# 15. SYSTEM-LEVEL DIAGNOSIS

**About This Chapter**

The advent of large, parallel computing systems containing hundreds or thousands of processing elements means that the problems associated with the testing and diagnosis of such systems are especially challenging and important. In this chapter we consider a formal model of system-level diagnosis in which one processing element is used to test and diagnose other processing elements. Using this model, several different measures of system diagnosability are defined and evaluated. Necessary and sufficient conditions on system structure to obtain defined levels of diagnosability are derived for the basic model and its various generalizations.

## 15.1 A Simple Model of System-Level Diagnosis

With the advent of VLSI, there has been much research and development related to large computing systems containing many processing elements connected in a network. In such systems an interesting possibility is their diagnosis using one subsystem (i.e., processing element) to diagnose other subsystems. A formal model for such diagnosis developed by Preparata, Metze, and Chien [Preparata *et al.* 1967], called the PMC model, has led to a large amount of research. This model is based upon the following three assumptions:

1. A system can be partitioned into units (called *modules*), and a single unit can individually test another unit.
2. On the basis of the responses to the test that is applied by a unit to another unit, the test outcome has a binary classification, "pass" or "fail" (i.e., the testing unit evaluates the tested unit as either fault-free or faulty).
3. The test outcome and evaluation are always accurate (i.e., a fault-free unit will be diagnosed as fault-free and a faulty unit will be diagnosed as faulty) if the testing unit is fault-free, but the test outcome and evaluation may be inaccurate if the testing unit itself is faulty.

With these assumptions a diagnostic system may be represented by a diagnostic graph in which each vertex (node) $v_i$ corresponds to a unit in the system, and a branch (arc) from $v_i$ to $v_j$ (denoted by $v_{ij}$) corresponds to the existence of a test by which unit $v_i$ evaluates unit $v_j$. The test outcome $a_{ij}$ associated with $v_{ij}$ is assumed to be as follows:

$a_{ij} = 0$ if $v_i$ and $v_j$ are both fault-free;

$a_{ij} = 1$ if $v_i$ is fault-free and $v_j$ is faulty;

$a_{ij} = \times$ (unspecified and indeterminate) if $v_i$ is faulty regardless of the status of $v_j$ (i.e., $\times$ can be 0 or 1).

The various test outcome situations are depicted in Figure 15.1.

Two implicit assumptions required by this assumed test outcome are that faults are permanent and that the tests applied by unit $v_i$ to unit $v_j$ can detect all possible faults in $v_j$.

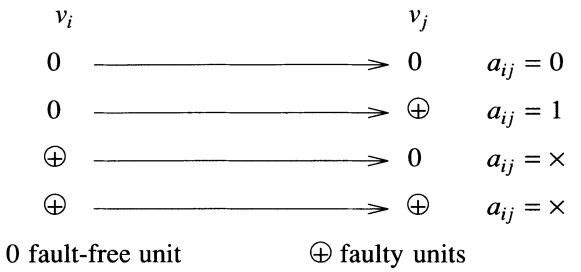



**Figure 15.1** Assumed test outcomes in the Preparata-Metze-Chien model

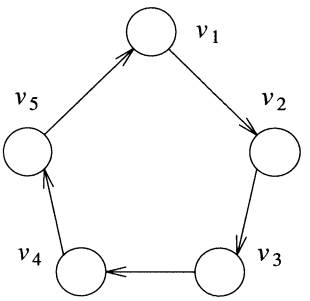
In the PMC model, faulty units can be identified by decoding the set of test outcomes, referred to as the *syndrome*, of the system. A fault in unit $v_i$ is *distinguishable* from a fault in unit $v_j$ if the syndromes associated with these two faults are different. The two faults are *indistinguishable* if their syndromes could be identical. These definitions can be directly extended to define distinguishable and indistinguishable multiple faults (i.e., sets of faulty units), sometimes referred to as *fault patterns*.

**Example 15.1:** Figure 15.2 shows a system with five units $v_1, ..., v_5$. The test syndromes shown in lines (a) and (b) correspond to the single faulty units $v_1$ and $v_2$ respectively. Since these two test syndromes have opposite values of $a_{51}$, these two faults are distinguishable. Line (c) shows the test syndrome associated with the multiple fault pattern $\{v_1,v_2\}$ (i.e., both $v_1$ and $v_2$ are faulty). This fault pattern is distinguishable from $v_2$ since lines (b) and (c) have opposite values of $a_{51}$. However, since the test syndromes in lines (a) and (c) may not be different, the single fault $v_1$ is indistinguishable from the multiple fault $\{v_1,v_2\}$. □

Two measures of diagnosability, *one-step diagnosability* and *sequential diagnosability*, were originally defined [Preparata *et al.* 1967]. A system of $n$ units is one-step $t$-fault diagnosable if all faulty units in the system can be identified without replacement, provided the number of faulty units does not exceed $t$. A system of $n$ units is sequentially $t$-fault diagnosable if at least one faulty unit can be identified without replacement, provided the number of faulty units does not exceed $t$.

