SIAM J. COMPUT.
Vol. 23, No. 5, pp. 895–905, October 1994

DIAGNOSIS OF $t/(t+1)$-DIAGNOSABLE SYSTEMS*

A. DAS†, K. THULASIRAMAN‡, AND V. K. AGARWAL§

Abstract. A classic PMC (Preparata, Metze, and Chien) multiprocessor system [F. P. Preparata, G. Metze, and R. T. Chien, IEEE Trans. Electr. Comput., EC-16 (1967), pp. 848–854] composed of n units is said to be $t/(t+1)$ diagnosable [A. D. Friedman, *A new measure of digital system diagnosis*, in Dig. 1975 Int. Symp. Fault-Tolerant Comput., 1975, pp. 167–170] if, given a syndrome (complete collection of test results), the set of faulty units can be isolated to within a set of at most $t+1$ units, assuming that at most t units in the system are faulty. This paper presents a methodology for determining when a unit v can belong to an allowable fault set of cardinality at most t. Based on this methodology, for a given syndrome in a $t/(t+1)$-diagnosable system, the authors establish a necessary and sufficient condition for a vertex v to belong to an allowable fault set of cardinality at most t and certain properties of $t/(t+1)$-diagnosable systems. This condition leads to an $O(n^{3.5})t/(t+1)$-diagnosis algorithm. This $t/(t+1)$-diagnosis algorithm complements the $t/(t+1)$-diagnosability algorithm of Sullivan [*The complexity of system-level fault diagnosis and diagnosability*, Ph.D. thesis, Yale University, New Haven, CT, 1986].

Key words. fault diagnosis, fault isolation, PMC models, test assignment, graph algorithms, vertex cover sets

AMS subject classifications. 68M15, 68R10

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 classic 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]. Subsequently, Raghavan [4] improved on this result by presenting an algorithm that runs in $O(nt^{2.5})$ time. Dahbura and Masson [5] 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 [6].

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. 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 $n^*\lceil (t+1)/2\rceil$ 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 [10] presented a polynomial time algorithm

*Received by the editors September 4, 1990; accepted for publication (in revised form) April 18, 1993.

†Departement d'informatique et de recherche operationelle, Université de Montréal, Montreal, Quebec, Canada.

‡Department of Electrical and Computer Engineering, Concordia University, Montreal, Quebec, Canada.

§Department of Electrical and Computer Engineering, McGill University, Montreal, Quebec, Canada.

for the t/t-diagnosability problem, and Yang, Masson, and Leonetti [11] presented an $O(n^{2.5})$ algorithm for the t/t-diagnosis problem. Sullivan also presented in [10] a polynomial time $t/(t+1)$-diagnosability algorithm based on a characterization of $t/(t+1)$-diagnosable systems also developed in [10].

The objective of this work is to develop an efficient diagnosis algorithm for $t/(t+1)$-diagnosable systems. The paper is organised as follows. In §2, we present certain basic definitions, notations, and results. With the objective of determining an effecient test for a vertex v to be in an allowable fault set of cardinality at most t, we then establish in §3 several properties of allowable fault sets and present a methodology for determining when a unit v belongs to an allowable fault set of cardinality at most t. Using these properties and certain properties of $t/(t+1)$-diagnosable systems, we develop in §4 a necessary and sufficient condition for a vertex v to belong to an allowable fault set of cardinality at most t. This leads to an $O(n^{3.5})$ algorithm for diagnosis of a $t/(t+1)$-diagnosable system. The work presented here is a revised version of our earlier paper [12].

2. Preliminaries. A multiprocessor system S consists of n units or processors, denoted by the set $U = \{u_1, u_2, \dots, u_n\}$. Each unit is assigned a subset of other units for testing. Thus the test interconnection 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 (respectively, 0) if u_i evaluates unit u_j to be faulty (respectively, fault free). Since all faults considered are permanent, the test outcome a_{ij} is reliable if and only if unit u_i is fault free. The collection of all test results over the entire system is referred to as a *syndrome*. If $a_{ij} = 0$ (respectively, 1) then u_i is said to have a 0-link (respectively, 1-link) to u_j and u_j is said to have a 0-link (respectively, 1-link) from u_i.

