system S with a syndrome corresponding to a fault set is given in Fig. 2. If $a_{ij} = 0$ (1) then u_i is said to have a 0-link (1-link) to u_j and u_j is said to have a 0-link (1-link) from u_i.

Given a syndrome, the **disagreement set** $\Delta_1(u_i)$ of $u_i \in U$ is defined as

$$\Delta_1(u_i) = \{u_j \mid a_{ij} = 1 \text{ or } a_{ji} = 1\}.$$

For a subset $W \subseteq U$,

$$\Delta_1(W) = \bigcup_{u_j \in W} \Delta_1(u_j).$$

Given a syndrome, the set of **0-descendents** of u_i is represented by the set

$$D_0(u_i) = \{u_j : \text{there is a directed path of 0-links from } u_i \text{ to } u_j\}$$

and for a set $W \subseteq U$, the **0-ancestors** of W denotes the set

$$A_0(W) = \{u_i : u_j \in D_0(u_i) \text{ and } u_j \in W\}.$$

For $u_i \in U$, $H_0(u_i)$ corresponds to the set $A_0(u_i) \cup \{u_i\}$.

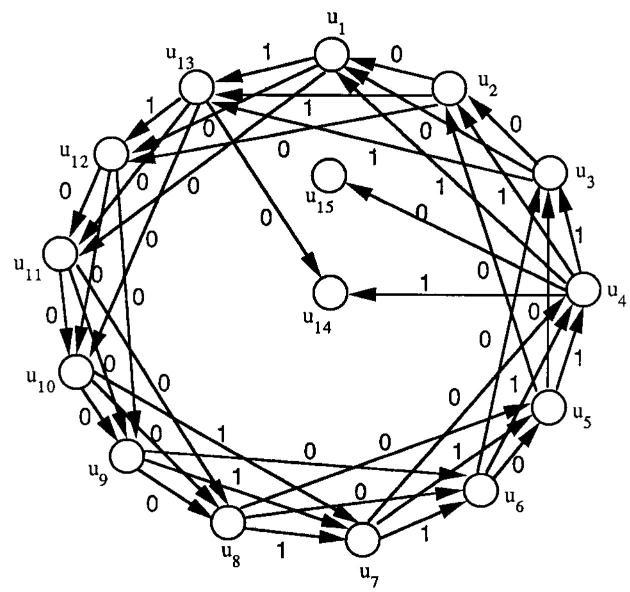


Fig. 2. A syndrome for a 3/4 diagnosable system.

The disagreement set, the 0-descendants and the 0-ancestors of the unit u_7 in Fig. 2 are given below.

$$\Delta_1(u_7) = \{u_5, u_6, u_8, u_9, u_{10}\}.$$

$$D_0(u_7) = \{u_4, u_{15}\}.$$

$$A_0(u_7) = \Phi.$$

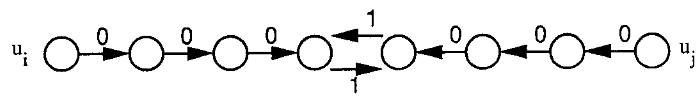
Definition 1[4]: Given a system S and a syndrome, a subset $F \subseteq U$ is an **allowable fault set** (AFS) if and only if

Condition 1: $u_i \in (U - F)$ and $a_{ij} = 0$ imply $u_j \in (U - F)$, and

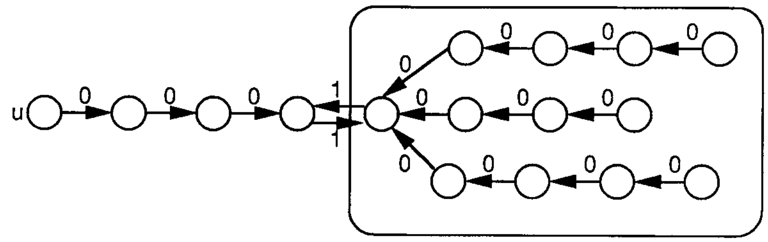
Condition 2: $u_i \in (U - F)$ and $a_{ij} = 1$ imply $u_j \in F$.

In other words, F is an AFS for a given syndrome if and only if the assumption that the units in F are faulty and the units in $U - F$ are fault-free is consistent with the given syndrome. In Fig. 2, the subsets $\{u_4, u_7, u_{13}\}$ and $\{u_4, u_7, u_{13}, u_{14}\}$ are allowable fault sets corresponding to the given syndrome. A **minimum allowable fault set** (MAFS) is an allowable fault set of minimum cardinality.

Definition 2[4]: Given a system S and a syndrome, the **implied faulty set** $L(u_i)$ of $u_i \in U$ is the set of all units of S that may be deduced to be faulty under the assumption that u_i is fault-free.



(a)



(b)

Fig. 3. (a) Implied fault path between two units. (b) Implied fault set for unit u.

It follows that

$$L(u_i) = \Delta_1(D_0(u_i)) \cup A_0(\Delta_1(D_0(u_i))).$$

Note that if $u_j \in L(u_i)$ then there exists a 1-link (u_k, u_l) or (u_l, u_k) such that there is a directed path of 0-links from u_i to u_k and a directed path of 0-links from u_j to u_l. Such a path will be referred to as an **implied-fault path** between u_i and u_j.

The implied fault path and the implied fault set for a unit u_i are shown in Fig. 3.

If $u_i \in L(u_i)$ then clearly the unit u_i is faulty. Such a unit will be in every AFS. Without loss of generality, we assume in this paper that $u_i \notin L(u_i)$ for any $u_i \in U$.

The following lemmas determine a few properties of AFS's and implied faulty sets.

Lemma 1[4]**:** Given a system S and a syndrome, each of the following statements holds:
(1) for $u_i, u_j \in U$, $u_i \in L(u_j)$ if and only if $u_j \in L(u_i)$,
(2) for $u_i, u_j \in U$, if $a_{ij} = 0$ then $L(u_j) \subseteq L(u_i)$,
(3) if $F \subseteq U$ is an AFS, then $\bigcup_{u_i \in U-F} L(u_i) \subseteq F$.

Q.E.D.

Lemma 2[12]**:** Given a system S and a syndrome, if F_1 and F_2 are AFS's then so is $(F_1 \cup F_2)$.

Q.E.D.

Lemma 3: Given a system S and a syndrome, let $F \subseteq U$ be an AFS containing $u_i \in U$. Then $H_0(u_i) \subseteq F$.

