A Polynomial Time Algorithm for Fault Diagnosability

by Gregory Sullivan

Yale University

Abstract

It is now possible to design and build systems which incorporate a large number of processing elements. For this reason, fault-diagnosis at the system level [16], a research area pioneered by the work of Preparata, Metze, and Chien [28], is of increasing importance. In [28], the fault-diagnosis properties of a system are modeled with a digraph, and the concept of t-diagnosability is introduced. A digraph is t-diagnosable if the system it models can correctly identify t (or fewer) faults by self-testing.

This concept has been explored extensively since 1967. Several classes of digraphs (e.g. boolean cube [3], $D_k$ [28, 26], $d(n, t, z)$ [6] de Bruijn variant [27]) have been analyzed in the literature for their t-diagnosis properties. In addition, several characterizations of the t-diagnosable digraphs have appeared [18, 2, 10]. Algorithms based on these characterizations were developed in [8, 10], however, they require exponential time and it was unknown if faster algorithms existed.

We resolve this open question by presenting the first polynomial time algorithm for t-diagnosability. The solution uses network flow techniques, runs in $O(|E||V|^{5/2})$ time and solves the more general formulation: Given a digraph determine the maximum $t$ for which the digraph is $t$-diagnosable. We also present part of our analysis of $t/s$-diagnosability. A digraph is $t/s$-diagnosable [15] if all faults can be localized to a set of at most $t$ vertices. (i.e. faulty vertices need not be uniquely identified.)

1. Introduction

In a system-level fault diagnosis problem there are a collection of objects (hardware modules, software modules, combinations thereof) and a set of diagnostic tests which objects perform on one another. From the results of these tests we hope to determine which, if any, of the objects are faulty. Following the model introduced in [28], we represent this problem with a directed graph in which each object is represented by a vertex and each test is represented by a directed edge. Specifically, there is an edge from $u$ to $v$ iff object $u$ tests object $v$.

Each object has two possible states 'good' or 'faulty'. Further, a test returns exactly one of two possible values 'good' or 'faulty'. Each of the tests is performed only once and they are performed all at once. Note, to be useful the set of test results should uniquely specify the 'faulty' objects. This goal is complicated by the fact that 'faulty' objects may produce spurious results in the tests they conduct. Below, we formalize two related but distinct problems: the $t$-fault diagnosis problem (or diagnosis problem) and the $t$-fault diagnosability problem (or diagnosability problem). In this paper we will use the graph terminology of Even [13]. Our graphs have no 'self loops' or 'parallel edges'. Let $G(V, E)$ be a digraph:

Definition 1.1. $L(V) = \{ L : L$ is a function from $V$ to \{ good, faulty \} $\}$ is the set of all vertex labelings.

Definition 1.2. $L(E) = \{ L : L$ is a function from $E$ to \{ good, faulty \} $\}$ is the set of all edge labelings.

Definition 1.3. $L_1 \in L(V)$ and $L_2 \in L(E)$ are compatible iff for all $u \rightarrow v \in E, (L_1(u) = good) \Rightarrow (L_2(v) = L_2(u \rightarrow v))$.

The above three definitions are the crux of the formalization of the diagnosis problem. If we think of the edge labeling as representing the results of a set of tests, then our goal is to find a vertex labeling compatible with the edge labeling. In particular, we would like a quickly computable function which given an edge labeling would yield a compatible vertex labeling. This is not enough, however, because the vertex labeling in which all vertices are 'faulty' is compatible with all edge labelings. We really want at least one vertex labeling to be compatible with an edge labeling. We can do this naturally by restricting the number of vertices that can be labeled 'faulty'. Let $t$ be positive integer.
Definition 1.4. \( L_t(V) = \{ L(V) : |\{ v : L(v) = \text{faulty}\}| \leq t \} \) are vertex labelings with at most \( t \) vertices labeled faulty.

Definition 1.5. A digraph \( G \) is \( t \)-diagnosable if there exists a function \( f \) from \( L(E) \) to \( L(V) \) such that if \( L_1 \in L(E) \) and \( L_2 \in L_t(V) \) are compatible then \( f(L_1) = L_2 \). We may restate this definition: A digraph \( G \) is \( t \)-diagnosable iff for any edge labeling \( L_1 \), if there exists any compatible vertex labeling \( L_2 \) it is unique.

Definition 1.6. Given a \( t \)-diagnosable digraph \( G \) and an edge labeling \( L \in L(E) \) the \( t \)-diagnosis problem is to find a vertex labeling \( L' \in L_t(V) \) compatible with \( L \) (if one exists).