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

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

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 denote the set

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

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

DEFINITION 1 [5]. *Given a system* S *and a syndrome, a subset $F \subseteq U$ is an* allowable fault set (AFS) *if and only if*

1. $u_i \in (U - F)$ *and* $a_{ij} = 0$ *imply* $u_j \in (U - F)$, *and*
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. A *minimum allowable fault set* (MAFS) is an allowable fault set of minimum cardinality.

DEFINITION 2 [5]. *Given a system* S *and a syndrome, the* implied-fault 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.*

It follows that

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

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. This observation motivates the definition of an *implied-fault path* between u_i and u_j.

DEFINITION 3. *Given a system* S *and a syndrome, a path P between u_i and u_j is an* implied-fault path *if there exist units u_k and u_l on P such that the following are satisfied.*

(i) *All the links of P that lie between u_i and u_k constitute a directed path of* 0*-links from u_i to u_k.*

(ii) *All the links of P that lie between u_j and u_l constitute a directed path of* 0*-links from u_j to u_l.*

(iii) *Either (u_k, u_l) or (u_l, u_k) is a* 1*-link on P.*

Given two sets X_i and X_j, $X_i \oplus X_j$ denotes the *symmetric difference* of X_i and X_j. That is,

$$X_i \oplus X_j = (X_i - X_j) \bigcup (X_j - X_i).$$

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 AFSs and implied faulty sets.

LEMMA 1 [5]. *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 $\bigcup_{u_i \in U-F} L(u_i) \subseteq F$.*

LEMMA 2 [10]. *Given a system* S *and a syndrome, if F_1 and F_2 are* AFSs *then so is* $(F_1 \bigcup F_2)$.

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 an 0-link from $U - F$ to F on this path, contradicting the assumption that F is an AFS. □

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

DEFINITION 4. *A subset $K \subseteq U'$ is called a* vertex cover set (VCS) [13] *of G' if every edge in G' is incident on at least one vertex in K. A* minimum vertex cover set (MVCS) *is a* VCS *of minimum cardinality in G'.*

DEFINITION 5. *A subset $M \subseteq E'$ is called a* matching [13] *if no vertex in U' is incident on 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 that are adjacent to u_i.

3. Basic properties of allowable fault sets. In this section we establish certain properties of allowable fault sets with respect to a given syndrome. Our study is directed toward investigating conditions for a vertex v to be in an allowable fault set of cardinality at most t. For this purpose we use the notion of implied-fault set and the implied-fault graph used by Dahbura and Masson [5] 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 $E^* = \{(u_i, u_j) : u_i \in L(u_j)\}$. 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. Finally, we define $G^*(F)$ to be the subgraph of G^* such that all edges that connect vertices entirely inside F have been deleted.

Recall that we have assumed 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 [5]. We present this lemma for the sake of completeness.

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^*.

Proof. (i) Let F be an AFS of G for the given syndrome. Assume F is not a VCS of G^*. Then there exist $u_i, u_j \in U - F$ such that (u_i, u_j) is an edge in G^*. Since all edges from $U - F$ into F in G are 1-links (F is an AFS of G) and an implied-fault path between u_i and u_j can contain only one 1-link, all vertices that lie on an implied-fault path between u_i and u_j must belong to $U - F$. But this implies that there is a 1-link between two vertices in $U - F$, contradicting the assumption that F is an AFS of G. This shows that (i) holds.

(ii) Let F be a minimal VCS of G^*. Assume (ii) does not hold. Then at least one of the following conditions is satisfied.

(a) There exist $u_i, u_j \in U - F$ with $a_{ij} = 1$.

