Discrete Event Dynamic Systems, 4, 197–212 (1994)

Diagnosability of Discrete Event Systems and Its Applications

FENG LIN
Department of Electrical and Computer Engineering, Wayne State University, Detroit, MI 48202

Received April 7, 1993; Revised August 13, 1993.

Abstract. As man-made systems become more and more complex, diagnostics of component failures is no longer an easy task that can be performed based on experience and intuition. Therefore, it is important to develop a systematic approach to diagnostic problems. Diagnostics can be done either on-line or off-line. By on-line diagnostics, we mean diagnostics performed while the system to be diagnosed is in normal operation. On the other hand, in off-line diagnostics, the system is not in normal operation. We will study both on-line and off-line diagnostics in this paper and identify main features and differences of these two types of diagnostics. We will also introduce the concept of diagnosability and study its properties, all in the framework of discrete event systems. This study is motivated by diagnostic problems in the automotive industry and we will emphasize its applications.

Keywords: Diagnostics, observation, control, discrete event systems

1. Introduction

Diagnostics is important in many application areas such as automobile manufacturing and repair. Before leaving an assembly line, each automobile must be tested to ensure its integrity. It is also proposed that during its operation, an automobile should have self test capability to diagnose component failures. Diagnostics is of course the key problem when an automobile is in repair. The complexity of automobiles has increased significantly in the past decade. More and more sensors, actuators and controllers have been used to meet stringent regulations on exhaust emissions and increasing demands on fuel economy. Nowadays an electronic engine control system alone consists of the following subsystems all under control of a electronic engine control module (EEC-IV): carburetor, throttle, injector, exhaust system, catalyst, evaporative emission system, exhaust gas recirculation system, inlet air temperature system, positive crankcase ventilation system, thermactor system, and fuel delivery system. Each subsystem has several sensors and actuators. It is imaginable that diagnosing such a system is not a trivial task. Even a skilled mechanic may not be able to find failures effectively. Trial and error methods could hardly work and a systematic approach is in demand. To this end, Ford has recently developed a computerized service bay diagnostic system (SBDS) to assist mechanics. SBDS is a huge success in terms of customer satisfaction and reduced warranty cost. This shows the importance of a systematic approach to diagnostics.

Diagnostic problems are not unique to automobiles. As man-made systems become more and more complex, detecting and locating component failures are no longer straightforward tasks. There is a strong need for a systematic study of diagnostic problems and diagnosability issues.

Diagnostics has been studied by scientist and engineers, especially for continuous variable systems, where diagnostics is done by means of parameter estimation, state estimation, etc. (Patton, Clark, and Frank 1989, Tsafestas, Singh, and Schmidt 1987a,b). These methods are suitable for specific types of failures and studies are done at a detailed level. At a high level, however, diagnostics of complex systems is better modeled by a discrete event model than by a differential or difference equation model. In a discrete event model, the failure status of system components are represented by states and the tests and their results described by events. We believe that such a discrete event model is sufficiently general to cover a large class of man-made systems.

In this paper, we will study two types of diagnostic problems: on-line diagnostics and off-line diagnostics, depending on whether the system to be diagnosed is in normal operation or not. We will propose a discrete event model for diagnostics, discuss diagnosability, and develop algorithms to calculate test points and test sequences. Examples will be given to illustrate the results.

Diagnostic problems have not been thoroughly studied in the framework of discrete event systems. However, issues related to diagnostics have been studied, mainly controllability and observability. In Lin and Wonham (1988), observability is studied under the assumption of no state observation and partial event observation; and the objective is to find a proper feedback control. In Ramadge (1986), observability is studied under the assumption of partial state observation and full event observation; and the objective is to determine the current state. In Ozveren and Willsky (1990), observability is studied under the assumption of partial event observation and no state observation; and the objective is also to determine the current state. All these studied are related to diagnostic problems because diagnostics can be viewed as determining the state of a system from events or other outputs. However, diagnosability is not just observability, for diagnosing a system requires performing tests in the system. In other words, to diagnose a system is not just to passively observe the system, but also to actively control the system. Control problems for discrete event systems have also been extensively studied (Cieslak et al. 1988, Lin and Wonham 1988, Ramadge and Wonham 1987). However, the concepts introduced in this paper are new and different from those studied in the literature.

2. Off-line and On-line Diagnostics

By off-line diagnostics, we mean diagnostics performed when the system to be diagnosed is not in normal operation. For example, what a mechanics does to an automobile in a repair shop can be viewed as off-line diagnostics. To perform off-line diagnostics, one can "open" the system, so to speak, access the inside, do various tests, and measure responses that may not be available from the system outputs. During off-line diagnostics, since the system is not actually in operation, the failure status of system components will not change, unless such changes are made in purpose. Also tests can be designed with great flexibility and the order of testing is not critical as far as diagnosability is concerned.