\( t \)-Diagnosis, \( t \)-diagnosability and many variants have been examined extensively in the literature [28, 18, 2, 7, 20, 16, 3, 4, 22]. Prior to this paper, algorithms to test \( t \)-diagnosability required exponential time [10, 8]. In particular, they required at least \( O(|V|^t) \) choose \( t \) time, and \( t \) can be as large as \( |(|V|/2)^t | \) in a \( t \)-diagnosable digraph. In [5] a polynomial time algorithm to approximate \( t \) is also presented. Its time complexity is the same as our algorithm’s, \( O(|E|^{|V|^t/2}) \), however, no bound is claimed and we have constructed examples where the true value of \( t \) and its approximation differ by a factor of two.

2. Characterization of \( t \)-Diagnosable Digraphs

In figure 1-a we give an example of a 1-diagnosable digraph. Figures 1-a, 1-b and 1-c give examples of edge labelings and their unique compatible vertex labelings from \( L_1(V) \). The label of each vertex is circled. Figures 1-c and 1-d show that the digraph is not 2-diagnosable, since they depict two vertex labelings from \( L_2(V) \) which are compatible with the same edge labeling. Figure 2 shows a 2-diagnosable digraph, an edge labeling and its unique compatible vertex labeling from \( L_2(V) \).

There is a simple proof [28] that if a digraph is \( t \)-diagnosable then the indegree of each of its vertices is \( t \) or greater. A large number of other partial characterizations of the \( t \)-diagnosable digraphs appear in the literature. The first full characterization is due to Hakimi and Amin [18]. Our statement of the theorem is closer to that of Allan, Kamada and Toida [2]. We include its proof here for completeness. The characterization uses the following definition.

Definition 2.1. Let \( G(V, E) \) be a digraph with \( Z \subseteq V \). \( \Gamma^{-1}(Z) = \{ v : v \in V \text{ and there exists } z \in Z \text{ such that } v \to z \in E \} - Z \) (i.e. the set of vertices in \( V - Z \) which have edges to some vertex in \( Z \)).

Theorem 2.1. A digraph \( G(V, E) \) is \( t \)-diagnosable if and only if \( |\Gamma^{-1}(Z)| + |Z|/2 \leq t \).

Proof. Part I: Let \( G(V, E) \) be a digraph which is not \( t \)-diagnosable. We will show there exists \( Z \subseteq V \) with \( Z \neq \emptyset \) and \( |\Gamma^{-1}(Z)| + |Z|/2 > t \). Note, by the definition of \( t \)-diagnosability there exist two different vertex labelings \( L_1, L_2 \in L_t(V) \) compatible with some edge labeling \( L' \) of \( G \). Let \( F_1 \) and \( F_2 \) be the sets of vertices labeled faulty by \( L_1 \) and \( L_2 \) respectively. Let \( Z = (F_1 \cup F_2) - (F_1 \cap F_2) \). Since \( F_1 \neq F_2 \) we know \( Z \neq \emptyset \). We claim, there is no edge from a vertex \( u \in (F_1 \cup F_2)^c \) to a vertex \( z \in Z \). Suppose there is such an edge. Since \( u \) is labeled ‘good’ by both \( L_1 \) and \( L_2 \) the label on \( u \rightarrow z \) in \( L' \) must equal the label on \( z \) in both \( L_1 \) and \( L_2 \), but the label on \( z \) differs in \( L_1 \) and \( L_2 \) - a contradiction. We can now conclude that \( |\Gamma^{-1}(Z)| \leq F_1 \cap F_2 \) since \( V - Z = (F_1 \cup F_2)^c - (F_1 \cap F_2) \)

Further:

\[ |F_1| \leq t, \]
\[ |F_2| \leq t, \]
\[ |F_1| + |F_2| \leq 2t, \]
\[ |F_1 \cap F_2| + |F_1 \cup F_2| \leq 2t, \]
\[ 2|F_1 \cap F_2| + |Z| \leq 2t, \]
\[ |F_1 \cap F_2| + |Z|/2 \leq t, \]
\[ |\Gamma^{-1}(Z)| + |Z|/2 \leq t. \]

This completes part I.