Proof: Suppose that $u_j \in H_0(u_i)$ is not a member of F. Since $u_j \in H_0(u_i)$ there exists a directed path of 0-links from u_j to u_i. Since $u_j \in U - F$ and $u_i \in F$, there exists a 0-link from $U - F$ to F on this path, contradicting the assumption that F is an AFS.

Q.E.D.

For what follows, let $G' = (U', E')$ denote a general, undirected graph.

Definition 3: A subset $K \subseteq U'$ is called a **vertex cover set** (VCS)[14] of G' if every edge in G' is incident to at least one vertex in K. A **minimum vertex cover set** (MVCS) is a VCS of minimum cardinality in G'.

Definition 4: A subset $M \subseteq E'$ is called a **matching**[14] if no vertex in U' is incident to more than one edge in M. A **maximum matching** is a matching of maximum cardinality in G'.

A **bipartite graph**, with bipartition (X, Y), is one whose vertex set can be partitioned into two subsets X and Y such that every edge is incident to a vertex in X and a vertex in Y. Finally, for $u_i \in U'$, $N(u_i)$ denotes the set of all vertices which are adjacent to u_i.

Definition 5[7]**:** A system S is t/s-**diagnosable** if and only if, given a syndrome, all faulty units can be isolated to within a set of at most $s \geq t$ units, provided that the number of faulty units in the system does not exceed t.

It should be observed that a system is trivially t/s-diagnosable if $n = s$. Thus, in this paper, it is required that $0 < t \leq s < n$. It should also be noted that under these conditions $n \geq 2t + 1$ for t/s-diagnosable systems.

3. *T/S*-Characterization: PMC Model

In the PMC model, two distinct fault sets F_1 and F_2 cannot generate a common syndrome if there is a test from the outside into the disjoint union (symmetric difference) of the two sets. For instance, Fig. 4 shows two subsets of a test interconnection graph $G(U, E)$ in which there is a test from the outside into the disjoint union of F_1 and F_2. Thus F_1 and F_2 cannot generate a common syndrome. This condition is both necessary and sufficient to ensure that two distinct subsets do not generate a common syndrome. This observation led to the following characterization by Kohda[15] for t-diagnosable systems.

> A system S with test interconnection graph $G = (U, E)$ under the PMC model is t-diagnosable if and only if for all distinct, nonempty subsets X_i, $X_j \subseteq U$, $|X_i| \leq t$, $|X_j| \leq t$, there is a test from $U - X_i - X_j$ into $X_i \oplus X_j$.

The above approach for characterizing fault sets which generate a common syndrome is used in this section to develop a characterization for a t/s-diagnosable system.

Recall (Sec. 2) that $n \geq 2t + 1$, for a nontrivial t/s-diagnosable system.

Definition 6: Given a system S and a subset $X \subseteq U$, a set $A = \{X_1, \ldots, X_r\}$ is said to be a t-**decomposition** of X if and only if $\bigcup_{1 \leq i \leq r} X_i = X$ and $0 < |X_i| \leq t$ for $1 \leq i \leq r$. The set P_X is the collection of all t-decompositions of X.

Theorem 1: A system S with test interconnection graph $G = (U, E)$ is t/s-diagnosable if and only if for all $X \subseteq U$, $|X| > s$, and for all t-decompositions $A \in P_X$, there exist subsets X_i, $X_j \in A$ such that there is a test from $U - X_i - X_j$ to $X_i \oplus X_j$.

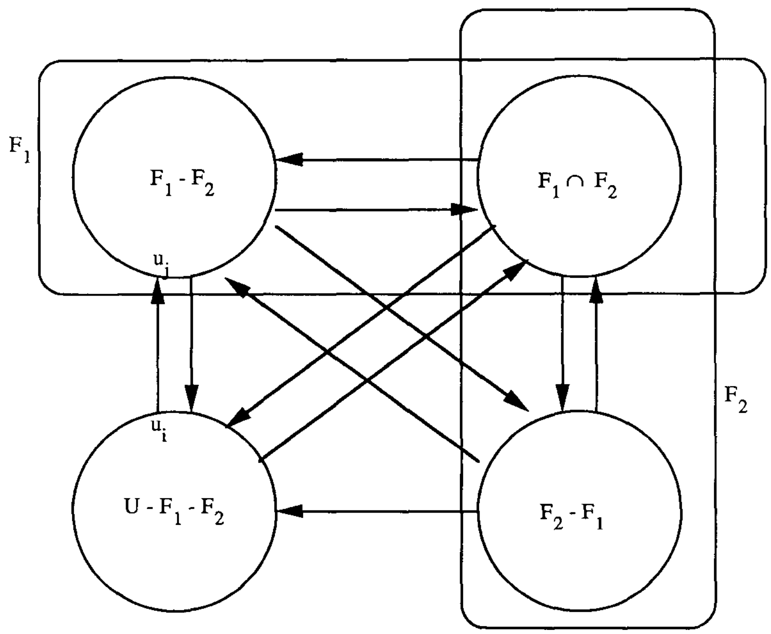


Fig. 4. Two fault sets which cannot generate a common syndrome under the PMC model.

Proof: (Necessity) Assume that the system S is t/s-diagnosable and that the condition of the theorem does not hold. Then there exists $X \subseteq U$ with $|X| > s$ and $A \in P_X$ such that for all $X_i, X_j \in A$ there is no test from $U - X_i - X_j$ to $X_i \oplus X_j$. Consider now the syndrome where for each edge $(u_k, u_l) \in E$ the outcome is defined as follows:

Case 1: $u_k \in U - X$ or $u_l \in U - X$.
<u>Condition 1.1</u>: $u_k, u_l \in U - X$; then set $a_{kl} = 0$.
<u>Condition 1.2</u>: $u_k \in U - X$ and for all $X_i \in A$, $u_l \in X_i$; then set $a_{kl} = 1$.
<u>Condition 1.3</u>: $u_k \in X$ and $u_l \in U - X$; then set $a_{kl} = 0$.

Case 2: $u_k, u_l \in X$.
<u>Condition 2.1</u>: $u_k, u_l \notin X_i$ for some $X_i \in A$; then set $a_{kl} = 0$.
(Note: In this case, there is no subset $X_j \in A$ such that $u_l \in X_j$ and $u_k \notin X_j$. For otherwise, there would be a test from $U - X_i - X_j$ to $X_i \oplus X_j$.)
<u>Condition 2.2</u>: For all $X_i \in A$ either $u_k \in X_i$ or $u_l \in X_i$; then set $a_{kl} = 1$.