These nice properties of off-line diagnostics may be absent in on-line diagnostics. In on-line diagnostics, the system to be diagnosed is in normal operation. Hence the operating state of the system is constantly changing and some changes cannot be prevented (in other

Table 1.

	on-line diagnostics	off-line diagnostics
state	changing	not changing
event	not all controllable	all controllable
observation	restricted to outputs	not restricted to outputs
test sequence	constraint	not constraint

words, some events are uncontrollable). Also the assumption that the system cannot be opened for inspection or testing during on-line diagnostics means that the measurements available are limited to observed system outputs. Another crucial constraint is that the tests to be performed and the order in which they should be performed must be feasible from the current operating state. The main differences between on-line and off-line diagnostics are summarized in table 1.

Because of significant differences between on-line diagnostics and off-line diagnostics, the approaches used to study them ought to be different. In the rest of the paper, we will propose a general framework for diagnostics and then discuss off-line diagnostics and on-line diagnostics as special cases.

3. Discrete Event Model for Diagnostics

We model the system to be diagnosed as a pair $G = (M, \Sigma_c)$. The first component M denotes a nondeterministics Mealy automaton:

$$M = (\Sigma, Q, Y, \delta, h)$$

where Σ is the set of finite events; Q is the set of states; Y is the output space; $\delta : \Sigma \times Q \rightarrow 2^Q$ is the state transition function, $\delta(\sigma, q)$ gives the set of possible next states if σ occurs at q; and $h : \Sigma \times Q \rightarrow Y$ is the output function, $h(\sigma, q)$ is the observed output when σ occurs at q. The second component $\Sigma_c \subseteq \Sigma$ is the set of controllable events, where the controllability of events is interpreted in a strong sense: a controllable event can be made to occur if physically possible.

States of the system describe conditions of its components. Therefore, to diagnose a failure is to identify which state or set of states the system belongs to. Thus depending on the requirements on diagnostics, we partition the state space Q into disjoint subsets (cells) and denote the desired partition by T. The state in the same cell are viewed as equivalent as far as failures under consideration are concerned. Our model is rather general since we do not put any restrictions on T.

This general model will be specialized to on-line and off-line diagnostics in the following sections.

4. Off-line Diagnostics

For off-line diagnostics, we specialize the model introduced in the previous section by assuming that the outputs are events observed, that is, $Y = \Sigma_o$, where $\Sigma_o \subseteq \Sigma$ is the set of observable events and the output map $h : \Sigma \times Q \to \Sigma_o$ is a projection defined as

$$h(\sigma, q) = \begin{cases} \sigma & \text{if } \sigma \in \Sigma_o \\ \epsilon & \text{otherwise.} \end{cases}$$

where ϵ is the empty string.

As discussed in Section 2, in off-line diagnostics all events are assumed to be controllable. Therefore, $\Sigma_c = \Sigma$. Since the failure status of system components will not change, information derived from all the test outputs are updated and relevant.

During off-line diagnostics, if an event $\sigma \in \Sigma_o$ is observed, then the possible state of the system is

$$Q(\sigma) = \{q \in Q : (\exists q' \in Q)\delta(\sigma, q') = q\}.$$

Hence, we know whether the system is in $Q(\sigma)$ or $Q - Q(\sigma)$ after observing σ. Therefore, each observable event partitions the state space into

$$T_\sigma = \{Q(\sigma), Q - Q(\sigma)\}.$$

Since there is no restriction on the tests to be performed in off-line diagnostics, we can observe all observable events that are physically possible and then determine which states the system is in. If this information is sufficient for us to determine which component is broken (i.e., which cell of T the system is in), then we say the system is off-line diagnosable. Formally,

Definition 1. G is said to be off-line diagnosable with respect to T if

$$\wedge_{\sigma \in \Sigma_o} T_\sigma \leq T$$

where $\wedge$ denotes conjunction and $\leq$ means "is finer than".

Clearly, diagnosability depends on both the observable event set Σ_o and the desired partition T. One problem of significance is how to find a smallest observable event set that makes G diagnosable for a given partition T. To solve this problem, we define the set of all observable event sets (OES) that ensure the diagnosability of the system as

$$OES(T) = \{\Sigma_o \subseteq \Sigma : G \text{is diagnosable with respect to } \Sigma_o \text{ and } T\}.$$

We would like to fine a minimal element in $OES(T)$.

Theorem 1 Minimal elements of $OES(T)$ exist, but may not be unique.