Part II: See figure 3. Let \( Z \) be a non-null subset of vertices in \( G \) with \( |\Gamma^{-1}(Z)| + |Z|/2 \leq t \). Note, since \( |\Gamma^{-1}(Z)| \) and \( t \) are integers we may also state \( |\Gamma^{-1}(Z)| + |Z|/2 \leq t \). We will show \( G \) is not \( t \)-diagnosable. Partition \( Z \) into two sets \( Z_1 \) and \( Z_2 \) with \( |Z_1| \leq |Z|/2 \) and \( |Z_2| \leq |Z|/2 \). Now consider \( F_1 = Z_1 \cup \Gamma^{-1}(Z) \) and \( F_2 = Z_2 \cup \Gamma^{-1}(Z) \). Note, \( F_1 \neq F_2 \) and also note:

\[ |F_1| = |Z_1| + |\Gamma^{-1}(Z)|, \]
\[ |F_2| \leq |Z_2| + |\Gamma^{-1}(Z)|, \]
\[ |F_1| \leq t, \text{ similarly } |F_2| \leq t. \]

Let \( L_1, L_2 \in L_t(V) \) be the vertex labelings which label exactly the sets \( F_1 \) and \( F_2 \) faulty, respectively. This is allowed since \( |F_1| \leq t \) and \( |F_2| \leq t \). We shall now construct an edge labeling \( L' \) compatible with \( L_1 \) and \( L_2 \). All edges of the form \( u \rightarrow v \) where \( u \in F_1 \) and \( v \in F_2 \) are labeled ‘faulty’. All edges \( u \rightarrow v \) with \( u \in F_2 \) and \( v \in Z_1 \) are labeled ‘faulty’. All edges \( u \rightarrow v \) with \( u \in Z_2 \) and \( v \in Z_1 \) are labeled ‘faulty’. All other
edges in $L'$ are labeled 'good' (see figure 3). To see that $L_2$ is compatible with $L'$, observe that all edges from $F'_2$ to $F_1$ are labeled 'faulty', and all edges between elements of $F'_2$ are labeled 'good'. A similar argument shows $L_2$ is compatible with $L'$. We conclude $G$ is not $t$-diagnosable which completes part II of the proof. Together, parts I and II complete the theorem.

3. Network flow Preliminaries

Our $t$-diagnosability algorithm uses techniques from network flow [14]. Note, these definitions allow capacities on both edges and vertices. Also, a cut is not a partition of the vertices.

**Definition 3.1.** A flow network is a tuple $(G(V, E), s_1, s_2, c)$

1. $G(V, E)$ is a digraph
2. $s_1$ and $s_2$ are vertices. $s_1$ is called the source, and $s_2$ is called the sink
3. $c$ is a function from $E \cup V$ to non-negative rationals (plus infinity). The value of the function is called the capacity of the vertex or edge.

**Definition 3.2.** A flow function, $f$, is a function from edges to non-negative rationals such that the following three conditions hold (where $IN(v) = \{v' \rightarrow v : v' \rightarrow v \in E\}$ and $OUT(v) = \{v \rightarrow v' : v \rightarrow v' \in E\}$):

- For all $v \in V \setminus \{s_1, s_2\}$, $\sum_{v \in IN(v)} f(e) - \sum_{v \in OUT(v)} f(e) = 0$
- For all $v \in V \setminus \{s_1, s_2\}$, $\sum_{v \in OUT(v)} f(e) \leq c(v)$
- For all $e \in E$, $0 \leq f(e) \leq c(e)$.

For convenience, the description of a flow network may assign values to $c(s_1)$ and $c(s_2)$. Note, however, these values do not appear in the equations above and do not act as constraints. That is, capacities on the source vertex and sink vertex always appear infinite, no matter what values are given to $c(s_1)$ and $c(s_2)$. This will simplify our discussion later.

**Definition 3.3.** The value of a flow $f$ is $F = \sum_{v \in IN(s_1)} f(e) - \sum_{v \in OUT(s_2)} f(e)$ A flow function of a network with maximum value is a max-flow.

The definition of a cut given below is different from the definition when edge weights are not used and is particularly useful in a flow network which has capacities on both edges and vertices. It is used in [24] for that type of network.

**Definition 3.4.** A cut of a network is a subset of edges and vertices, $C \subseteq E \cup V - s_1, s_2$ such that any path from $s_1$ to $s_2$ contains at least one member of the set. The capacity of a cut is the sum of the capacities of its members. A cut of a network with minimum capacity is a min-cut.

**Theorem 3.1.** In a flow network the value of a max-flow equals the capacity of a min-cut.

**Proof.** See [14, 24].

4. Relationship Between Network Flow and $t$-Diagnosability

We now define a digraph and capacity function which we use to show the basic relationship between network flow and $t$-diagnosability.

**Definition 4.1.** Given digraph $G(V, E)$ we define the digraph $G'(V', E')$ as follows (see figures 4-a and 4-b):

- $V' = V \cup \{s_1\}$
- $E' = E \cup \{s_1 \rightarrow v : v \in V\}$

We also define a capacity function $c'$ on $E' \cup V'$:

- For all $e \in \{s_1 \rightarrow v : v \in V\}$, $c'(e) = 1/2$.
- For all $e \in E$, $c'(e) = \infty$.
- For all $v \in V'$, $c'(v) = 1$.