Let X_i be a member of A. We show that X_i is an AFS of S for the above syndrome.

Let (u_k, u_l) be an edge in G with $u_k, u_l \in U - X_i$.

(i) If $u_k, u_l \in U - X$ then Condition 1.1 applies and $a_{kl} = 0$.
(ii) If $u_k \in X$ and $u_l \in U - X$, then Condition 1.3 applies and $a_{kl} = 0$.
(iii) If $u_k, u_l \in X$ then by Condition 2.1, $a_{kl} = 0$.

Thus, for an edge (u_k, u_l) with $u_k, u_l \in U - X_i$ $a_{kl} = 0$.

Next let (u_k, u_l) be an edge in G with $u_k \in U - X_i$ and $u_l \in X_i$.

(i) If $u_k \in U - X$ and $u_l \in X_j$ for all X_j, then by Condition 1.2, $a_{kl} = 1$.

(ii) If $u_k \in X$ then, as we have noted before, Condition 2.1 does not occur and so by condition 2.2, $a_{kl} = 1$.

Thus, for an edge (u_k, u_l) with $u_k \in U - X_i$ and $u_l \in X_i$, $a_{kl} = 1$.

From the above, it follows that X_i is an allowable fault set.

Since X_i is an arbitrary member of A, it follows that, for the above syndrome, each $X_i \in A$ is an allowable fault set of size less than or equal to t. Since the union of all these allowable fault sets is X and $|X| > s$, no subset of units of U of size at most s can isolate the faulty units for the above syndrome. Hence S is not t/s-diagnosable, a contradiction.

(Sufficiency). Proof is given by using a contrapositive argument. Assume S is not t/s-diagnosable. Then there exists a syndrome, say θ, and subsets $X_1, X_2, \ldots, X_m$ of cardinality at most t such that these subsets are allowable fault sets with respect to θ and that $|X| > s$, where X is the union of $X_1, X_2, \ldots, X_m$.

Suppose that for some pair X_i, X_j, $1 \leq j < k \leq m$ there is a test from $U - X_i - X_j$ to $X_i \oplus X_j$. Let (u_k, u_l) be such a test edge. Without loss of generality, let $u_l \in X_i$. If X_i is the fault set then the test outcome $a_{kl} = 1$; if X_j is the fault set then $a_{kl} = 0$. This contradicts the assumption that both X_i and X_j are allowable fault sets for θ. This shows that the condition of the theorem is not satisfied.

Q.E.D.

4. Basic Properties of Allowable Fault Sets

Our approach to t/s-diagnosis is first to develop an efficient test to determine whether a vertex v of a t/s-diagnosable system is an AFS of cardinality at most t. The set of all vertices which satisfy this property will be the required isolating faulty units. This is ensured from Lemma 2. With this objective in mind we first present in this section several properties of AFS's in a t/s-diagnosable system. Our investigations in this chapter are based on the notions of the implied-fault set and the implied-fault graph used by Dahbura and Masson[4] in their study.

Given a syndrome for a system S, define the **implied-fault graph** $G^* = (U^*, E^*)$ to be an undirected graph such that $U^* = U$ and $E^* = \{(u_i, u_j) : u_i \in L(u_j)\}$. Recall that $L(u_i)$ is the set of all units of S that may be deduced to be faulty under the assumption that u_i is fault-free and that $H_0(u_i)$ corresponds to the set $A_0(u_i) \cup \{u_i\}$ where $A_0(u_i)$ is the set of 0-ancestors of $\{u_i\}$. For $u \in U$, let G_u^* denote the subgraph of G^* obtained after all units in $H_0(u)$ and all edges incident on these units have been removed from G^*. Let K_u represent an MVCS of G_u^* and let $G - H_0(u)$ denote the subgraph of G where all vertices in $H_0(u)$ along with all edges incident on these vertices have been removed from G. These concepts are illustrated in Fig. 5 for the test interconnection graph and the syndrome shown in Fig. 2. Finally, we define $G^*(F)$ to be the subgraph of G^* such that all edges which connect vertices entirely inside F have been deleted.

Note that if $u_i \in L(u_i)$ then u_i can immediately be identified as faulty. Thus we assume that $u_i \notin L(u_i)$ for any $u_i \in U$. This means that G^* has no self-loops.

The results of the following lemma can be found in Ref. 4.

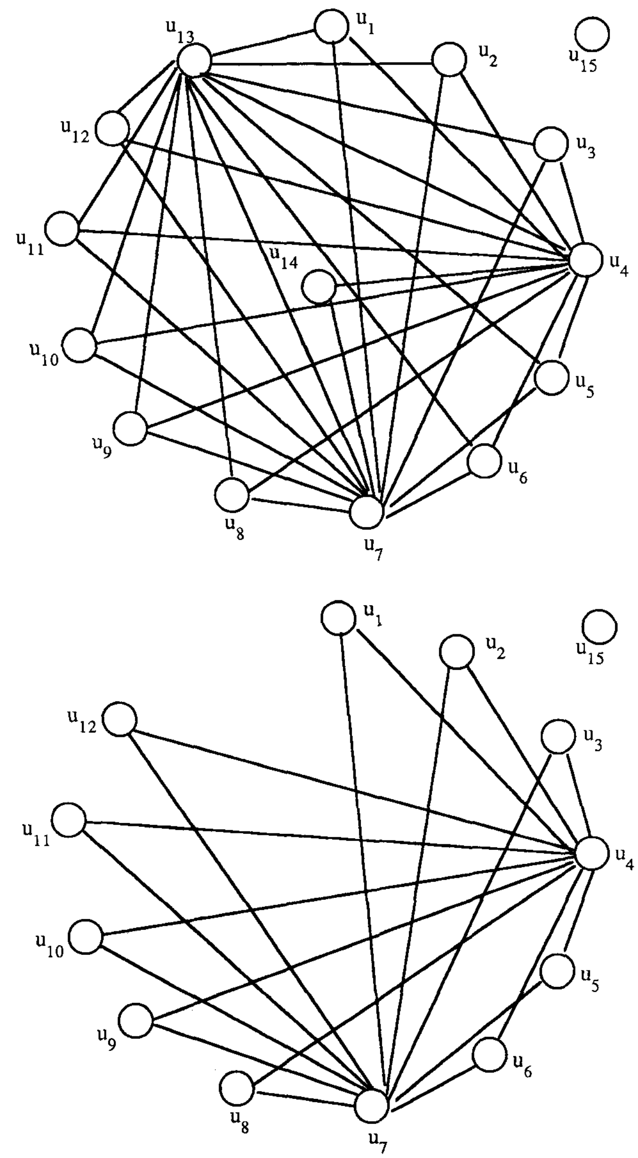


Fig. 5. Implied fault graphs G^* and $G^*_{u_{14}}$.