Proof: The proof of the existence of minimal elements is straightforward since Σ is finite. The following example shows that they may not be unique. Let

$$\begin{aligned} \Sigma &= \{\alpha, \beta\} \\ Q &= \{q_1, q_2\} \\ \delta(\alpha, q_1) &= \{q_2\} \\ \delta(\beta, q_1) &= \{q_2\} \\ \delta(\sigma, q) &= \emptyset \text{ for all other transitions} \end{aligned}$$

and

$$T = \{\{q_1\}, \{q_2\}\}.$$

Then both $\{\alpha\}$ and $\{\beta\}$ are minimal elements of $OES(T)$. ■

From Theorem 1, we can conclude that we may be able to find more than one set of observable events, each set is minimal in the sense that removing any event from the set will make the system not diagnosable. Practically, we can find a cost-effective minimal observable event set by first ordering the events in terms of the difficulty (and hence cost) in detection:

$$\Sigma = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$$

and then removing events one by one in the given order until the diagnosability of the system is no longer ensured using the following algorithm.

Algorithm 1.

```
begin
  Input:
  read $G$;
  read $T$;
  read the order $\Sigma = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$;
  Initialization:
  $\min OES := \Sigma$;
  Removal:
  for $i = 1$ to $n$ do begin
  $\min OES := \min OES - \{\sigma_i\}$;
  if $G$ is not diagnosable with respect to $\min OES$ and $T$ then
  $\min OES := \min OES \cup \{\sigma_i\}$;
  end;
  Output:
  write $\min OES$;
  end.
```

In some cases, however, the observable event set is given because the available test points and test sets are given. If the observable event set Σ_o is given but G is not diagnosable with respect to T, then we would like to find the finest partition coarser that T with respect to which G is diagnosable. Therefore, we define the set of all diagnosable partitions that are coarser than T as

$$D(T) = \{T' : T \leq T' \text{ and } G \text{ is diagnosable with respect to } T'\}.$$

The infimal element (with respect to $\leq$) in this set is the finest partition that we are looking for. The following theorem proves its existence.

Theorem 2 The set $D(T)$ is closed under conjunction. Therefore, the infimal element exists.

Proof: Let $T_1, T_2 \in D(T)$. Then

$$\begin{aligned} T &\leq T_1 \text{ and } \wedge_{\sigma\in\Sigma_o} T_\sigma \leq T_1 \\ T &\leq T_2 \text{ and } \wedge_{\sigma\in\Sigma_o} T_\sigma \leq T_2. \end{aligned}$$

Therefore

$$T \leq T_1 \wedge T_2 \text{ and } \wedge_{\sigma\in\Sigma_o} T_\sigma \leq T_1 \wedge T_2.$$

That is

$$T_1 \wedge T_2 \in D(T).$$

■

This finest partition will tell us which states are distinguishable for a given set of observable events. It will thus reveal "the degree of diagnosability". It will be shown in the next section that this partition can provide valuable information about how to partition system components into modules.

5. A Circuit Example

Let us consider the circuit in Figure 1. The possible states of the circuit are:

(w1,w2)	R_1 working, R_2 working;
(w1,s2)	R_1 working, R_2 shorted;
(w1,o2)	R_1 working, R_2 open;
(s1,w2)	R_1 shorted, R_2 working;
(o1,w2)	R_1 open, R_2 working.

Here we assume that there is only a single failure in the circuit for simplicity. We define the following events:

$$\begin{aligned} &\sigma_1 : V_{out} = 0; \\ &\sigma_2 : V_{out} = V_{in}; \\ &\sigma_3 : I = 0; \\ &\sigma_4 : I \neq 0. \end{aligned}$$

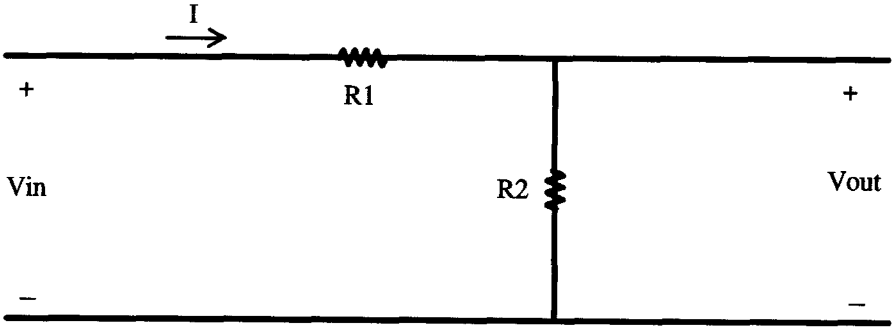

Figure 1.