(b) There exist $u_j \in F, u_i \in U - F$ with $a_{ij} = 0$.

Assume (a) holds. Then the edge (u_i, u_j) is in G^*. But this contradicts the fact that F is a VCS of G^* since neither u_i nor u_j is a member of F.

Now assume (b) holds and (a) does not hold. Since F is a minimal VCS of G^* there exists a unit u_k in $U - F$ such that (u_j, u_k) is an edge in G^*; otherwise $F - \{u_j\}$ will be a VCS, contradicting the minimality of F. Hence $u_j \in L(u_k)$. Since $a_{ij} = 0$, it follows that $u_i \in L(u_k)$ and so (u_i, u_k) is an edge in G^*. Since neither u_i nor u_k is a member of F, this contradicts the fact that F is a VCS of G^*.

(iii) Statement (iii) follows from (i) and (ii). □

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. We first prove 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 $H_1 \bigcup H_0(v)$ is an AFS of G. Hence if $|H_1| < |H|$ then $H_1 \bigcup H_0(v)$ 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 $G - H_0(v)$.

We will now prove 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 $F - H_0(v)$, which is 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^* that 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. □

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_v^*.

Proof. Let $F_1 = F - H_0(v)$. From Lemma 3 and the proof of Lemma 5, it follows that F_1 is an AFS of $G - H_0(v)$. Then from Lemma 4, F_1 is a VCS of $(G - H_0(v))^*$. Thus, by Lemma 6, F_1 is a FCS of G_v^*. □

THEOREM 1. *Given a syndrome for a system* S, F *is an* AFS *of minimum cardinality among all allowable fault sets that contain unit* $v \in U$ *if and only if* $F - H_0(v)$ *is a* MVCS *of* G_v^*.

Proof. The proof follows from Lemmas 4, 5 and 6. □

The condition given in the above theorem can be used to test whether 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, a problem known to be NP complete. Therefore we would like to develop a test that requires determining an MVCS of a bipartite graph. With this objective in mind, we first 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 that will be used in the following section to develop the appropriate diagnosis algorithm.

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

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

For each vertex v in G, let

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

and

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

THEOREM 2. *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 $H = F - H_0(v)$. Since, by Lemma 3, $H_0(v) \subseteq F$, it follows that $|H| = |F| - |H_0(v)| \leq t - |H_0(v)| = t_v$. Define $B_X(H) = (U_X, E_X)$ to be the vertex-induced subgraph of B_v, where

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

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

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

Clearly $F_X = \{x_i : u_i \in H\}$ and $F_Y = \{y_i : u_i \in H\}$ are VCSs 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 $B_v - B_X(H) - B_Y(H)$ connects vertices in F_B. Therefore F_B is a VCS of B_v, contradicting our assumption that the cardinality of an MVCS of B_v is greater than t_v. Hence v is not contained in any AFS of cardinality at most t. □

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

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

and

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

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 $u_j \notin H_0(v)$; 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. □

LEMMA 9. *Given a syndrome for a system* S, *a unit $v \in U$, and an* MVCS *$F_B(v)$ of B_v, 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 $u_j \in F_v - F_I$. □

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 that 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. □

4. $O(n^{3.5})$ algorithm for diagnosis of a $t/(t+1)$-diagnosable system. In this section we present a necessary condition for a system S to be $t/(t+1)$ diagnosable. We then establish that in the case of a $t/(t+1)$-diagnosable system, the condition of Theorem 2 is both necessary and sufficient for a vertex v to be in an AFS of cardinality at most t. This will lead to an $O(n^{3.5})$ diagnosis algorithm to isolate all faulty units to within at most $t+1$ units in a $t/(t+1)$-diagnosable system.

Recall (§1) that a system S is said to be $t/(t+1)$ diagnosable if, given a syndrome, the set of faulty processors can be isolated to within a set of at most $t+1$ processors provided that the number of faulty processors does not exceed t.