Lemma 4: Given a syndrome for a system S, we have the following:
(i) Every AFS of G is a VCS of G^*.
(ii) If $F \subseteq U$ is a minimal VCS of G^*, then F is an AFS of G.
(iii) $F \subseteq U$ is an MAFS of G if and only if F is an MVCS of G^*.

Lemma 5: F is an AFS in G of minimum cardinality containing unit v if and only if $H = F - H_0(v)$ is an MAFS of $G - H_0(v)$.

Proof: (Necessity) We first show that H is an AFS of $G - H_0(v)$. Since $U - F = (U - H_0(v)) - H$ and F is an AFS of G all edges within $(U - H_0(v)) - H$ are 0-links and all edges from $(U - H_0(v)) - H$ into H are 1-links. Hence H is an AFS of $G - H_0(v)$. To show that H is an MAFS of $G - H_0(v)$, assume H_1 is an AFS of $G - H_0(v)$. Clearly all edges with both vertices incident on vertices in $(U - H_0(v)) - H_1$ are 0-links and all edges from $U - H_0(v) - H_1$ into H_1 are 1-links. Now consider edges from $(U - H_0(v)) - H_1$ into $H_0(v)$. These edges must all be 1-links, otherwise the vertices incident on these edges would all belong to $H_0(v)$. This shows that the set $H_1 \cup H_0(v)$ is an AFS of G. Hence if $|H_1| < |H|$ then $H_1 \cup H_0(v)$ is an AFS of smaller cardinality than F, contradicting the fact that F is an AFS of minimum cardinality containing v. Hence $|H_1| \geq |H|$ and H is an MAFS of $G - H_0(v)$.

(Sufficiency) If $F - H_0(v)$ is an MAFS of $G - H_0(v)$ then as we have shown in the proof of necessity, F is an AFS of G. If F is not an AFS in G of minimum cardinality containing v, then let F_1 be an AFS of G containing v with $|F_1| < |F|$. But then $F_1 - H_0(v)$, from the necessity part, would be an AFS of $G - H_0(v)$ of smaller cardinality than $F - H_0(v)$, a contradiction.

Lemma 6: For $v \in U$, $(G - H_0(v))^* = G_v^*$.

Proof: Since the vertex sets of both graphs are the same, we need only show that the edge sets are identical. Clearly every edge in $(G - H_0(v))^*$ is in G_v^*. Now assume that there is an edge (u_i, u_j) in G_v^* which is not in $(G - H_0(v))^*$. Then every implied-fault path in G between u_i and u_j must contain at least one vertex from $H_0(v)$. But this implies that either u_i or u_j is a member of $H_0(v)$, contradicting the assumption that both vertices are members of $G - H_0(v)$. Hence the two edge sets are also identical.

Q.E.D.

Lemma 7: Given a syndrome for a system S, let $F \subseteq U$ be an AFS containing $v \in U$. Then $F - H_0(v)$ is a VCS of G_u^*.

Proof: Let $F_1 = F - H_0(v)$. From Lemma 3 and the proof of Lemma 6, it follows that F_1 is an AFS of $G - H_0(v)$. Then from Lemma 5, F_1 is a VCS of $(G - H_0(v))^*$. Thus, by Lemma 7, F_1 is a VCS of G_v^*.

Q.E.D.

Theorem 2: Given a syndrome for a system S, F is an AFS of minimum cardinality among all allowable fault sets that contain unit $u \in U$ if and only if $F - H_0(v)$ is an MVCS of G_v^*.

Proof: Proof follows from Lemmas 5, 6 and 7.

The condition in the above theorem can be used to test if a unit belongs to an AFS of cardinality at most t for a given syndrome. However this condition requires determining an MVCS for a general undirected graph. But the associated decision problem, the Vertex Cover Problem, is known to be NP-Complete. So, we would like to develop a test which requires determining an MVCS of a bipartite graph. With this objective in mind, we now define a bipartite graph for each vertex v. This bipartite graph is derived from G_v^*. We then relate an MVCS of this graph to an AFS containing vertex v and establish certain properties of this AFS which will be used in the following sections to develop appropriate diagnosis algorithms.

Given a system S and a syndrome, define $B = (U_B, E_B)$ to be the undirected bipartite graph with bipartition (X, Y) where

$$X = \{x_1, \ldots, x_n\}, \qquad Y = \{y_1, \ldots, y_n\}$$

and

$$E_B = \{(x_i, y_j) : u_i \in L(u_j) \text{ in S}\}.$$

For $v \in U$, define the undirected bipartite graph $B_v = (U_v, E_v)$ with bipartition (X_v, Y_v) to be the vertex induced subgraph of B such that

$$X_v = \{x_i : u_i \in U - H_0(v)\},$$

$$Y_v = \{y_i : u_i \in U - H_0(v)\}.$$

Figure 6 illustrates these concepts for the test interconnection graph and the syndrome given in Fig. 2. For each vertex v in G, let

$$t_v = t - |H_0(v)|,$$

and

$$U_v = U - H_0(v).$$

Theorem 3: Given a syndrome for a system S, a unit $v \in U$ does not belong to any AFS of cardinality at most t if B_v has an MVCS of cardinality greater than $2t_v$.