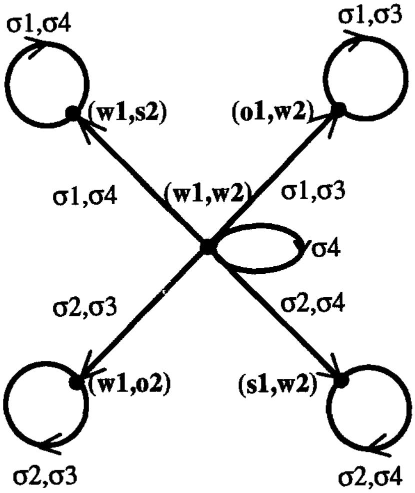

Figure 2.

By examining the circuit, we find that, for example, $V_{out} = 0$ implies that either R_1 is open or R_2 is shorted while $V_{out} = V_{in}$ implies that either R_1 is shorted or R_2 is open. Therefore, the state transitions are given in Figure 2.

Diagnosability of the circuit depends on Σ_o and T. Let $\Sigma_o = \{\sigma_1, \sigma_2\}$ (that is, only V_{in} and V_{out} cat be measured) and the desired partition $T = \{\{(\text{w1}, \text{w2})\}, \{(\text{w1}, \text{s2})\}, \{(\text{w1}, \text{o2})\}, \{(\text{s1}, \text{w2})\}, \{(\text{o1}, \text{w2})\}\}$. Then the circuit is not diagnosable, for the partition $T_{\sigma_1} \wedge T_{\sigma_2}$ shown in Figure 3 is not finer than T. However if $\Sigma_o = \{\sigma_1, \sigma_2, \sigma_3\}$ (that is, in addition we can also measure I), then the partition $T_{\sigma_1} \wedge T_{\sigma_2} \wedge T_{\sigma_3}$ shown in Figure 4 is equal to T. Therefore, the circuit is diagnosable. This example demonstrates that diagnosability

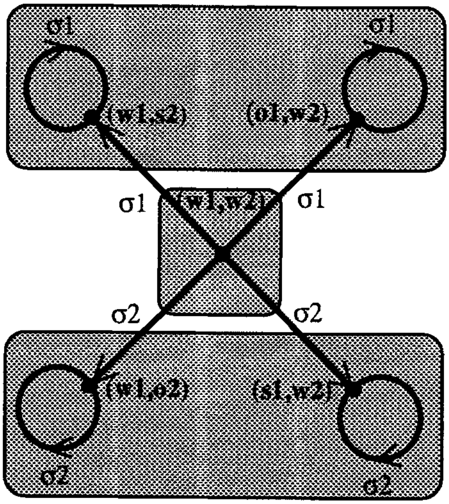

Figure 3.

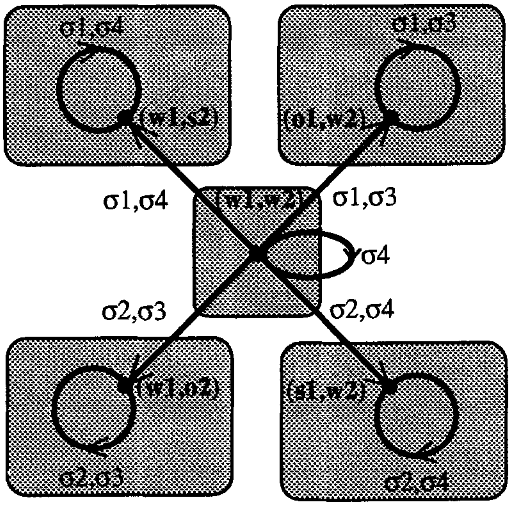

Figure 4.

depends on the observable events. On the other hand, diagnosability also depends on the desired partition T. In this circuit example, suppose we are only interested in knowing if

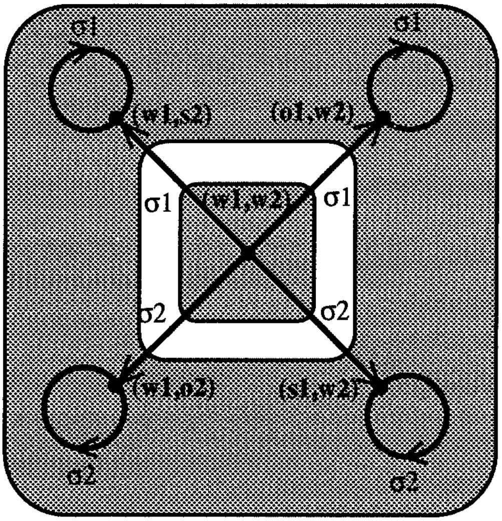

Figure 5.

the circuit is working or not. Then the desired partition T is shown in Figure 5. That is, we do not care if the circuit is in (w1,s2), (o1,w2), (w1,o2), or (s1,w2) for they are all bad. With respect to this partition, the circuit is diagnosable even if the observable event set is $\Sigma_o = \{\sigma_1, \sigma_2\}$. Thus, if only V_{in} and V_{out} are available for measurements, then R_1 and R_2 should be considered as one module in diagnostics.