Our algorithm is based on the following theorem.

**Theorem 4.1.** Digraph $G(V, E)$ is $t$-diagnosable iff for all $v \in V$ the value of the max-flow in the flow network $(G'(V', E'), s_1, v, c')$ is greater than $t$.

**Proof.** Part I: Suppose there exists $s_2 \in V$ such that the max-flow in $(G'(V', E'), s_1, s_2, c')$ is less than or equal to $t$. We will show $G$ is not $t$-diagnosable. Let $C_1$ and $C_2$ be the edges and vertices, respectively, in a min-cut. There are two types of edges in $G'$, those with capacity $1/2$ and those with infinite capacity.

Since $C_1$ and $C_2$ form a cut of finite capacity we can conclude each edge in $C_1$ has capacity $1/2$. All vertices in $G'$ have capacity one so each vertex in $C_2$ has capacity one, thus:

$$|C_1|/2 + |C_2| \leq t$$

Let $Z = \{v \rightarrow s_1 \rightarrow v \in C_1\}$, and note $Z \neq \emptyset$ because $s_1 \rightarrow s_2$ must be in $C_1$, thus $s_2 \in Z$. Also note, trivially, $Z \subseteq V$. We claim $\Gamma^{-1}(Z) \subseteq C_2$ (this is $\Gamma^{-1}(Z)$ in $G(V, E)$).

Assume not. There exists $y \in \Gamma^{-1}(Z)$ with $y \notin C_2$. Thus, there
exists $u \in \mathbb{Z}$ with $y \rightarrow u \in E$. Since $s_1 \rightarrow u \in C_1$ there is a path from $u$ to $s_2$ which is not cut by any member of $C_1$ or $C_2$. This follows because if all paths from $u$ to $s_2$ were cut then $C_1 - \{s_1 \rightarrow u\}$ and $C_2$ would be a smaller cut than the min-cut.

Now, consider the path from $s_1$ to $y$ (an edge), from $y$ to $u$ (also an edge), and from $u$ to $s_2$. Below, we will show this path is not cut by any members of $C_1$ or $C_2$. $s_1$ is not in the cut by definition of a cut. $s_1 \rightarrow y$ is not in the cut; else $y$ would be in $Z$ and by definition $y$ is in $\Gamma^{-1}(Z)$. $y$ is not in the cut, because by definition above $y \notin C_2$. $y \rightarrow u$ is not in the cut because it has infinite capacity. $u$ is not in the cut; else $C_1 - \{s_1 \rightarrow u\}$ and $C_2$ would be a smaller cut than the min-cut. Finally, the fact that the path from $u$ to $s_2$ is not cut was shown above. This reasoning allows us to conclude by contradiction that $\Gamma^{-1}(Z) \not\subseteq C_2$. So:

$$|C_1|/2 + |C_2| \leq t$$

$$|Z|/2 + |Z| \leq t$$

This shows $G$ is not $t$-diagnosable by our earlier characterization, and thus completes part I of the proof.

Part II: Suppose $G$ is not $t$-diagnosable. We will show that for some $s_2 \in V$, there is a cut in the flow network $(G'(V', E'), s_1, s_1, s_1')$ which has capacity less than or equal to $t$. Let $Z$ be a non-null set of vertices such that $|\Gamma^{-1}(Z)| + |Z|/2 \leq t$. Let $s_2$ be an arbitrary member of $Z$. We claim the following sets form a cut in the flow network:

$$C_1 = \{s_1 \rightarrow z : s_1 \rightarrow z \in E', z \in Z\}$$

$$C_2 = \Gamma^{-1}(Z) \setminus \Gamma^{-1}(Z) \cap G(V, E)$$

Suppose $C_1 \cup C_2$ is not a cut. Consider some uncatt path from $s_1$ to $s_2$. Since $s_1 \notin Z$ and $s_2 \in Z$ there is an edge $q_1 \rightarrow q_2$ in the path with $q_1 \notin Z$ and $q_2 \in Z$. If $q_1 = s_1$ then $q_1 \rightarrow q_2$ is in $C_1$ a contradiction. If $q_1 \neq s_1$ then $q_1 \in \Gamma^{-1}(Z)$ and hence $q_1 \in C_2$ another contradiction. So $C_1 \cup C_2$ is a cut. Its capacity is less than or equal to $t$ because:

$$|Z|/2 + \Gamma^{-1}(Z) \leq t$$

$$|C_1|/2 + |C_2| \leq t$$

This finishes part II and our proof is complete.