Proof: Let the cardinality of an MVCS of B_v be greater than $2t_v$. Assume $v \in U$ belongs to an AFS F such that $|F| \leq t$. Let $H = F - H_0(v)$. Clearly $|H| \leq t_v$. Define $B_X(H) = (U_X, E_X)$ to be the vertex induced subgraph of B_v, where

$$U_X = \{x_i : u_i \in H\} \cup \{y_i : u_i \in U_v - H\}.$$

$B_Y(H) = (U_Y, E_Y)$ is defined to be the vertex induced subgraph of B_v, where

$$U_Y = \{x_i : u_i \in U_v - H\} \cup \{y_i : u_i \in H\}.$$

Clearly $F_X = \{x_i : u_i \in H\}$ and $F_Y = \{y_i : u_i \in H\}$ are VCS's of $B_X(H)$ and $B_Y(H)$ respectively. It follows that $F_B = F_X \cup F_Y$ is a VCS of $B_X(H) \cup B_Y(H)$. Since F is an AFS, in G^* there are no edges connecting vertices of $U - F$. From this it follows that every edge in B_v connects vertices in F_B. Therefore F_B is a VCS of B_v, contradicting our

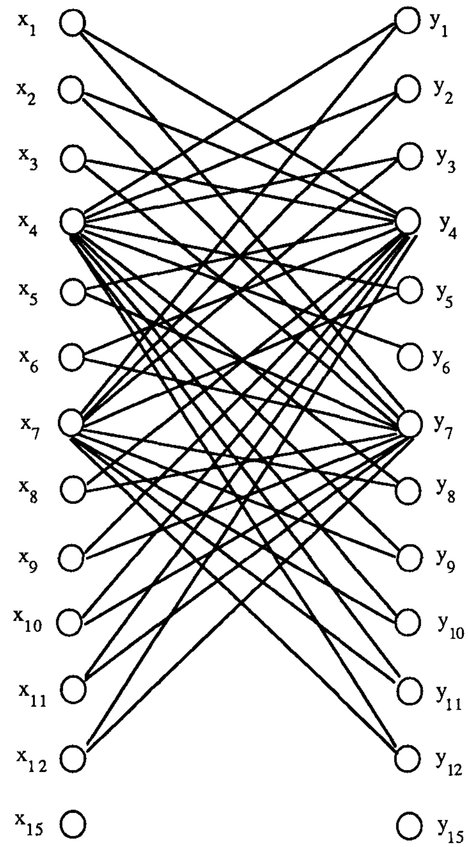


Fig. 6. Bipartite graph corresponding to $G^*_{u_{14}}$.

assumption that the cardinality of an MVCS of B_v is greater than $2t_v$. Hence v is not contained in any AFS of cardinality at most t.

Q.E.D.

We have shown in Ref. 13 that in the case of $t/t+1$-diagnosable systems the condition of the above theorem is also necessary for a vertex not to be in an AFS of cardinality at most t. Unfortunately this condition is not necessary for $t/t+k$-diagnosable systems when $k > 1$. To develop an efficient $t/t+k$-diagnosis algorithm when $k > 1$ we carry out a further study of an MCVS of B_v.

In the following we use $F_B(v)$ to denote an MVCS of B_v. For a given $F_B(v)$ let

$$F_I = \{u_i \mid x_i \in F_B(v) \text{ and } y_i \in F_B(v)\}$$

and

$$F_v = \{u_i \mid x_i \in F_B(v) \text{ or } y_i \in F_B(v)\}.$$

We now proceed to establish certain properties of F_v.

Lemma 8: $F_v \cup H_0(v)$ is an AFS of G.

Proof: Assume the contrary. Then at least one of the following conditions is satisfied.
(a) There exist $u_i, u_j \in U - F_v - H_0(v)$ with $a_{ij} = 1$.
(b) There exist $u_j \in F_v \cup H_0(v)$ and $u_i \in U - (F_v \cup H_0(v))$ with $a_{ij} = 0$.

Assume (a) holds. Then the edge (u_i, u_j) is in G_v^*. Hence (x_i, y_j) is an edge in B_v. But this contradicts the fact that $F_B(v)$ is a VCS of B_v since neither x_i nor y_j is a member of $F_B(v)$.

Now assume (b) holds and (a) does not hold. Clearly $u_j \notin H_0(v)$; for otherwise u_i would also belong to $H_0(v)$. Thus $u_j \in F_v$. Hence either x_j or y_j is a member of $F_B(v)$. Without loss of generality let $x_j \in F_B(v)$. Since $F_B(v)$ is an MVCS of B_v, there exists y_k in B_v with $y_k \notin F_B(v)$ such that (x_j, y_k) is an edge in B_v. Hence $u_j \in L(u_k)$. Since $a_{ij} = 0$, $u_i \in L(u_k)$. Hence (x_i, y_k) is an edge in B_v. Since neither x_i nor y_k is a member of $F_B(v)$, this contradicts the fact that $F_B(v)$ is a VCS of B_v.

Q.E.D.

Lemma 9: Given a syndrome for a system S and a unit $v \in U$, we have the following:
(i) In G^*, there is no edge (u_i, u_j) with $u_i \in U - (F_v \cup H_0(v))$ and $u_j \in F_v - F_I$.
(ii) In G, there is no edge (u_i, u_j) with $u_i \in U - (F_v \cup H_0(v))$ and $u_j \in F_v - F_I$.

Proof: (i) Assume the contrary. Let (u_i, u_j) be an edge from $U - (F_v \cup H_0(v))$ into $F_v - F_I$ in G^*. Then either x_j or y_j is not a member of $F_B(v)$. Thus in B_v either the edge (x_i, y_j) or the edge (x_j, y_i) is not incident on any vertex in $F_B(v)$, contradicting the fact that $F_B(v)$ is a VCS of B_v.
(ii) By Lemma 8, the set $F_v \cup H_0(v)$ is an AFS of G. Thus every edge from $U - (F_v \cup H_0(v))$ into $F_v - F_I$ in G must be a 1-link. So if such an edge (u_i, u_j) exists in G, then (u_i, u_j) is an edge in G^*. Thus from (i) it follows that there is no edge (u_i, u_j) in G with $u_i \in U - (F_v \cup H_0(v))$ and $u_j \in F_v - F_I$.

Q.E.D.

Lemma 10: Every AFS of G contained in $F_v \cup H_0(v)$ contains the subset F_I.

Proof: To show that every AFS of G contained in $F_v \cup H_0(v)$ contains the subset F_I it suffices to show that every VCS of G^* contained in $F_v \cup H_0(v)$ contains F_I. The above assertion holds if every vertex in F_I is incident on some vertex of $U - (F_v \cup H_0(v))$ in G^*. Assume the contrary. Let u_k be a vertex in F_I which is not incident on any vertex of the set $U - (F_v \cup H_0(v))$. Then let $W_B(v) = \{x_i | u_i \in F_v\} \cup \{y_i | u_i \in F_I - \{u_k\}\}$. From Lemma 9(i) and the construction of B_v it follows that in B_v, there is no edge (x_i, y_j) with $u_i \in U - (F_v \cup H_0(v))$ and $u_j \in F_v - F_I$. So $W_B(v)$ is a VCS of B_v. But $|W_B(v)| = |F_B(v)| - 1$. This contradicts the assumption that $F_B(v)$ is an MVCS of B_v. Thus every vertex in F_I is incident on some vertex of $U - (F_v \cup H_0(v))$ in G^*. This implies that every VCS of G^* contained in $F_v \cup H_0(v)$ contains the subset F_I. By Lemma 4, it follows that every AFS of G contained in $F_v \cup H_0(v)$ contains the subset F_I.