It should be observed that a system is trivially $t/(t+1)$ diagnosable if $n = t+1$. Thus it is required that $0 \le t < n-1$. It should be noted [1] that under these conditions $n \ge 2t+1$ for $t/(t+1)$-diagnosable systems.

THEOREM 3. *If* S, *a multiprocessor system with test interconnection* $G = (U, E)$, *is* $t/(t+1)$ *diagnosable then for all* $X_i, X_j \subseteq U$ *with* $|X_i| > t$, $X_j \not\subseteq X_i$, *and* $|X_i| + |X_j| \le 2t$, *there exists a test from* $U - X_i - X_j$ *into* $X_i \oplus X_j$.

Proof. Assume S is $t/(t+1)$ diagnosable but the condition does not hold. Then there exist $X_i, X_j \subseteq U$ with $|X_i| > t$, $X_j \not\subseteq X_i$, $|X_i| + |X_j| \le 2t$ such that there is no test from $U - X_i - X_j$ into $X_i \oplus X_j$.

Since $|X_i| > t$ and $X_j \not\subseteq X_i$, $|X_i \cup X_j| > t+1$, we construct two sets F_1 and F_2 from X_i and X_j by moving elements from $X_i - X_j$ into $X_j - X_i$ until F_1 and F_2 have cardinality at most t. Thus we obtain two sets F_1 and F_2 with $|F_1| \le t$, $|F_2| \le t$ such that there is no test from $U - F_1 - F_2$ into $F_1 \oplus F_2$. Now consider the following syndrome (see Fig. 1) where for each edge $(u_k, u_l) \in E$ the outcome is defined as follows.

Case 1. $u_l \in U - (F_1 \cup F_2)$; then set $a_{kl} = 0$.
Case 2. $u_l \in F_1 \cup F_2$.
- 2.1. $u_l \in F_1 \cap F_2$; then set $a_{kl} = 1$.
- 2.2. $u_k, u_l \in F_1 - F_2$; then set $a_{kl} = 0$.
- 2.3. $u_k, u_l \in F_2 - F_1$; then set $a_{kl} = 0$.
- 2.4. $u_k \in F_1 \cap F_2$; then set $a_{kl} = 1$.
- 2.5. $u_k \in F_1 - F_2$ and $u_l \in F_2 - F_1$; then set $a_{kl} = 1$.
- 2.6. $u_k \in F_2 - F_1$ and $u_l \in F_1 - F_2$; then set $a_{kl} = 1$.

Both F_1 and F_2 are allowable fault sets of cardinality at most t for the given syndrome and $|F_1 \cup F_2| > t+1$. This contradicts the assumption that S is $t/(t+1)$ diagnosable. □

Recall from the previous section that $F_B(v)$ is an MVCS of B_v and F_v and F_I are sets derived from $F_B(v)$.

THEOREM 4. *Given a syndrome for a* $t/(t+1)$*-diagnosable system* S, *a unit* $v \in U$ *belongs to an* AFS *of cardinality at most t if and only if* $|F_B(v)| \le 2t_v$.

Proof. If $|F_B(v)| > 2t_v$ then, by Theorem 2, G does not contain an AFS of cardinality at most t containing the unit v.

Now assume $|F_B(v)| \le 2t_v$. If $F_v \cup H_0(v)$ contains an AFS of G of cardinality at most t containing the unit v then we are through. So assume $|F_B(v)| \le 2t_v$ and $F_v \cup H_0(v)$ does not contain any AFS of G of cardinality at most t containing the unit v. From Lemma 8, $F_v \cup H_0(v)$ is an AFS of G containing the unit v. If $F_v = F_I$ then $|F_v \cup H_0(v)| \le t$ since $|F_B(v)| \le 2t_v$. So we further assume that $F_v \ne F_I$. Since G^* does not contain any units with