Sequential diagnosability implies a multistep diagnostic procedure for the identification of all faulty units. In the first iteration one or more faulty units are identified and replaced by other units, which are assumed to be fault-free. After this replacement the test is rerun and additional faulty units may be identified. The process is repeated until all faulty units are identified and replaced, requiring at most $t$ iterations (steps). As previously stated, it is assumed that all replacement units are fault-free and that no faults occur during the testing process.

The following theorem presents some general *necessary* properties of the diagnostic graph required for one-step diagnosability.




| | $a_{12}$ | $a_{23}$ | $a_{34}$ | $a_{45}$ | $a_{51}$ | Faulty unit(s) |
|---|---|---|---|---|---|---|
| (a) | × | 0 | 0 | 0 | 1 | $v_1$ |
| (b) | 1 | × | 0 | 0 | 0 | $v_2$ |
| (c) | × | × | 0 | 0 | 1 | $\{v_1, v_2\}$ |

**Figure 15.2** A system and associated test outcomes

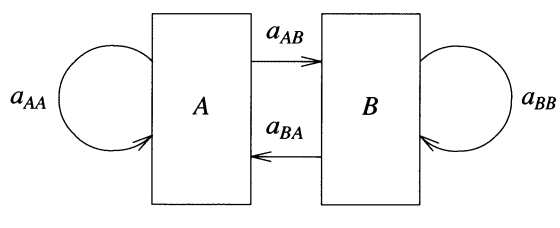
**Theorem 15.1:** In a one-step $t$-fault diagnosable system

a. There must be at least $2t+1$ units.

b. Each unit must be diagnosed by at least $t$ other units.

**Proof**

a. Suppose there are $n \leq 2t$ units. Then the vertices can be partitioned into two disjoint sets $A$ and $B$ each containing at most $t$ vertices. The diagnostic graph can then be represented as shown in Figure 15.3, where $a_{AA}$ is the set of connections within $A$, $a_{AB}$ is the set of connections from $A$ to $B$, $a_{BA}$ is the set of connections from $B$ to $A$, and $a_{BB}$ is the set of connections within $B$. Figure 15.3(b) shows the value of the test syndromes for the two disjoint fault patterns consisting of (1) all units in $A$ being faulty and (2) all units in $B$ being faulty.




(a)

| | $a_{AA}$ | $a_{AB}$ | $a_{BA}$ | $a_{BB}$ |
|---|---|---|---|---|
| (1) | × | × | 1 | 0 |
| (2) | 0 | 1 | × | × |

(b)

**Figure 15.3** Partition of system into two subsystems

Since no test outcome must have a different value for these two fault patterns, they are indistinguishable and hence the system is not one-step $t$-fault diagnosable.

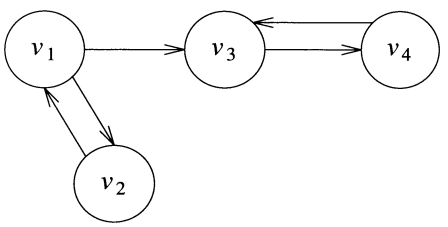
b. Suppose some module $v_i$ is tested by $k < t$ other modules $v_1, v_2, ..., v_k$. Consider the following two sets of faulty units:

$$A = \{v_1, v_2, ..., v_k\}$$

$$B = \{v_1, v_2, ..., v_k, v_i\}.$$

These fault conditions will produce indistinguishable test syndromes, and since both fault patterns contain at most $t$ faults, the system is not one-step $t$-fault diagnosable. □

The conditions of Theorem 15.1 are necessary but are not sufficient, as can be seen for the system of Figure 15.4(a). Since the test syndromes for fault patterns $\{v_1\}$ and $\{v_2\}$ may be identical, this system is not one-step one-fault diagnosable, although it does satisfy both of the necessary conditions of Theorem 15.1 for $t = 1$.




(a)

| Faulty unit | $a_{12}$ | $a_{13}$ | $a_{21}$ | $a_{34}$ | $a_{43}$ |
|---|---|---|---|---|---|
| $(v_1)$ | × | × | 1 | 0 | 0 |
| $(v_2)$ | 1 | 0 | × | 0 | 0 |
| $(v_3)$ | 0 | 1 | 0 | × | 1 |
| $(v_4)$ | 0 | 0 | 0 | 1 | × |

(b)

**Figure 15.4** A system and single fault test syndromes

However, the conditions of Theorem 15.1 can be used to show that a class of systems for which the number of vertices is $n = 2t + 1$ and each unit is tested by exactly $t$ other units is optimal (i.e., has the minimal number of testing links) for any one-step $t$-fault diagnosable system. Such a system has $m = nt$ testing links, which is minimal. One such optimal class of system is called a $D_{\delta t}$ system. In such a system there is a testing link from $v_i$ to $v_j$ if and only if $j = (i+\delta m) \bmod n$, where $n$ is the number of vertices, $\delta$ is an integer, and $m = 1, 2, ..., t$. Figure 15.5 shows such a system with $\delta = t = 2$ (i.e., a $D_{22}$ system). $D_{\delta t}$ systems in which the values of $\delta$ and $n = 2t + 1$ are relatively prime are optimal with respect to the number of testing links, for one-step $t$-fault diagnosability.