Q.E.D.

5. Diagnosis of a $t/t + k$-Diagnosable System

In this section we first show that the set $F_v \cup H_0(v)$ indeed contains an AFS of cardinality at most t if such an AFS is present in the system. We also show that no such AFS will be present if $|F_v| > t_v + k$. Thus the search for an AFS of cardinality at most t containing vertex v need be confined to a set of cardinality at most $t_v + k$. This leads to a $t/t + k$-diagnosis algorithm which is polynomial for each fixed integer k.

Theorem 4: $F_v \cup H_0(v)$ contains an AFS F_1 containing unit v such that for every AFS F_2 of G containing unit v, $|F_1| \leq |F_2|$.

Proof: Let F_1 be an AFS of smallest cardinality containing unit v such that $F_1 \subseteq F_v \cup H_0(v)$. Assume F_2 to be an AFS of G containing unit v. Let $F_3 = (F_v - F_1) \cup (F_1 \cup H_0(v))$ where $F_I = \{u_i | x_i$ and y_i both belong to $M_v\}$. We observe that $F_I \cup H_0(v) \subseteq F_1$, since every AFS of G containing v in $F_v \cup H_0(v)$ contains $F_I \cup H_0(v)$.

First we note that since F_1 and F_2 are VCS's of G^*, there are no edges in the subgraphs of G^* induced by the vertex sets $U - F_1$ and $U - F_2$. Also, by Lemma 9(i), for every edge in G^* with one vertex in $U - F_1 - F_3$, the other vertex is in $F_1 \cap F_3$. From these facts we conclude that $((F_3 \cap F_2) - F_1) \cup ((F_3 \cup F_2) \cap F_1)$ is a VCS of G^*. The shaded area in Fig. 7(a) corresponds to this VCS which lies entirely within $F_v \cup H_0(v)$.

We now claim that the following inequality holds (See Fig. 7(b)):

$$|(F_3 \cap F_2) - F_1| \geq |F_1 - F_2 - F_3|. \tag{1}$$

Assume (1) is not true. Then the VCS $((F_3 \cap F_2) - F_1) \cup ((F_3 \cup F_2) \cap F_1)$ is of smaller cardinality than F_1 and so by Lemma 4(ii) it contains an AFS of G of cardinality smaller than F_1, a contradiction.

By Lemma 9(i), in B_v for every edge (x_i, y_j) with $u_i \in U - F_1 - F_2 - F_3$, the vertex u_j is in $F_1 \cap F_3$ since $F_I \cup H_0(v) = F_1 \cap F_3$. From this and the fact that F_2 is a VCS of G^*, it follows that in B_v for every edge (x_i, y_j) with $u_i \in U - F_1 - F_2 - F_3$ the vertex u_j is in $F_1 \cap F_2 \cap F_3 - H_0(v)$. So the set

$$F_a = \{x_i | u_i \in (F_1 \cup F_2 \cup F_3) - H_0(v)\} \cup \{y_i | u_i \in (F_1 \cap F_2 \cap F_3) - H_0(v)\}$$

is a VCS of B_v.

We claim that the following inequality also holds (See Fig. 7(c)):

$$|F_2 - F_1 - F_3| \geq |(F_3 \cap F_1) - F_2|. \tag{2}$$

If (2) is not true, then $|F_a| < |F_B(v)|$ because (See Fig. 7(d)) $|F_B(v)| - |F_a| = |(F_3 \cap F_1) - F_2| - |F_2 - F_1 - F_3| > 0$, contradicting the fact that $F_B(v)$ is an MVCS of B_v.

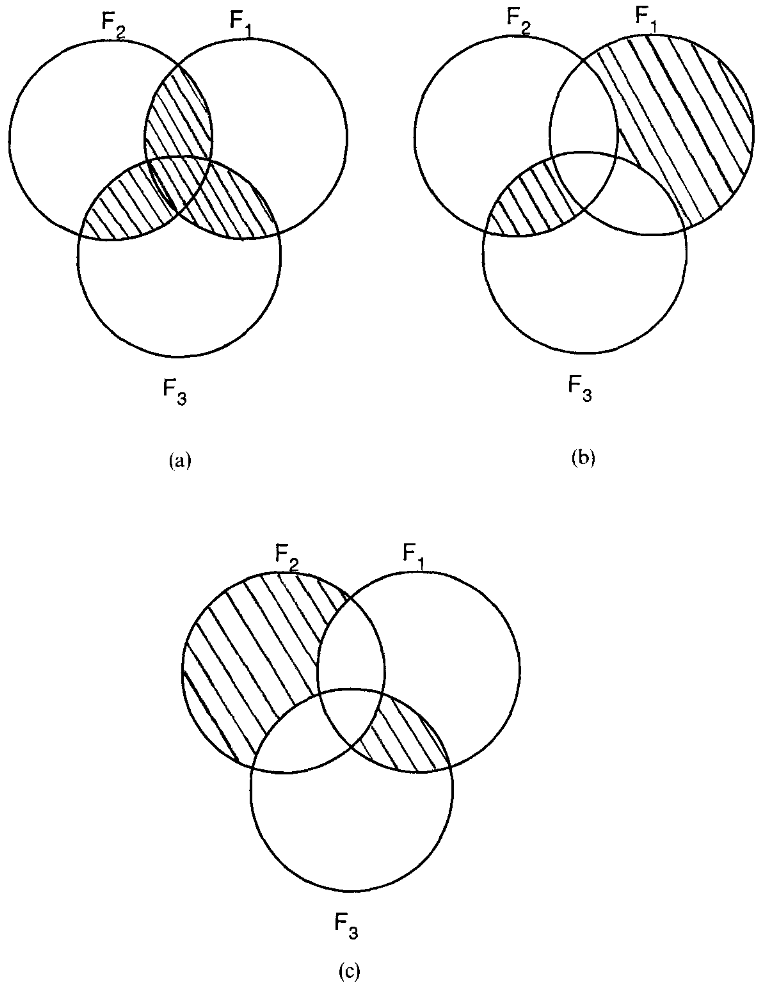


Fig. 7. Illustrations for Theorem 4.