We have applied the proposed framework for off-line diagnostics to the test of mixed (digital and analogy) signal circuits in automobiles. The results show that the proposed framework is suitable for the following tasks: (1) checking testability of a circuit; (2) finding the degree of testability; (3) computing minimal test points; (4) dividing a circuit into modules; and (5) designing for testability. The detailed investigation is reported in Lin, Markee, and Rado (1993).

6. On-line Diagnostics

During on-line diagnostics, not all events are controllable (i.e., can be initiated). Only events in Σ_c can be initiated. We denote by Σ_c^* the set of all strings of events over Σ_c, including the empty string ϵ. A string $u \in \Sigma_c^*$ is called a control.

For on-line diagnostics, we specialize our model introduced in Section 3 by assuming that M is a deterministics Moore automaton, that is, $\delta : \Sigma \times Q \rightarrow Q$ is a deterministic map and $h : Q \rightarrow Y$ is a state output map. Without loss of generality, we assume that δ is a total function, otherwise we can add an extra state q_d to Q and define $\delta(\sigma, q) = q_d$ if $\delta(\sigma, q)$ is originally undefined. The map h is usually many to one. In other words, the states may not be distinguishable from the outputs and diagnostics need to be performed. Since the failure status of system components may change during on-line diagnostics, only the current state output is updated and relevant.

The goal of diagnostics is to find which cell of T the system G belongs to by issuing a sequence of control $u \in \Sigma_c^*$ and observing the outputs. To know what output is expected from G, we need to know what is the behavior of G. The behavior is described by all possible strings of events that can occur in G. Note that after a sequence of control $u \in \Sigma_c^*$ is issued the behavior of G is restricted, because G must execute the events in u and execute them in the order given by u. Meanwhile some events in $\Sigma - \Sigma_c$ may also occur, for they are not controllable. Therefore, the behavior of G under control u is described by

$$B(u) = P^{-1}\{u\}$$

where $P : \Sigma^* \to \Sigma_c^*$ is the projection defined recursively as

$$\begin{aligned} P\epsilon &= \epsilon \\ P(s\sigma) &= \begin{cases} Ps & \text{if } \sigma \notin \Sigma_c \\ (Ps)\sigma & \text{if } \sigma \in \Sigma_c \end{cases} . \end{aligned}$$

We do not know which state G is in when we start diagnostics. If we only know that G starts with some state in $I \subseteq Q$ (in the worst case, when no knowledge on the state is available, $I = Q$), then the set of possible states after the execution of control u, is given by

$$S(u, I) = \{q \in Q : (\exists s \in B(u))(\exists q' \in I)\delta(s, q') = q\}.$$

With these notations, we can now define on-line diagnosability. We say that u diagnoses G with respect to T if, after executing u, which cell of T the current state of G belongs to can be determined by observing the current output of G.

Definition 2. A control u diagnoses G in I with respect to T if

$$(\forall q, q' \in S(u, I))h(q) = h(q') \Rightarrow q =_T q'$$

where $q =_T q'$ denotes that q and q' belong to the same cell under the partition T.

Definition 3. G is said to be on-line diagnosable with respect to T if there exists a control u that diagnoses G in Q with respect to T.

The problem of checking on-line diagnosability can be translated into a reachability search problem as follows. Given a G, define $\tilde{G}$ as

$$\tilde{G} = (\Sigma_c, X, \xi)$$

where $X = 2^Q$ and $\xi : \Sigma_c \times X \to X$ is defined as $\xi(\sigma, x) = \{q \in Q : (\exists q' \in x)(\exists t \in (\Sigma - \Sigma_c)^*)\delta(\sigma t, q') = q\}$.

For a state $x \in X$ (i.e., $x \subseteq Q$), we said that h is finer than T in x, denote $(h \leq T)|_x$, if

$$(\forall q, q' \in x) h(q) = h(q) \Rightarrow q =_T q'.$$

Denote the set of states satisfying the above condition as

$$X_m = \{x \in X : (h \leq T)|_x\}.$$

Denote the reachable states from states in $X' \subseteq X$ via strings in Σ'^* as

$$RS(X', \Sigma'^*) = \{x \in X : (\exists x' \in X')(\exists s \in \Sigma'^*)\xi(s, x') = x\}.$$