5. Algorithm

It is clear by theorem 4.1 that we can test if a digraph is $t$-diagnosable by solving $|V|$ network flow problems in $(G'(V', E'))$, $(s_1, s_2, e')$. However, it is easier to prove a lower time complexity for our algorithm by solving flow problems in the related network below.

Definition 5.1. Given a digraph $G(V, E)$ we define $G^e(V', E')$ as follows (see figures 4-a and 4-c)

$$V' = \{s_1\} \cup \{v_0,i, v_1,i, v_2,i : v_i \in V\}, \text{ where } V = \{v_1, v_2, v_3, \ldots, v_{|V|}\}$$

$$E' = \{s_1 \rightarrow v_0,i, v_0,i \rightarrow v_1,i, v_0,i \rightarrow v_2,i : v_i \in V\} \cup \{v_1,i \rightarrow v_1,i, v_1,i \rightarrow v_2,i, v_2,i \rightarrow v_2,i, v_i \rightarrow v_j : v_i \in E\}$$

We also define a capacity function $c^e$ on $E' \cup V'$:

For all $e \in E'$, $c^e(e) = \infty$.
For all $v \in V'$, $c^e(v) = 1$.

For this digraph one can show the following:

Theorem 5.1. The max-flow in $(G'(V', E'), s_1, v_1, e')$ equals $F$ if the max-flow in $(G^e(V', E'), s_1, v_1, e')$ equals $2F$ for all $v_i \in V$.

Proof. Straightforward application of the cut definition.

We now present the algorithm.

Input: digraph $G(V, E)$.
Output: max int $t$ such that $G$ is $t$-diagnosable.

1. If there exists a vertex with in-degree zero then output 'not diagnosable' and STOP.
2. Construct digraph $G^e(V', E')$.
3. $X := \lfloor \min(i \in \{1, 2, 3, \ldots, |V|\}) \rfloor$ of $FLOW((G^e(V', E'), s_1, v_1, e'))$.
4. Output largest integer strictly less than $X/2$.

In the first step of the algorithm we check if there are any vertices with in-degree zero. If there are such vertices then the digraph is not $t$-diagnosable (for any positive integer $t$). To see this, suppose $v \in V$ has in-degree zero. Let $L \in \mathcal{L}(E)$ be an edge labelling in which all edges are labelled 'good'. Let $L_0 \in \mathcal{L}(V)$ be a vertex labelling in which all vertices are labelled 'good', and let $L_0 \in \mathcal{L}(V)$ be a vertex labelling in which all vertices are labelled 'good' except $v$ which is labelled 'faulty'. The correctness of the remainder of the algorithm follows from theorems proved earlier.
Now we are ready to analyze the complexity of this algorithm. We assume digraphs are represented using an adjacency list representation [1]. Checking if any vertex has in-degree zero can be done in $O(|E|)$. The remainder of the algorithm solves $|V|$ network flow problems in the digraph $G'((V', E'))$ where $|V'| = 3|V| + 1$ and $|E'| = 3|V| + 4|E|$. However, the algorithm solves these problems only if each vertex has in-degree one or greater. In this case, $|V| \leq |E|$, thus $|E'| \leq 7|E|$. Now we can use a result of Even and Tarjan [12], who showed that Dinic’s algorithm [11] for finding a maxflow in a network, $(G(V, E), s_1, s_2, c)$ in which the capacity of each vertex is one and the capacity of each edge is infinite, has a time complexity of $O(|E||V|^{5/2})$. So the complexity of our algorithm is bounded by $O(|E||V|^{5/2})$ or more simply $O(|E||V|^{3/2})$.

6. t/s-Diagnosability

Friedman [15] introduced the concept of t/s-diagnosability which was further analyzed in [6] and [23]. A digraph is t/s-diagnosable if the system it models can localize all faults to a set of s components, assuming t or fewer of the components are faulty (i.e., faulty vertices need not be uniquely identified). We define this formally. First, a preliminary definition: (Notation: “union: $r \in \{1, 2, \ldots, s\}$ $F_r$” is used for “$\cup_{r \in \{1, 2, \ldots, s\}} F_r$”)

Definition 6.1. If $L \in \mathcal{L}(E)$ then $F \subseteq V$ is a compatible fault set of $L$ iff the vertex labelling $L' \in \mathcal{L}(V)$ which labels each element of $F$ ‘faulty’ and all other vertices ‘good’ is compatible with $L$.