Some general classes of system that are sequentially $t$-fault diagnosable have also been developed. One such class of systems has $m = n + 2t - 2$ testing links and is illustrated by the system shown in Figure 15.6 for the case $t = 6$ and $n = 14$.

A *single-loop system* is a system in which each unit is tested by and tests exactly one other unit, and all units of the system are contained within one testing loop. For such

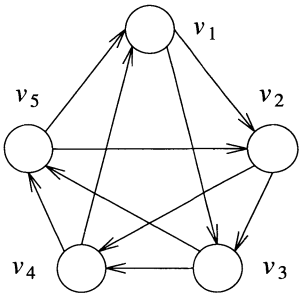



**Figure 15.5** An optimal 2-fault diagnosable system

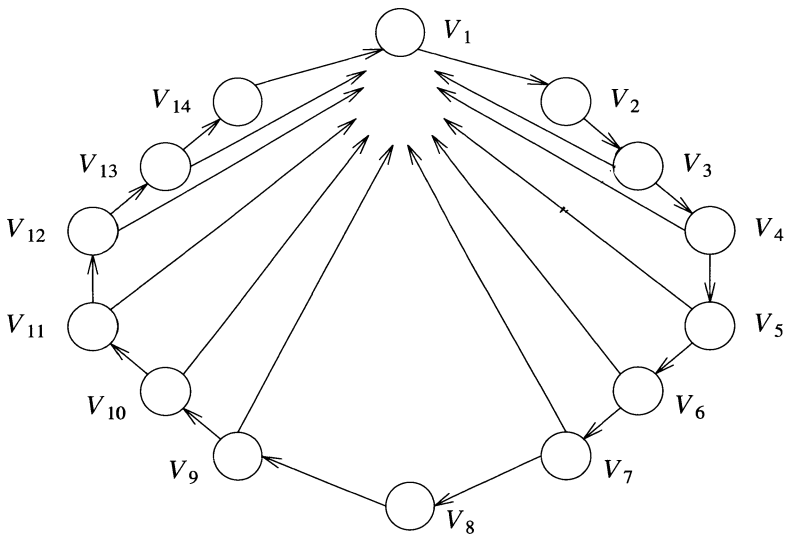



**Figure 15.6** A sequentially 6-fault diagnosable system

systems having $n$ units, if $t = 2b + c$, and $c = 0$ or 1, a necessary and sufficient condition for sequential $t$-fault diagnosability is

$$n \geq 1 + (b+1)^2 + c(b+1).$$

In order for a system to be sequentially $t$-fault diagnosable for any set of fault patterns $(F_1,F_2,...,F_r)$ that are not distinguishable, all fault patterns in this set must have a common element (i.e., $F_1 \cap F_2 \cap ... \cap F_r \neq \emptyset$). Since the system in the proof of

Theorem 15.1(a) does not satisfy this condition, any system with fewer than $2t + 1$ units is not sequentially $t$-fault diagnosable.

**Example 15.2:** We will examine the diagnostic capabilities of the system of Figure 15.7. Since $n = 5$, from Theorem 15.1(a) we know that the system is at most 2-fault diagnosable (either sequentially or in one step). Furthermore, since vertex 3 is only tested by vertex 2, it follows from Theorem 15.1(b) that the system is at most one-fault diagnosable in one step. The tables of Figure 15.7 show the test outcomes for all single and double fault patterns.

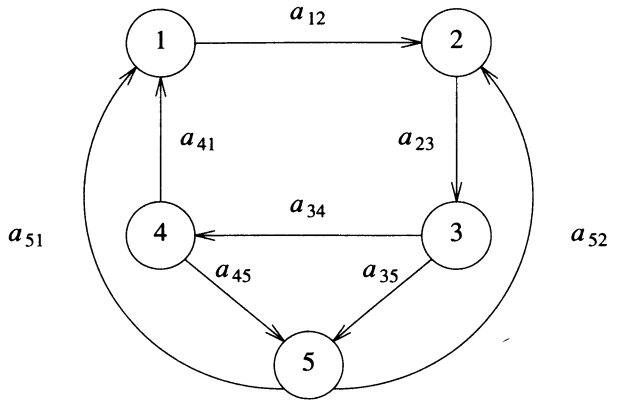
Since for each pair of fault patterns containing a single fault the fault syndromes are distinguishable (i.e., at least one test outcome has to have a different binary value for the two different fault patterns), this system is one-step one-fault diagnosable. To determine if the system is sequentially 2-fault diagnosable, we must examine and compare the test syndromes for all fault patterns containing two faults to determine distinguishable test syndromes. The set of fault patterns that do not satisfy the one-step distinguishability criteria are {(2,3),(2,4)}, which have a common element 2, and {(3,4),(3,5)}, which have a common element 3. Therefore the system is sequentially 2-fault diagnosable, since for any test outcome at least one module can definitely be determined as faulty and replaced. □