Theorem 3 G is on-line diagnosable if and only if

$$RS(\{Q\}, \Sigma_c^*) \cap X_m \neq \emptyset$$

Proof: Let us first prove by induction on the length of strings that for all $u \in \Sigma_c^*$,

$$S(u, Q) = \xi(u, Q).$$

For $u = \epsilon$, clearly

$$S(\epsilon, Q) = Q = \xi(\epsilon, Q).$$

Assume $S(u, Q) = \xi(u, Q)$ is true for all $u \in \Sigma_c^*$, $|u| \leq n$. Then for all $\sigma \in \Sigma_c$,

$$\begin{aligned}
& q \in S(u\sigma, Q) \\
\Leftrightarrow\ & (\exists s \in P^{-1}(u\sigma))(\exists q' \in Q)\delta(s, q') = q \\
\Leftrightarrow\ & (\exists w \in P^{-1}u)(\exists t \in (\Sigma - \Sigma_c)^*)(\exists q' \in Q)\delta(w\sigma t, q') = q \\
\Leftrightarrow\ & (\exists w \in P^{-1}u)(\exists t \in (\Sigma - \Sigma_c)^*)(\exists q' \in Q)(\exists q'' \in Q)\delta(w, q') = q'' \wedge \delta(\sigma t, q'') = q \\
\Leftrightarrow\ & (\exists q'' \in Q)(\exists t \in (\Sigma - \Sigma_c)^*)(\exists w \in P^{-1}u)(\exists q' \in Q)\delta(w, q') = q'' \wedge \delta(\sigma t, q'') = q \\
\Leftrightarrow\ & (\exists q'' \in Q)(\exists t \in (\Sigma - \Sigma_c)^*)q'' \in S(u, Q) \wedge \delta(\sigma t, q'') = q \\
\Leftrightarrow\ & (\exists q'' \in Q)(\exists t \in (\Sigma - \Sigma_c)^*)q'' \in \xi(u, Q) \wedge \delta(\sigma t, q'') = q \\
\Leftrightarrow\ & q \in \xi(\sigma, \xi(u, Q)) \\
\Leftrightarrow\ & q \in \xi(u\sigma, Q).
\end{aligned}$$

Hence,

$$\begin{aligned}
& G \text{ is on-line diagnosable} \\
\Leftrightarrow\ & (\exists u \in \Sigma_c^*)(\forall q, q' \in S(u, Q))h(q) = h(q') \Rightarrow q =_T q' \\
\Leftrightarrow\ & (\exists u \in \Sigma_c^*)(h \leq T)|_{\xi(u.Q)} \qquad \blacksquare \\
\Leftrightarrow\ & (\exists u \in \Sigma_c^*)\xi(u, Q) \in X_m \\
\Leftrightarrow\ & RS(\{Q\}, \Sigma_c^*) \cap X_m \neq \emptyset.
\end{aligned}$$

Since the number of states in X may reach $2^{|Q|}$, a reachability search in $\tilde{G}$ has complexity of $O(2^{|Q|})$ in the worst case. So in practice, we may not want to construct $\tilde{G}$ but rather to use the following algorithm to find a control u that diagnoses G.

Algorithm 2.

```
begin
  Input:
  read $G$;
  read $I$;
  read $T$;
  Initialization:
  $U := \{\epsilon\}$;
  $v(\epsilon) := I$;
  Recursive Search:
  2: for all $u \in U$ do begin
  for all $\sigma \in \Sigma_c$ do begin
  $v(u) := RS(v(u), (\Sigma - \Sigma_c)^*)$;
  if $(\forall q, q' \in v(u)) h(q) = h(q') \Rightarrow q =_T q'$ then go to 1
  else begin
  $U := U \cup \{u\sigma\}$;
  $v(u\sigma) := RS(v(u), \{\sigma\})$;
  end;
  end;
  $U := U - \{u\}$;
  end;
  go to 2;
  Output:
  1: write $u$;
  end.
```

This algorithm may not converge if G is not on-line diagnosable. However, as to be shown in the next section, if G is diagnosable, then the algorithm may find a control u much faster than first constructing $\tilde{G}$.

7. Exhaust Gas Recirculation System

In an automobile, an exhaust gas recirculation system is used to control the emission of oxides of nitrogen by adjusting the amount of exhaust gas to be recirculated into the engine. Because exhaust gas does not burn, the recirculation reduces the peak combustion temperatures. This in turn reduces the amount of oxides of nitrogen. The exhaust gas recirculation system is depicted in Figure 6.

The flow of exhaust gas is controlled by the exhaust gas recirculation valve. The flow of mixed exhaust gas, intake air and fuel is control by the throttle. The valve may fail: it can get stuck at open or get stuck at closed. To diagnose the valve failures, a sequence of control is issued and the percentage amount of oxides of nitrogen in the exhaust manifold is measured by an exhaust gas sensor. The system consists of six events.