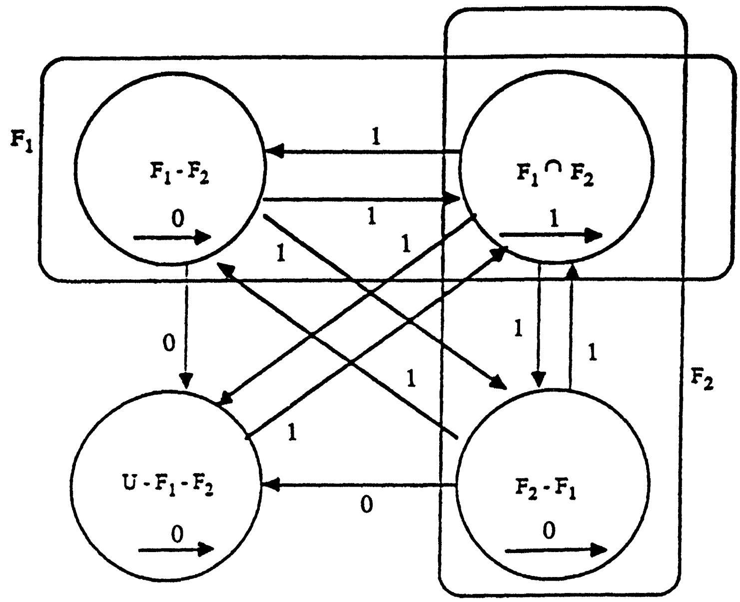

FIG. 1. *Two allowable fault sets generating a common syndrome.*

self-loops and $F_v \neq F_I$, the subset $|F_v - F_I| \geq 2$. Let F_α be an AFS of smallest cardinality containing unit v such that $F_\alpha \subseteq F_v \cup H_0(v)$. Clearly $|F_\alpha| > t$.

By Lemma 10 every AFS of G contained in $F_v \cup H_0(v)$ contains the subset F_I, and since $v \in F_\alpha$, it follows that $F_I \cup H_0(v) \subseteq F_\alpha$.

We next show that $F_\alpha \neq F_v \cup H_0(v)$. Let $u_i \in F_v - F_I$. Then $W = F_v - \{u_i\}$ is a VCS of G_v^* because, by Lemma 9(i), in G_v^* there is no edge (u_i, u_j) with $u_i \in U - (F_v \cup H_0(v))$ and $u_j \in F_v - F_I$. Hence by Lemma 6, W is a VCS of $(G - H_0(v))^*$. This means that, by Lemma 4(ii), W contains an AFS of $G - H_0(v)$. Thus $W \cup H_0(v)$ has an AFS of G containing unit v and of cardinality less than that of $F_v \cup H_0(v)$. Now let $F_a = F_\alpha - (H_0(v) \cup F_I)$, $F_b = (F_v \cup H_0(v)) - F_\alpha)$, and $F_\beta = F_b \cup H_0(v) \cup F_I$. Since F_α is an AFS of smallest cardinality containing v such that $F_\alpha \subseteq F_v \cup H_0(v)$, it follows that $|F_b| = |(F_v \cup H_0(v)) - F_\alpha| > 0$ and $F_\beta \not\subseteq F_\alpha$ (see Fig. 2).

Now

$$\begin{aligned} |F_\alpha| + |F_\beta| &= 2|F_I| + 2|H_0(v)| + |F_a| + F_b| \\ &= |F_B(v)| + 2|H_0(v)| \\ &\leq 2t_v + 2|H_0(v)| \leq 2t \end{aligned}$$

(see also Fig. 2).

Since $U - F_\alpha - F_\beta = U - (F_v \cup H_0(v))$ and $F_\beta \oplus F_\alpha = F_v - F_I$, it follows from Lemma 9(ii) that in G there is no edge (u_i, u_j) with $u_i \in U - (F_v \cup H_o(v)$ and $u_j \in F_v - F_I$.