The PMC model of diagnosable systems is restricted to systems in which an individual unit is capable of testing another unit, and the measures of diagnosability are restricted to worst-case measures and to repair strategies in which only faulty units are replaced. It has not been possible to apply this simple model of system-level diagnosis directly to actual systems. However, it has laid the groundwork for subsequent research that has attempted to generalize the model and add more realistic constraints associated with actual systems. Because of the extensive research that has been done in this area and the lack of current practical applications, we will present a relatively broad overview of the general direction of this work and omit a detailed presentation of the mathematics involved.

## 15.2 Generalizations of the PMC Model

### 15.2.1 Generalizations of the System Diagnostic Graph

In the PMC model a test is applied by a single unit, which if faulty invalidates the test. This assumption can be generalized to include the possibility that application of a test requires the combined operation of more than one unit [Russell and Kime 1975a], as well as the possibility that a unit is known to be fault-free at the beginning of the diagnosis [Russell and Kime 1975b]. For example, the diagnosis of the IBM System/360 Model 50 has been described with a generalized diagnostic graph (GDG) [Hackl and Shirk 1965], shown in Figure 15.8. Here the units are represented as follows: $v_1$ is the main storage, $v_2$ is the ROM control, $v_3$ is the ALU, $v_4$ is the local storage, and $v_5$ is the channel. Each unit $v_i$ has associated with it a corresponding fault condition $f_i$. The test $t_1$ for the fault $f_1$ associated with unit $v_1$ will be valid even in the presence of other faulty units. Therefore the GDG has no arc labeled $t_1$. The single arc labeled $t_2$ from $f_1$ to $f_2$ indicates (as in the basic PMC model) that unit $v_1$ (previously verified by $t_1$) is sufficient to test and verify unit $v_2$. The two arcs labeled $t_3$ from $f_1$ to $f_3$ and from $f_2$ to $f_3$ respectively indicate that if either $v_1$ or $v_2$




| Faulty units | $a_{12}$ | $a_{23}$ | $a_{34}$ | $a_{35}$ | $a_{41}$ | $a_{45}$ | $a_{51}$ | $a_{52}$ |
|---|---|---|---|---|---|---|---|---|
| 1 | × | 0 | 0 | 0 | 1 | 0 | 1 | 0 |
| 2 | 1 | × | 0 | 0 | 0 | 0 | 0 | 1 |
| 3 | 0 | 1 | × | × | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 1 | 0 | × | × | 0 | 0 |
| 5 | 0 | 0 | 0 | 1 | 0 | 1 | × | × |

| Faulty units | $a_{12}$ | $a_{23}$ | $a_{34}$ | $a_{35}$ | $a_{41}$ | $a_{45}$ | $a_{51}$ | $a_{52}$ |
|---|---|---|---|---|---|---|---|---|
| (1,2) | × | × | 0 | 0 | 1 | 0 | 1 | 1 |
| (1,3) | × | 1 | × | × | 1 | 0 | 1 | 0 |
| (1,4) | × | 0 | 1 | 0 | × | × | 1 | 0 |
| (2,3) | 1 | × | × | × | 0 | 0 | 0 | 1 |
| (2,4) | 1 | × | 1 | 0 | × | × | 0 | 1 |
| (2,5) | 1 | × | 0 | 1 | 0 | 1 | × | × |
| (3,4) | 0 | 1 | × | × | × | × | 0 | 0 |
| (3,5) | 0 | 1 | × | × | 0 | 1 | × | × |
| (4,5) | 0 | 0 | 1 | 1 | × | × | × | × |

**Figure 15.7**

or both are faulty, then $t_3$ will be invalidated. Similarly tests $t_4$ and $t_5$ require $v_1$, $v_2$, and $v_3$ for them all to be fault-free.