α_1: open the valve;
α_2: close the valve;

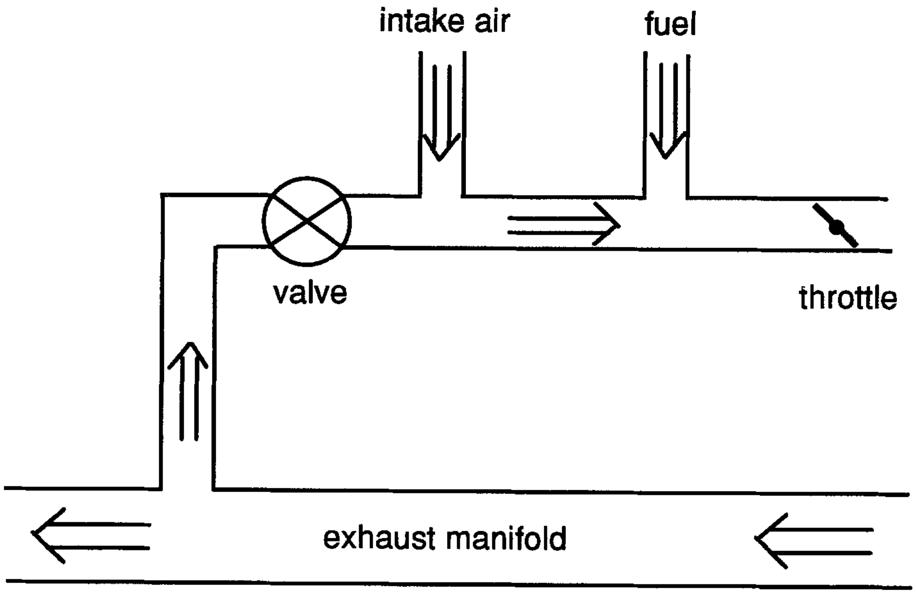

Figure 6.

α_3: the valve gets stuck at open;
α_4: the valve gets stuck at closed;
α_5: open the throttle;
α_6: close the throttle.

The valve may be in one of the following four states: normal-open (NO), normal-closed (NC), stuck-open (SO), and stuck-closed (SC). The state transition is described in Figure 7. On the other hand, the state of the throttle is either open or closed. The state diagram of the throttle is given in Figure 8.

When the valve and the throttle run concurrently and independently, the state of the exhaust gas recirculation system is a pair: (state of the valve, state of the throttle). There are $4 \times 2 = 8$ possible states as shown in Figure 9, where the states are numbered as follows.

state q_1: (the valve stuck-closed, the throttle closed);
state q_2: (the valve normal-closed, the throttle closed);
state q_3: (the valve normal-open, the throttle closed);
state q_4: (the valve stuck-open, the throttle closed);
state q_5: (the valve stuck-closed, the throttle open);
state q_6: (the valve normal-closed, the throttle open);
state q_7: (the valve normal-open, the throttle open);
state q_8: (the valve stuck-open, the throttle open).

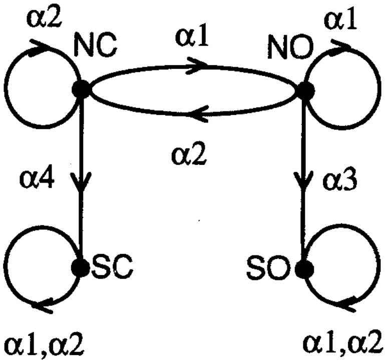

Figure 7.

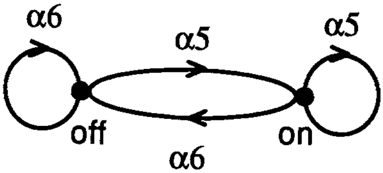

Figure 8.

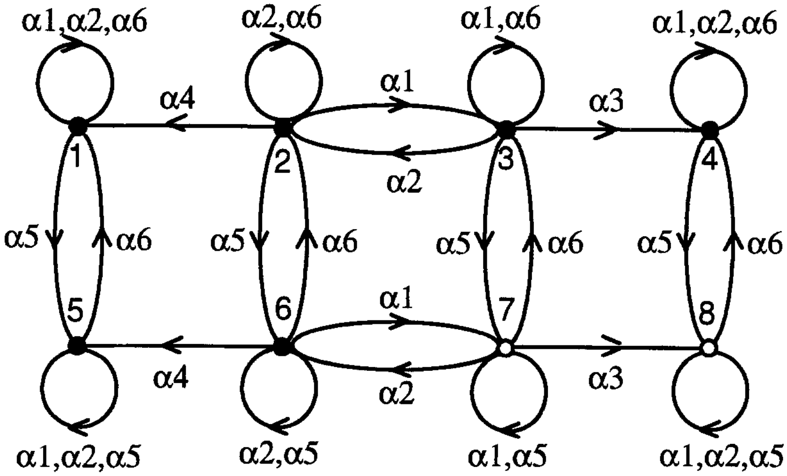

Figure 9.