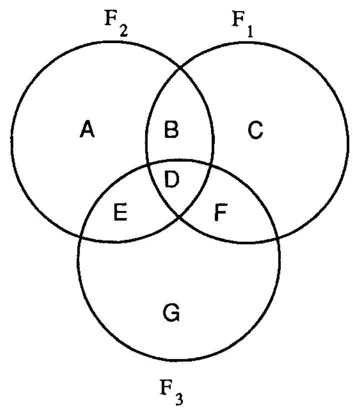
Thus (1) and (2) are true. But this implies that $F_2| \geq F_1|$. It follows that the set F_1 contained in $F_v \cup H_0(v)$ is a smallest AFS containing v.

Q.E.D.

Theorem 5: Given a syndrome for a $t/t + k$ system S, if $|F_v| > t_v + k$ for some unit $v \in U$, then G does not have an AFS of cardinality at most t containing v.

Proof: Assume the contrary. Let F_1 be an AFS of smallest cardinality contained in $F_v \cup H_0(v)$ of which v is a member. From Theorem 4, F_1 is an AFS of smallest cardinality of which v is a member. Thus $|F_1| \leq t$. Let $F_2 = (F_v \cup H_0(v)) - (F_1 - F_I - H_0(v))$. We claim that $|F_2| \leq |F_1|$. For otherwise, the set

$$M = \{x_i | u_i \in F_1 - H_0(v)\} \cup \{y_i | u_i \in F_1 - H_0(v)\}$$



(d)

$$|F_a| = |A| + |B| + |C| + 2|D| + |E| + |F| + |G| - 2H_0(v)$$

$$|F_{B(v)}| = |B| + |C| + 2|D| + |E| + 2|F| + |G| - 2H_0(v)$$

Fig. 7. (*Continued*)

would be a vertex cover of B_v and since $|M| < |F_B(v)|$, this would contradict the minimality of $|F_B(v)|$. Hence $|F_2| \leq |F_1| \leq t$.

Consider the two sets F_1 and F_2. $|F_1| \leq t$, $|F_2| \leq t$ and $|F_1 \cup F_2| > t + k$. Since all edges from $U - F_v - H_0(v)$ into $F_v \cup H_0(v)$ are incident on $F_I \cup H_0(v)$, there is no test from $U - F_1 - F_2$ into $F_1 \oplus F_2$. This contradicts the assumption that the system is $t/t + k$-diagnosable.

Q.E.D.

Our diagnosis algorithm for isolating all faulty units in a $t/t + k$-diagnosable system is as follows. For each v, we determine a maximum matching K_v of B_v. If $|K_v| > 2t_v$ then, by Theorem 3, v does not belong to any AFS of cardinality at most t. Otherwise we determine from K_v an MVCS $F_B(v)$ of B_v. We then construct F_v and F_I. If $F_v \leq t_v$ then v is in an AFS of cardinality at most t. If not, we check if F_v contains a VCS of cardinality at most t_v. We do so by taking all possible subsets W of F_v of cardinality equal to t_v with $F_I \subseteq W$ and examining if W is a VCS of the subgraph induced on G_v^* by the vertex set F_v. A formal description of the algorithm is given below.

Algorithm 1: $t/t + k$-Diagnosis

Step 1: Given a $t/t + k$-diagnosable system S and a syndrome, construct the bipartite graph $B = (U_B, E_B)$ with bipartition (X, Y).

Step 2: Set $F = \phi$; for all $v \in U$, label v unmarked.

Step 3: **While** there exists an unmarked $v \in U$
begin

Step 3.1: Label v marked
Step 3.2: Set $t_v = t - |H_0(v)|$.
Step 3.3: Construct B_v from B.
Step 3.4: Compute a maximum matching K_v of B_v using the Hopcroft/Karp algorithm.[16]
Step 3.5: **If** $|K_v| \leq 2t_v$ **then**
begin
Compute an MVCS $F_B(v)$ of B_v from K_v using the König Construction Technique.[14]
Determine F_v and F_I from $F_B(v)$.
If $|F_v| \leq t_v$ **then** add v to F
else if $|F_v| \leq t_v + k$ **then**
For each subset W with $F_I \subseteq W$ and $W = t_v$ check if W is a VCS of the subgraph induced on G^* by the vertex set F_v. If so, add v to F.
end
end
Step 4: **If** $|F| \leq s$ **then** F is the required set.

The correctness of the above algorithm follows from Theorems 3, 4 and 5.

Regarding complexity of this algorithm, the bipartite graph in Step 1 can be constructed in $O(n^{2.5})$ operations.[4] Computations in Steps 3.1–3.4 is dominated by the computation of a maximum matching in a bipartite graph which is of $O(n^{2.5})$. Step 3.5 may require computing all subsets of F_v of cardinality equal to t_v and testing each of them for the required VCS property. This step may require $|E|C_{t_v}^{|F_v|}$ operations. Note that $|F_v| \leq t_v + k$. Since $C_{t_v}^{|F_v|} = O(t_v^k)$ and $t_v < t$, the overall complexity of the algorithm is $O(n^{3.5} + mnt^k)$.

Note that if, in the above algorithm, a unit v is included in the set F then all units in $F_I \cup H_0(v)$ can also be added to F. So for these units, we do not need to perform Step 3 separately. Though, by doing so, we may reduce the number of computations, it will not affect the overall complexity of the algorithm.

Given a valid syndrome, if an AFS does not contain v, then it must contain $L(v)$, the set of units implied faulty when v is implied to be fault-free. Then by Theorem 3, a unit v does not belong to an AFS of cardinality at most t if the bipartite graph $B_{L(v)}$, the subgraph induced on B when vertices corresponding to $L(v)$ have been removed, contains an MVCS of cardinality at most $2(t - L(v))$. Using this we can modify Algorithm 1 to identify all units which belong to every AFS of cardinality at most t. The following is a formal description of such an algorithm.

Algorithm 2:

Step 1: Given a $t/t + k$-diagnosable system S with test interconnection graph $G = (U, E)$ and a syndrome arising from a t-fault situation, construct G^* and remove all vertices with self-loops. From the resulting graph, construct the bipartite graph $B = (U_B, E_B)$ with bipartition (X, Y).