A very general approach consists of using algebraic expressions to represent conditions under which a test is invalidated as well as to represent fault conditions detected by a test [Adham and Friedman 1977]. A set of fault patterns is described by a Boolean expression in the variables $\{f_1, f_2, \ldots, f_n\}$, where $f_i$ is 1 if $v_i$ is faulty and $f_i$ is 0 if $v_i$ is fault-free. Associated with any test $t_k$ are two Boolean functions, the invalidation function $I(t_k)$, which has the value 1 for any fault pattern that invalidates the test $t_k$,

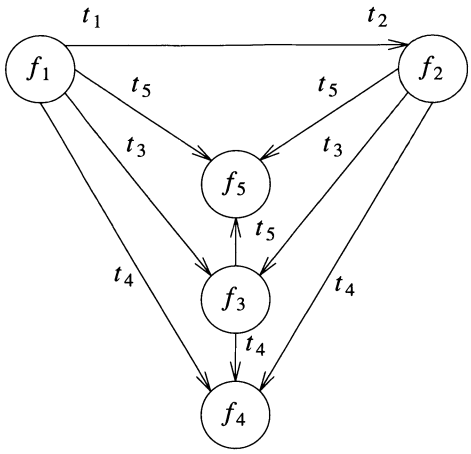



**Figure 15.8** Diagnostic graph of IBM System/360 Model

and the detection function $D(t_k)$, which has the value 1 for any fault pattern that is detected by $t_k$. Although this model can handle many cases that cannot be handled by graph-based models, it is too complex to be useful for large systems.

The complexities inherent in the algebraic model can be reflected in a much simpler, but less accurate, probabilistic model in which a test detects a fault $f_i$ with probability $p_i$ where $1 > p_i > 0$ [Fujiwara and Kinoshita 1978]. We shall now consider several similar types of generalization of the PMC model.

## 15.2.2 Generalization of Possible Test Outcomes

In the PMC model the outcome of a test applied to unit $v_j$ by unit $v_i$ is defined as shown in Figure 15.1. This assumption of the PMC model can be generalized in many ways, as shown in Figure 15.9 [Kavianpour 1978].

The different models represented in this table range from a "perfect" tester, $A_\infty$, in which the test outcome always corresponds to a perfect diagnosis of faulty units even when the testing unit is itself faulty, to the "0-information" tester, $A_0$, which never provides an assured-reliable test outcome even when the testing unit is fault-free. Many variants of the original model of Figure 15.1 as summarized in Figure 15.9 have been considered by various researchers.

The PMC model is represented by the column labeled $A_p$. The column labeled $A_0$ represents "zero information" since the test outcome is always unpredictable regardless of the condition of $v_j$ (the unit being tested) and $v_i$ (the unit testing $v_j$ ). The column labeled $A_\infty$ represents "total information" since the test outcome always represents accurately the condition of $v_j$. In column $A_{pT}$ the test outcome is unpredictable when $v_i$ is not faulty and $v_j$ is faulty. Therefore $v_a$ cannot detect all faults in $v_j$. This represents "incomplete" or "partial testing". In all of the seven models other than $A_0$ and $A_{pT}$ the test outcome always accurately reflects the condition of $v_j$ when $v_i$ is not

| $a_{ij}$ | $A_\infty$ | $A_W$ | $A_B$ | $A_y$ | $A_\mu$ | $A_\lambda$ | $A_p$ | $A_{pT}$ | $A_0$ |
|---|---|---|---|---|---|---|---|---|---|
| $0 \rightarrow 0$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | × |
| $0 \rightarrow \oplus$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | × | × |
| $\oplus \rightarrow 0$ | 0 | 1 | × | 0 | 0 | 1 | × | × | × |
| $\oplus \rightarrow \oplus$ | 1 | 1 | 1 | 0 | × | × | × | × | × |

**Figure 15.9** Different models of system diagnosis

faulty with differing assumptions when $v_i$ is faulty such as no information (the PMC model $A_p$), always indicating a fault ($A_w$), and never indicating a fault ( $A_y$).

### 15.2.3 Generalization of Diagnosability Measures

Originally only two measures of system-level diagnosability, one-step $t$-fault diagnosability and sequential $t$-fault diagnosability, were proposed. Both these measures imply a very conservative philosophy of system maintenance in which only faulty units are permitted to be replaced. In actuality there exists a trade-off between the necessity of repeating tests (in order to identify all the faulty units in a sequentially diagnosable system) and the necessity of replacing fault-free units. Consider, for example, the $n$−unit single-loop system shown in Figure 15.10, with the assumed test outcome defined by $a_{12} = a_{23} = 1$ and all other $a_{ij} = 0$. Assuming $n > t$, we can conclude that unit $v_2$ is faulty and units $v_i$, $v_{i+1}$, ..., $v_n$, $v_1$ are all fault-free where $i = t + 2$. Units $v_3$, ..., $v_{i-1}$ may be either faulty or fault-free. To determine the status of these units we could replace unit $v_2$ and then repeat the tests (possibly $t$ times in all) and eventually determine the status of all units while ensuring that no fault-free unit has ever been replaced. Alternatively, without repeating the tests we could replace units $v_2$, ..., $v_{i-1}$, ensuring that all faulty units have been replaced but perhaps replacing some fault-free units as well. Thus the trade-off between repeating tests (i.e., speed of diagnosis) and diagnostic accuracy (i.e., the number of fault-free units that are replaced) becomes apparent. To reflect this situation another measure of system-level diagnosis has been defined [Friedman 1975]. A system is $k$-step $t/s$ (read $t$-out-of-$s$) diagnosable if by $k$ applications of the diagnostic test sequence any set of $f \leq t$ faulty units can be diagnosed and repaired by replacing at most $s$ units. Clearly $s \geq t$ and $n \geq s$. Measures of the diagnosability of the system are the average or expected value of $s - f$ as well as the maximum value of $s - f$. These new measures have been considered for regular systems such as $D_{\delta t}$ systems, of which single-loop systems are a special case.