When the system is in states q_7 or q_8, the throttle is open and the valve is open (normal-open or stuck-open) and hence the percentage amount of oxides of nitrogen decreases. While in all other states, the percentage amount of oxides of nitrogen will not decrease. To distinguish these two different situations, we use solid circle to denote states 1 through 6 in Figure 9.

The events $\alpha_1, \alpha_2, \alpha_5$, and α_6 are controllable because we can issue control to force these events. While the events α_3 and α_4 are uncontrollable, because we cannot prevent a failure from occurring.

Y and h describe the exhaust gas sensor, which tells us whether the percentage amount of oxides of nitrogen is decreasing or not. So, $Y = \{decreasing,\ not\ decreasing\}$ and

$$\begin{aligned}
h(q_1) &= not\ decreasing;\\
h(q_2) &= not\ decreasing;\\
h(q_3) &= not\ decreasing;\\
h(q_4) &= not\ decreasing;\\
h(q_5) &= not\ decreasing;\\
h(q_6) &= not\ decreasing;\\
h(q_7) &= decreasing;\\
h(q_8) &= decreasing.
\end{aligned}$$

Suppose we want to know if the valve is stuck-open. This is the case if G is in q_4 or q_8, hence the desired state partition is

$$T = \{\{q_1, q_2, q_3, q_5, q_6, q_7\}, \{q_4, q_8\}\}.$$

Assume that we have no prior knowledge on which state the system is in. In other words, $I = Q$. Then using Algorithm 2, we can find the control $u = \alpha_5\alpha_2$ that diagnoses G, because $S(u, I) = \{q_5, q_6, q_8\}$ and

$$(\forall q, q' \in S(u, I))h(q) = h(q') \Rightarrow q =_T q'.$$

On the other hand, $u' = \alpha_5\alpha_1$ does not diagnose G because $S(u', I) = \{q_5, q_7, q_8\}$ and if we take $q = q_7$ and $q' = q_8$, then $h(q) = h(q')$ but $q \neq_T q'$.

8. Conclusion

We studied both on-line and off-line diagnostics and proposed a general model for both types of diagnostics. We define on-line diagnosability and off-line diagnosability that capture the main requirements on diagnostics. For on-line diagnostics, we use a deterministic Moore automaton with partial state observation and no event observation. For off-line diagnostics, we use a nondeterministic Mealy automaton with no state observation and partial event observation. Although these assumptions are not critical to our diagnosability theory and can be relaxed, we have not found applications that require such relaxations. To illustrate the usefulness of this diagnosability theory, we applied it to two practical problems.

9. Acknowledgement

The author would like to thank the following researchers and engineers at Ford Motor Company for many insightful discussions: Joe Gormley, John Markee, Bill Rado, Dennis Rhee, Jack Tarlor and Carl Thatcher. Financial support from Ford and from the National Science Foundation under grant ECS-9213922 is also sincerely acknowledged.

References

R. Cieslak, C. Desclaux, A. Fawaz, and P. Varaiya. Supervisory control of discrete-event processes with partial observations. *IEEE Transactions on Automatic Control*, 33(3):249–260, 1988.

F. Lin, J. Markee, and B. Rado. Design and test of mixed signal circuits: A discrete-event approach, submitted to *32th IEEE Conference on Decision and Control*, 1993.

F. Lin and W. M. Wonham. On observability of discrete event systems. *Information Sciences*, 44(3):173–198, 1988.

C. M. Ozveren and A. S. Willsky. Observability of discrete event dynamic systems. *IEEE Transactions on Automatic Control*, 35(7):797–806, 1990.

R. J. Patton, R. N. Clark and P. M. Frank (editors). *Fault Diagnosis in Dynamic Systems: Theory and Application*. Prentice Hall, 1989.

P. J. Ramadge. Observability of discrete event systems. In *Proceedings of 25th IEEE Conference on Decision and Control*, pp. 1108–1112, 1986.

R. J. Ramadge and W. M. Wonham. Supervisory control of a class of discrete event processes. *SIAM J. Control and Optimization*, 25(1):206–230, 1987.

S. Tzafestas, M. Singh, and G. Schmidt (editors). *System Fault Diagnostics, Reliability and Related Knowledge-based Approaches, Volume 1, Fault Diagnostics and Reliability*. Kluwer Academic Publishers, 1987a.

S. Tzafestas, M. Singh, and G. Schmidt (editors). *System Fault Diagnostics, Reliability and Related Knowledge-based Approaches, Volume 2, Knowledge-based and Fault-Tolerant Techniques*. Kluwer Academic Publishers, 1987b.