Definition 6.2. A digraph is t/s-diagnosable iff for all edge labelings $L'$ of the set of vertices labelled faulty by some compatible vertex labeling $L$, $L' \in \mathcal{L}(V)$ has size at most $s$, i.e. if $L_1, L_2, \ldots, L_k$ are compatible with $L'$ and $F_1, F_2, \ldots, F_k$ are the compatible fault sets then the $|\cup_{r \in \{1, 2, \ldots, k\}} F_r| \leq s$.

Theorem 6.1. If $L$ is an edge labelling of digraph $G(V, E)$ and $F_1$ and $F_2$ are compatible fault sets of $L$ then $F_1 \cup F_2$ is a compatible fault set of $L$.

Proof. Let $L_{F_1}, L_{F_2}$ and $L_{F_1 \cup F_2}$ be the vertex labellings specified by the fault sets. By definition we have, for all $u \rightarrow v \in E$, $(L_{F_1}(u) = \text{good}) \Rightarrow (L_{F_2}(v) = L(u \rightarrow v))$, and we have for all $u \rightarrow v \in E$, $(L_{F_2}(u) = \text{good}) \Rightarrow (L_{F_2}(v) = L(u \rightarrow v))$. Also, note the following two facts: for all $u \rightarrow v \in E$, $(L_{F_1}(u) = \text{good}) \Rightarrow (L_{F_1\cup F_2}(u) = \text{good})$ and $(L_{F_2}(u) = \text{good})$; for all $u \rightarrow v \in E$, $(L_{F_1}(u) = L(u \rightarrow v))$ and $(L_{F_2}(u) = L(u \rightarrow v)) \Rightarrow (L_{F_1\cup F_2}(u) = L(u \rightarrow v))$. We conclude, for all $u \rightarrow v \in E$, $(L_{F_1\cup F_2}(u) = \text{good}) \Rightarrow (L_{F_1\cup F_2}(v) = L(u \rightarrow v))$.

We now show t/s-diagnosability is co-NP-complete, and sketch polynomial time algorithms for t/t and t/(t+1)-diagnosability. (In the full paper we shall show that for any fixed integer $k > 1$, t/kt-diagnosability is co-NP-complete, and there is a polynomial time algorithm for t/(t+k)-diagnosability).

Theorem 6.2. If digraph $G(V, E)$ is not t/s-diagnosable then there is an edge labelling and compatible fault sets $F_1, F_2, \ldots, F_r$ with $r \leq s - t + 2$ such that for all $i \in \{1, 2, \ldots, r\}$, $|F_i| \leq t$ and $|\cup_{r \in \{1, 2, \ldots, r\}} F_r| > s$.

Proof. If $G$ is not t/s-diagnosable then there is an edge labelling and compatible fault sets $F_1, F_2, \ldots, F_r$ such that for all $i \in \{1, 2, \ldots, r\}$, $|F_i| \leq t$ and $|\cup_{r \in \{1, 2, \ldots, r\}} F_r| > s$. Let $F$ be a set of fault sets satisfying the above. If $F_i \in F$ and $|F_i| \leq t$ then $(F - \{F_i, F_j\}) \cup \{F_i, F_j\}$ defines a set of fault sets which still satisfy the properties above. Also, if $F \subseteq (F \subseteq \cup_{r \in \{1, 2, \ldots, r\}} F_i)$ then $F - \{F_i\}$ still satisfies the properties above. These two facts allow us to construct a set of fault sets $\{F_1, F_2, \ldots, F_r\}$ with the following property: For all $i \in \{1, 2, \ldots, r\}$, $|\cup_{r \in \{1, 2, \ldots, i\}} F_r| \geq t + i - 1$. Thus, when $r = s - t + 2$ we have $|\cup_{r \in \{1, 2, \ldots, r\}} F_r| \geq s + 1$.

We show that deciding if a digraph is t/s-diagnosable is co-NP-complete. We require the following problem descriptions.

NAME: Clique

INSTANCE: Graph $G(V, E)$, positive integer $k \leq |V|$.

QUESTION: Does $G$ contain a clique of size $k$ or more i.e., a subset $V' \subseteq V$ with $|V'| \geq k$ such that every two vertices in $V'$ are joined by an edge in $E$?

NAME: Bipartite Smothering

INSTANCE: Bipartite graph $G(V, E)$, vertex sets $A$ and $B$ which partition $V$ (i.e., $A \cup B = V$ and $A \cap B = \emptyset$) such that all edges are between members of $A$ and $B$, positive integers $k_A \leq |A|$ and $k_B \leq |B|$.

QUESTION: Can $k_A$ (or fewer) vertices in $A$ smother $k_B$ (or more) vertices in $B$ i.e., is there a set
The clique problem is NP-complete [21, 17].