Step 2: Set $F = \phi$; for all $v \in U$, label v unmarked.
Step 3: **While** there exists an unmarked $v \in U$
begin
Step 3.1: Label v marked.
Step 3.2: Set $t_{L(v)} = t - |L(v)|$.
Step 3.3: Construct $B_{L(v)}$ from B.
Step 3.4: Compute a maximum matching $K_{L(v)}$ of $B_{L(v)}$ using the Hopcroft/Karp algorithm.[16]
Step 3.5: **If** $|K_{L(v)}| > 2t_{L(v)}$ **then** add v to F.
else
begin
Compute an MVCS $F_B(v)$ of $B_{L(v)}$ from $K_{L(v)}$ using the König Construction Technique.[14]
Determine F_v and F_I from $F_B(v)$.
If $|F_v| > t_{L(v)} + k$ **then** add v to F
else if $|F_v| > t_{L(v)}$ **then**
For each subset W with $F_I \subseteq W$ and $W = t_{L(v)}$ check if W is a VCS of the subgraph induced on G^* by the vertex set F_v. If not add v to F.
end
end
Step 4: F is the required set of units which lie in every AFS of cardinality at most t.

Thus for a $t/t + k$-diagnosable system not only can all faulty units be isolated to within at most $t + k$ faulty units, but also all units which lie in every AFS of cardinality at most t can be identified in polynomial time for every fixed positive integer k. The units of the set F obtained by the algorithm given above can be correctly identified to be faulty. Note that if a $t/t + k$-diagnosable system is not sequentially t-diagnosable then the set F produced by the above algorithm may be empty.

6. On the Diagnosis of a Sequentially t-Diagnosable System

Recall that (Sec. 1) a system is sequentially t-diagnosable if and only if given any syndrome there exists a unit v which is present in every allowable fault set of cardinality at most t. Algorithm 2 of the previous section can easily be modified to arrive at an algorithm for diagnosis of a sequentially t-diagnosable system. The only modification required is to substitute t for k. The complexity of this algorithm can be shown to be $O(n^{3.5} + mnt^t)$.

7. Conclusions

In this paper we have studied the problem of diagnosing t/s-diagnosable systems. We have presented a $t/t + k$-diagnosis algorithm which runs in polynomial time for each fixed integer k. We have also shown how this algorithm can be modified to design an algorithm for identifying all units which lie in every AFS of cardinality at most t of a $t/t + k$ diagnosable system. These units can then be correctly identified as faulty. We then presented an approach for diagnosing a sequentially t-diagnosable system. This approach leads to an algorithm which is of complexity $O(n^{3.5} + mnt^t)$. The t/t-diagnosis algorithm of Ref. 10, the $t/t + 1$-diagnosis algorithm of Refs. 13, 17 and the $t/t + k$-diagnosis algorithm of this paper complement the corresponding $t/t + k$-diagnosability algorithms of Sullivan.[11] It might be possible to improve the complexity of this algorithm using the characterizations and properties of sequentially t-diagnosable systems developed in Refs. 12, 18.

References

1. F. P. Preparata, G. Metze, and R. T. Chien, "On the connection assignment problem of diagnosable systems", *IEEE Trans. Elect. Comput.* **EC-16** (1967) 848–854.
2. S. L. Hakimi, and A. Amin, "Characterization of the connection assignment of diagnosable Systems," *IEEE Trans. Comput.* **C-23** (1974) 86–88.
3. G. F. Sullivan, "A polynomial time algorithm for fault diagnosability", in *Proc. 25th Ann. Symp. Foundations Computer Science*, Oct. 1984, pp. 148–156.
4. A. T. Dahbura, and G. M. Masson, "A practical variation of the $O(n^{2.5})$ fault diagnosis algorithm", in *14th Int. Symp. Fault-Tolerant Computing*, 1984.
5. G. F. Sullivan, "An $O(t^3 + |E|)$ fault identification algorithm for diagnosable systems", *IEEE Trans. Comput.* **C-37** (1988) 388–397.
6. A. K. Somani, D. Avis, and V. K. Agarwal, "A generalized theory for system-level diagnosis", *IEEE Trans. Comput.* **C-36** (1987) 538–546.
7. A. D. Friedman, "A new measure of digital system diagnosis", in *Dig. 1975 Int. Symp. Fault-Tolerant Computing*, June 1975, pp. 167–170.
8. A. Kavianpour, and A. D. Friedman, "Efficient design of easily diagnosable systems", in *Proc. 3rd USA-Japan Computing Conf.*, 1978, pp. 251–257.
9. K. Y. Chwa, and S. L. Hakimi, "On fault identification in diagnosable systems", *IEEE Trans. Comput.* **C-30** (1981) 414–422.
10. C. L. Yang, G. M. Masson, and R. A. Leonetti, "On fault identification and isolation in t_1/t_1-diagnosable systems", *IEEE Trans. Comput.* **C-35** (1986) 639–643.
11. G. Sullivan, "The complexity of system-level fault diagnosis and diagnosability", Ph. D. Dissertation, Yale University, 1986.
12. V. Raghavan, "Diagnosability issues in multiprocessor systems", Ph. D. Dissertation, University of Minnesota, 1989.
13. A. Das, K. Thulasiraman, V. K. Agarwal and K. B. Lakshmanan, "t/s-diagnosable systems: a characterization and diagnosis algorithm", *15th Int. Conf. on Graph-Theoretic Concepts in Computer Science*, Rolduc, Holland.
14. J. A. Bondy, and U. S. R. Murty, *Graph Theory with Applications*, Elsevier North-Holland, New York, 1976.
15. T. Kohda, "On one-step diagnosable systems containing at most t-faulty units", *Syst. Comput. Controls* **9** (1978) 30–37.
16. J. E. Hopcroft, and R. M. Karp, "A $n^{2.5}$ algorithm for maximum matching in bipartite graphs", *SIAM J. Comput.* **2** (1973).
17. A. Das, "Diagnosability and diagnosis of sparsely interconnected multiprocessor systems", Ph. D. Dissertation, Concordia University, Montreal, 1989.
18. S. Huang, J. Xu, and T. Chen, "Characterization and design of sequentially t-diagnosable systems", in *Dig. 19th Int. Symp. Fault-Tolerant Computing*, June 1989, pp. 554–559.