Thus we have $|F_\alpha| > t$, $F_\beta \not\subseteq F_\alpha$, $|F_\alpha| + |F_\beta| \leq 2t$, and there is no test from $U - F_\alpha - F_\beta$ into $F_\alpha \oplus F_\beta$. This, by Theorem 3, contradicts our assumption that the system S is $t/(t+1)$ diagnosable. □

Given a valid syndrome for a $t/(t+1)$-diagnosable system S and a unit v in S, we have shown that the bipartite graph B_v has an MVCS of cardinality at most $2t_v$ if and only if G has an AFS of cardinality at most t containing the unit v. Since an MVCS of a bipartite graph has

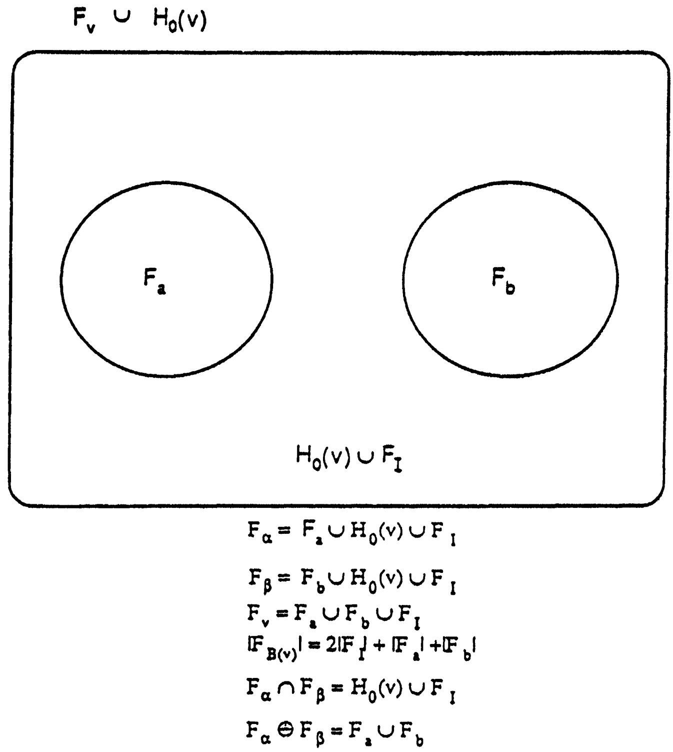

FIG. 2. *Illustration for proof of Theorem* 4.

the same cardinality as a maximum matching of the bipartite graph [13], it follows that B_v has a maximum matching of cardinality at most $2t_v$ if and only if G has an AFS of cardinality at most t containing the unit v. Thus Theorem 4 can be stated in an equivalent manner as follows.

THEOREM 5. *Given a syndrome for a $t/(t+1)$-diagnosable system* S, *a unit $v \in U$ belongs to an* AFS *of cardinality at most t if and only if B_v has a maximum matching of cardinality at most* $2t_v$.

The above theorem suggests the following $t/(t+1)$-diagnosis algorithm.

ALGORITHM. Diagnosis of a $t/(t+1)$-diagnosable system

Step 1. Given a $t/(t+1)$-diagnosable system S and a valid 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

3.1. Label v marked.

3.2. Set $t_v = t - |H_0(v)|$.

3.3. Construct B_v from B.

3.4. Compute a maximum matching K_v of B_v using the Hopcroft/Karp algorithm [14].

3.5. **If** $|K_v| \leq 2t_v$ **then** add v to F.

end

Step 4. F is the required set.

The proof of correctness of the above algorithm is as follows.