An interesting special case of $t/s$ diagnosability is when $s = t$. In this case all fault patterns consisting of $t$ faulty units are exactly diagnosed, but patterns consisting of $f < t$ faulty units may be inexactly diagnosed (requiring the replacement of at most $t - f$ fault-free units) [Kavianpour and Friedman 1978]. Consider the system of Figure 15.11. Since each unit is only tested by two other units, the system is not one-step 3-fault diagnosable. This is verified by the test outcome shown in

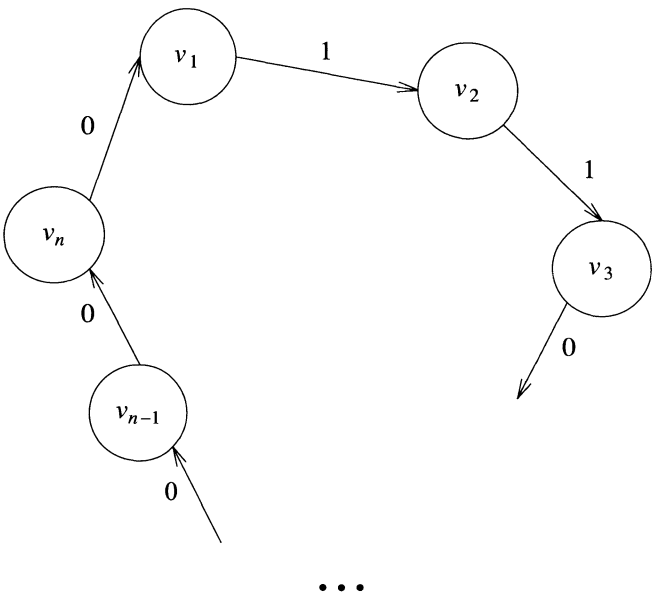



**Figure 15.10** A single-loop system with $n$ units

Figure 15.11(a). Assuming $t = 3$, we can deduce that unit $v_7$ is not faulty, since if it were faulty then $v_6$, $v_5$, and $v_4$ would also be faulty (as a consequence of the test outcomes ($a_{67}$=$a_{56}$=$a_{45}$=0), and hence there would be four faulty units, thus violating the upper bound $t = 3$. Since $v_7$ is fault-free, then $v_1$ and $v_2$ must be faulty (as a consequence of the test outcomes $a_{71} = a_{72} = 1$). In a similar manner we can then deduce that $v_6$, $v_5$, and $v_4$ are not faulty. Since $v_3$ is only tested by $v_1$ and $v_2$, both of which are faulty, we cannot determine whether $v_3$ is faulty or not. Thus this system is not one-step 3-fault diagnosable.

It can be shown, however, that the system is one-step 3/3 diagnosable. This implies that any fault pattern consisting of three faulty units can be exactly diagnosed, but some fault patterns of $f < 3$ faulty units can only be diagnosed to within three units. Consider the test outcome shown in Figure 15.11(b) produced by the set of three faulty units $\{v_1,v_3,v_4\}$. We can deduce that $v_2$ is not faulty, since if $v_2$ were faulty then $v_7$, $v_6$, and $v_5$ would also be faulty (as a consequence of the test outcomes $a_{72} = a_{67} = a_{56} = 0$), thus violating the upper bound $t = 3$. Since $v_2$ is not faulty, $v_3$ and $v_4$ are faulty (as a consequence of the test outcomes $a_{23} = a_{24} = 1$). Similarly we then deduce that $v_7$ is not faulty and consequently $v_1$ is faulty. We have thus identified the set of three faulty units. It can be shown that this can always be done for any set of three faulty units for the system shown. It is thus apparent that $t/t$ diagnosability necessitates fewer testing branches than $t$–fault diagnosability, thus again