**Theorem 0.3.** Bipartite smothering is NP-complete

*Proof.* It is in NP since vertex sets $A$ and $B$ provide a certificate. Let graph $G(V, E)$ and positive integer $k$ be an instance of the clique problem. We define an instance of the bipartite smothering problem as follows: Let $G'(V', E')$ be a graph with $V' = V \cup E$ and $x \rightarrow y \in E'$ iff $x \in V$, $y \in E$, and $y$ is incident to $x$ in $G(V, E)$. Also let $A = V$, $B = E$, $k_A = k$, and $k_B = (k(k-1))/2$. One may verify that $G(V, E)$ has a clique of size $k$ (or more) iff $G'(V', E')$ contains $k_A$ (or fewer) members of $A$ which smother $k_B$ (or more) members of $B$.

**NAME:** t/s-Diagnosability

**INSTANCE:** Digraph $G(V, E)$, positive integers $t$ and $s$ with $t \geq s$.

**QUESTION:** Is $G$ t/s-diagnosable?

**Theorem 0.4.** t/s-Diagnosability is co-NP-complete

*Proof.*

Sketch: If $G$ is not t/s-diagnosable then there is an edge labeling and compatible fault sets $F_1, F_2, ..., F_r$ with $r \leq s - t + 2$ which certify $G$ is not t/s-diagnosable. If $s \geq |V|$ then $G$ is t-s-diagnosable, so the certificate has polynomial size. Thus, the problem is in co-NP.

Let $G(V, E)$, $A$, $B$, $k_A$, $k_B$ be an instance of bipartite smothering. We will first give a reduction which works when $k_B > 1$. We define the following instance of t/s-diagnosability. Let $G'(V', E')$ be a graph with $V' = V \cup D$ where $D$ is a set disjoint with $V$ and $|D| \geq 2k_A + 3$. Further, $u \rightarrow v \in E'$ iff $(u, v) \in A \cup D$ and $u \neq v$ (or $u \in A$ and $v \in E$ and $u-v \in V$). Lastly, let $t = k_A + 1$ and $s = k_B + k_A - 1$.

We claim $k_A$ (or fewer) members of $A$ smother $k_B$ (or more) members of $B$ iff $G(V', E')$ is not t/s-diagnosable (assuming $k_B > 1$). Assume $k_A$ (or fewer) members of $A$ smother $k_B$ (or more) members of $B$. Call the corresponding vertex sets $V_A$ and $V_B$. (If necessary pad $V_A$ so that $|V_A| = k_A$. The new set still smother $V_B$.) Now, consider the following edge labeling for $G'$. For all $u \rightarrow v \in E'$, $L(u \rightarrow v) = fault$ if $v \in V_A$ otherwise $L(u \rightarrow v) = good$. Consider the following fault sets $F_1 = V_A \cup \{v\}$, for each $v \in V_B$. One can verify that $F_1, F_2, ..., F_{|V_B|}$ are compatible fault sets of $L$ in $G'$. We also note $|union: i \in \{1, 2, ..., k_B\} of F_i| \geq k_A + k_B > s$.

Now, suppose $G'(V', E')$ are not t/s-diagnosable. Then there exists $L$ an edge labelling of $E'$ and $F_1, F_2, ..., F_r$ compatible fault sets such that $|F_i| \leq k_A + 1$ for $i \in \{1, 2, ..., r\}$ and $|union: i \in \{1, 2, ..., r\} of F_i| > k_A + k_B - 1$. We define $F_{core} = (intersection: i \in \{1, 2, ..., r\} of F_i)$, and we define $F_{periph} = (union: i \in \{1, 2, ..., r\} of F_i) - F_{core}$. Let $F_{core} = F_{core} \cap A$. One can establish that $F_{periph} \subseteq B$. After this, one can establish that $F_{core}$ smother $F_{periph}$ in $G$, and $|F_{core}| \leq k_A$ and $|F_{periph}| \geq k_B$.

To complete the proof of the theorem we describe our reduction for an instance of bipartite smothering $G(V, E)$, $A$, $B$, $k_A$, $k_B$ when $k_B = 1$. Note, we can in polynomial time determine $|l^{-1}(u)|$ for each element $u \in B$. This information determines if $k_A$ vertices can smother $k_B = 1$ vertices. If they can smother then we define our reduction to yield an arbitrary instance of the t/s-diagnosability problem which is t/s-diagnosable, otherwise it yields an instance which is not t/s-diagnosable.