Essentially the algorithm proceeds as follows. Given a syndrome, for each unit $v \in U$ the algorithm tests if the cardinality of a maximum matching of B_v is at most $2t_v$. If unit v satisfies this requirement, then v is added to the set F. When the algorithm terminates we have

$$F = \{v : v \in U \text{ and } B_v \text{ has a maximum matching of cardinality at most } 2t_v\}.$$

Given a valid syndrome, in $t/(t+1)$-diagnosis we are required to isolate all faulty units to within a set of cardinality at most $t+1$. In other words, we need to determine the set of all units that are likely to be faulty under the given syndrome. By the definition of a $t/(t+1)$-diagnosable system, a unit v is likely to be faulty if and only if it belongs to an AFS of cardinality at most t. It then follows from Theorem 5 that a unit v is likely to be faulty if and only if B_v has a maximum matching of cardinality at most $2t_v$. The set F determined by the algorithm is therefore the required set consisting of all units that are likely to be faulty. By the definition of a $t/(t+1)$-diagnosable system, this set has cardinality at most $t+1$. Thus F is the required set isolating all the faulty units to within a set of cardinality at most $t+1$. This completes the proof of correctness of our $t/(t+1)$-diagnosis algorithm.

The bipartite graph in step 1 can be constructed in $O(n^{2.5})$ operations [5]. Step 2 requires $O(n)$ operations. The computation within step 3 is dominated by the computation of a maximum matching that requires $O(n^{2.5})$ operations [14]. Since step 3 is performed for each unit in U, the complexity of the entire algorithm is $O(n^{3.5})$.

5. Conclusions. In this paper we have studied the problem of diagnosing $t/(t+1)$-diagnosable systems. We presented a diagnosis for $t/(t+1)$-diagnosable systems that runs in $O(n^{3.5})$ time. This algorithm is based on the structure of allowable fault sets (§3) and on certain properties of $t/(t+1)$-diagnosable systems (§4).

REFERENCES

[1] F. P. Preparata, G. Metze, and R. T. Chien, *On the connection assignment problem of diagnosable systems*, IEEE Trans. Electr. Comput., EC-16 (1967), pp. 848–854.

[2] S. L. Hakimi and A. Amin, *Characterization of the connection assignment of diagnosable systems*, IEEE Trans. Comput., C-23 (1974), pp. 86–88.

[3] G. F. Sullivan, *A polynomial time algorithm for fault diagnosability*, in Proc. 25th Annual Symp. Foundations Comput. Sci., Orlando, FL, (1984), pp. 148–156.

[4] V. Raghavan, *Diagnosability issues in multiprocessor systems*, Ph.D. thesis, University of Minnesota, Minneapolis, MN, 1989.

[5] 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 Comput., 1984, pp. 428–433.

[6] G. F. Sullivan, *An $O(t^3 + |E|)$ fault identification algorithm for diagnosable systems*, IEEE Trans. Comput., Pans, C-37 (1988), pp. 388–397.

[7] A. D. Friedman, *A new measure of digital system diagnosis*, in Dig. 1975 Int. Symp. Fault-Tolerant Comput., (1975), pp. 167–170.

[8] A. Kavianpour and A. D. Friedman, *Efficient design of easily diagnosable systems*, in Proc. 3rd USA-Japan Comput. 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), pp. 414–422.

[10] G. Sullivan, *The complexity of system-level fault diagnosis and diagnosability*, Ph.D. thesis, Yale University, New Haven, CT, 1986.

[11] 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), pp. 639–643.

[12] A. Das, K. Thulasiraman, V. K. Agarwal, and K. B. Lakshmanan, *t/s-diagnosable systems: A characterization and diagnosis algorithm*, in Proc. 15th International Conference on Graph-Theoretic Concepts in Computer Science, Rolduc, Holland, 1989, pp. 34–45.

[13] J. A. BONDY AND U. S. R. MURTHY, *Graph Theory with Applications*, Elsevier North-Holland, Amsterdam, 1976.

[14] J. E. HOPCROFT AND R. M. KARP, *A $n^{2.5}$ algorithm for maximum matching in bipartite graphs*, SIAM J. Comput., 2 (1973), pp. 225–231.