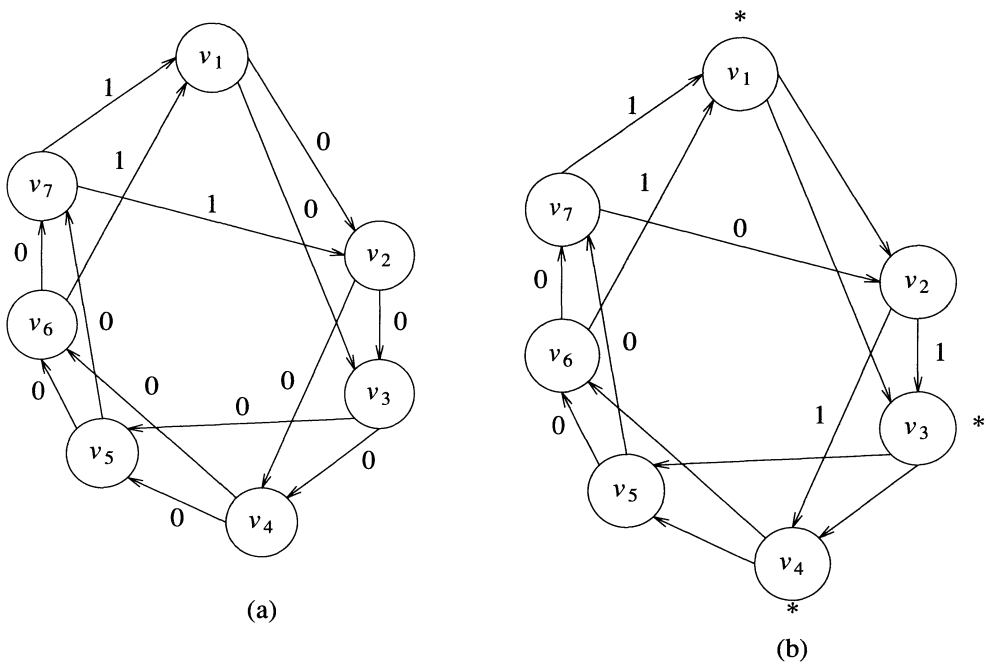



**Figure 15.11** A system demonstrating *t*/ *t* diagnosability

demonstrating the inherent trade-off in system-level diagnosis between accuracy of diagnosis and system complexity.

Many other generalizations of the PMC model have been studied. Such generalizations allow constraints encountered in actual systems to be more closely modeled. However, additional extensions and modifications are necessary to make the model applicable to actual systems [Friedman and Simoncini 1980].

The assumption that a unit can test other units requires complete access to the units being tested. This may necessitate a complex interconnection network. Testing links represent logical interconnections, and the directed graph is a logical representation of the diagnostic capabilities of a system. Consequently, a directed graph is not necessarily a simplified representation of a system's data-flow structure. It must still be determined what types of internal system organizations can most efficiently support the diagnostic procedures implied by a directed graph. Modeling of the diagnostic phase as well as normal operation of actual systems requires additional attention. An integrated approach to the modeling of fault-tolerant computing systems should consider both normal and diagnostic operations as well as reconfiguration. Thus, despite a considerable amount of work in this research area, practical applications still seem quite remote.

# REFERENCES

[Adham and Friedman 1977] M. Adham and A. D. Friedman, "Digital System Fault Diagnosis," *Journal of Design Automation & Fault-Tolerant Computing*, Vol. 1, No. 2, pp. 115-132, February, 1977.

[Barsi *et al.* 1976] F. Barsi, F. Grandoni, and P. Maestrini, "A Theory of Diagnosability of Digital Systems," *IEEE Trans. on Computers*, Vol. C-25, No. 6, pp. 885-893, June, 1976.

[Blount 1977] M. Blount, "Probabilistic Treatment of Diagnosis in Digital Systems," *Proc. 7th Annual Intn'l. Conf. on Fault-Tolerant Computing*, pp. 72-77, June, 1977.

[Dahbura and Masson 1984] "An $0(n^{2.5})$ Fault Identification Algorithm for Diagnosable Systems," *IEEE Trans. on Computers*, Vol. C-33, No. 6, pp. 486-492, June, 1984.

[Friedman 1975] A. D. Friedman, "A New Measure of Digital System Diagnosis," *Digest of Papers 1975 Intn'l. Symp. on Fault-Tolerant Computing*, pp. 167-169, June, 1975.

[Friedman and Simoncini 1980] A. D. Friedman and L. Simoncini, "System-Level Fault Diagnosis," *Computer*, pp. 47-53, March, 1980.

[Fujiwara and Kinoshita 1978] H. Fujiwara and K. Kinoshita, "Connection Assignment for Probabilistically Diagnosable Systems," *IEEE Trans. on Computers*, Vol. C-27, No. 3, pp. 280-283, March, 1978.

[Hackl and Shirk 1965] F. J. Hackl and R. W. Shirk, "An Integrated Approach to Automated Computer Maintenance," *IEEE Conf. on Switching Theory and Logical Design*, pp. 298-302, October, 1965.

[Hakimi and Nakajima 1984] S. L. Hakimi and K. Nakajima, "On Adaptive Systems Diagnosis," *IEEE Trans. on Computers*, Vol. C-33, No. 3, pp. 234-240, March, 1984.