We now describe the fast algorithms for t/t and t/(t+1). In [6] a characterization of t/t-diagnosable digraphs appears which may be restated as follows:

**Theorem 0.5.** A digraph $G(V, E)$ is t/t-diagnosable iff $|V| \leq t$ or for all $Z \subseteq V$ with $|Z| \geq 2$, $|l^{-1}(Z)| + |Z|/2 > t$.

To design an algorithm using this fact we note that, for any pair of vertices $v_i$ and $v_j$ we can modify $G'$ by adding a sink vertex $s_2$, adding directed edges from $v_i$ to $s_2$ and from $v_j$ to $s_2$, and changing the capacities of $v_i$ and $v_j$ to infinity. We claim that:

**Theorem 0.6.** Digraph $G(V, E)$ is t/t-diagnosable iff $|V| \leq t$ or for all $v_i, v_j \in V$ the value of the max-flow in the flow network $(G'(V', E'), s_1, s_2, c')$ is greater than $t$.

We can construct a modified $G''$ to solve the network flow problems and achieve a time complexity of $O(|E||V|^2)$. The following characterization of t/(t+1)-diagnosable digraphs can also be used to design an algorithm.
Theorem 6.7. A digraph \( G(V,E) \) is \( t/(t+1) \)-diagnosable iff 
\[ |V| \leq t+1 \text{ or } (\text{for all } Z \subseteq V \text{ with } |Z| \geq 4, |\Gamma[Z]|+|Z|/2 > t) \]
and 
\[ (\text{for all } v_1, v_2, v_3 \in V, \text{ with no edge between } v_i \text{ and } v_j, 1 \leq i \leq j \leq 3, |\Gamma^{-1}\{v_1, v_2, v_3\}| \leq t-1) \]

We can immediately test if \( |V| \leq t+1 \). In \( |V|^3 \) time we can check whether 
( for all \( v_1, v_2, v_3 \in V, \) with no edge between \( v_i \) and \( v_j \), \( 1 \leq i \leq j \leq 3, |\Gamma^{-1}\{v_1, v_2, v_3\}| \leq t-1 \). Finally, for any four vertices \( v_4, v_5, v_6 \text{ and } v_7 \), we can modify \( G' \) by giving those vertices infinite capacity, adding a sink vertex \( s_2 \) and adding directed edges from the four vertices to \( s_2 \). A theorem analogous to the one above holds and there is an algorithm with time complexity \( O(|E||V|^{5/2}) \).

7. Other Diagnosabilities

The diagnosability questions for several other types of system-level fault diagnosis are co-NP-complete. In probabilistic fault diagnosis [25], \( p-t \)-diagnosability is co-NP-complete. In weighted fault diagnosis [25], \( t \)-diagnosability is co-NP-complete. In fault diagnosis with formulas [15] (even with just disjunction), \( t \)-diagnosability is co-NP-complete (in preparation).
(Note, this does not rule out the usefulness of these concepts since some classes of digraphs may be provably diagnosable and these digraphs may even have fast diagnosis algorithms.)

8. Diagnosis

Recall the \( t \)-diagnosis problem is: Given a \( t \)-diagnosable digraph \( G \) and an edge labeling \( L \in \mathcal{L}(E) \) find a vertex labeling \( L' \in \mathcal{L}(V) \) compatible with \( L \) (if one exists). In [20] Kameda, Toida and Allan present a back-track algorithm for diagnosis and a clever analysis which shows its complexity is only \( O(n^3) \). Recently, Dahbura and Masson [9] presented an elegant \( O(n^2\cdot 3) \) algorithm for this problem. Their solution, however, requires computation of a transitive closure. We have found an \( O(t^3 + |E|) \) diagnosis algorithm (where \( t \) is the max number of faulty elements) which is a modification of Kameda et al's algorithm (in preparation).

Another approach to the diagnosis problem is to restrict the digraphs considered. Dahbura et al [8] presented a fast \( O(|E|) \) algorithm for diagnosis of 'self-implicating' systems. We have developed an \( O(|E|) \) diagnosis algorithm for a superset of the 'self-implicating' systems which includes \( t \)-vertex-connected digraphs (independently discovered by D. Angluin and S. Eisenstat) (in preparation).

9. Conclusion

We have presented the first polynomial time algorithm for testing \( t \)-diagnosability. This is a significant advance in system-level fault diagnosis. We also presented part of our analysis of \( t/s \)-diagnosability, including the fact that it is co-NP-complete and that there are polynomial algorithms for \( t/t \) and \( t/(t+1) \)-diagnosability.

10. Acknowledgment

The author thanks D. Gusfield for many valuable discussions and pointers, especially the suggestion to examine network flow techniques and connectivity testing. The author also thanks D. Angluin for many fruitful discussions, and for suggesting the problem area.
References