[Kavianpour 1978] A. Kavianpour, "Diagnosis of Digital System Using *t/s* Measure," Ph.D. Thesis, University of Southern California, June, 1978.

[Kavianpour and Friedman 1978] A. Kavianpour and A. D. Friedman, "Efficient Design of Easily Diagnosable Systems," *3rd USA-Japan Computer Conf.*, pp. 14.1-14.17, 1978.

[Kreutzer and Hakimi 1987] "System-Level Fault Diagnosis: A Survey," *Microprocessing and Microprogramming*, Vol. 20, pp. 323-330, 1987.

[Mallela and Masson 1978] S. Mallela and G. M. Masson, "Diagnosable Systems for Intermittent Faults," *IEEE Trans. on Computers*, Vol. C-27, No. 6, pp. 560-566, June, 1978.

[Preparata *et al.* 1967] F. P. Preparata, G. Metze, and R. T. Chien, "On the Connection Assignment Problem of Diagnosable Systems," *IEEE Trans. on Electronic Computers*, Vol. EC-16, No. 6, pp. 848-854. December, 1967.

[Russell and Kime 1975a] J. D. Russell and C. R. Kime, "System Fault Diagnosis: Closure and Diagnosability With Repair," *IEEE Trans. on Computers*, Vol. C-24, No. 11, pp. 1078-1088, November, 1975.

[Russell and Kime 1975b] J. D. Russell and C. R. Kime, "System Fault Diagnosis: Masking, Exposure, and Diagnosability Without Repair," *IEEE Trans. on Computers*, Vol. C-24, No. 12, pp. 1155-1161, December, 1975.

# PROBLEMS

**15.1** Consider a diagnostic graph consisting of a loop of $n$ modules.

a. Prove that such a system is one-step $t$-fault diagnosable only for $t < 2$.

b. Prove that such a system is one-step 2/3 fault diagnosable if $n > 6$ by showing that for any fault pattern produced by two or fewer faults, at least $n - 3$ modules can be ascertained to be properly functioning under the assumption that at most two modules can be faulty.

**15.2** Consider a system whose diagnostic graph has five nodes {0,1,2,3,4} and an edge from $i$ to $(i + 1)$ mod 5 and from $i$ to $(i + 2)$ mod 5 for all $i$.

a. Prove that such a system is one-step two-fault diagnosable and sequentially two-fault diagnosable.

b. What is the maximum number of edges that can be removed from this graph so that it is still one-step two-fault diagnosable, or so that it is still sequentially two-fault diagnosable?

**15.3**

a. Prove that the system shown in Figure 15.12, is one-step 3/3 diagnosable.

b. Prove that if any edge is removed the system is not one-step 3/3 diagnosable.

c. For the test outcome shown in Figure 15.12, assuming $t = 3$, determine the set of faulty modules to within $s = 3$ units.

**15.4** For the system shown in Figure 15.13 and for each of the models of Figure 6.9

a. Determine the maximum value of $t$ for which the system is one-step $t$ fault diagnosable.

b. Determine the maximum value of $t^1$ for which the system is sequentially $t^1$-fault diagnosable.

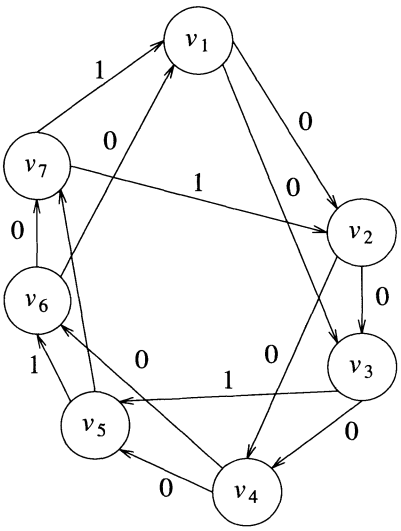



**Figure 15.12** Problem 15.3

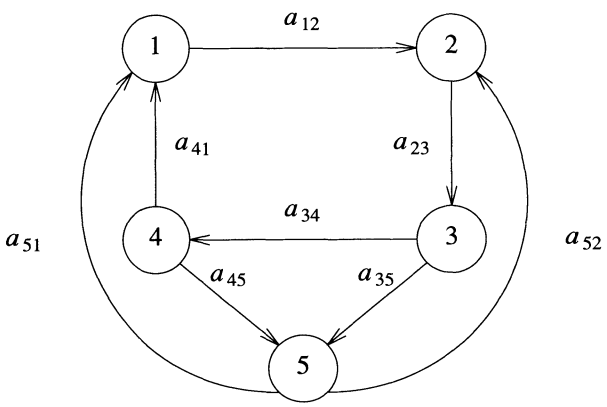



**Figure 15.13** Problem 15.4