

INFORMATION TO USERS

This dissertation was produced from a microfilm copy of the original document. While the most advanced technological means to photograph and reproduce this document have been used, the quality is heavily dependent upon the quality of the original submitted.

The following explanation of techniques is provided to help you understand markings or patterns which may appear on this reproduction.

1. The sign or "target" for pages apparently lacking from the document photographed is "Missing Page(s)". If it was possible to obtain the missing page(s) or section, they are spliced into the film along with adjacent pages. This may have necessitated cutting thru an image and duplicating adjacent pages to insure you complete continuity.
2. When an image on the film is obliterated with a large round black mark, it is an indication that the photographer suspected that the copy may have moved during exposure and thus cause a blurred image. You will find a good image of the page in the adjacent frame.
3. When a map, drawing or chart, etc., was part of the material being photographed the photographer followed a definite method in "sectioning" the material. It is customary to begin photoing at the upper left hand corner of a large sheet and to continue photoing from left to right in equal sections with a small overlap. If necessary, sectioning is continued again — beginning below the first row and continuing on until complete.
4. The majority of users indicate that the textual content is of greatest value, however, a somewhat higher quality reproduction could be made from "photographs" if essential to the understanding of the dissertation. Silver prints of "photographs" may be ordered at additional charge by writing the Order Department, giving the catalog number, title, author and specific pages you wish reproduced.

University Microfilms

300 North Zeeb Road
Ann Arbor, Michigan 48106

A Xerox Education Company

73-6946

YEH, Kou-Min, 1937-
A THEORETIC STUDY OF FAULT DETECTION PROBLEMS
IN SEQUENTIAL SYSTEMS.

The University of Michigan, Ph.D., 1972
Engineering, electrical

University Microfilms, A XEROX Company, Ann Arbor, Michigan

A THEORETIC STUDY OF FAULT DETECTION
PROBLEMS IN SEQUENTIAL SYSTEMS

By

Kou-Min Yeh

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Computer, Information and Control Engineering)
in The University of Michigan
1972

Doctoral Committee:

Associate Professor John F. Meyer, Chairman
Professor William A. Porter
Professor Norman R. Scott
Assistant Professor Bernard P. Zeigler

PLEASE NOTE:

**Some pages may have
indistinct print.**

Filmed as received.

University Microfilms, A Xerox Education Company

ACKNOWLEDGEMENT

The author wishes to express his sincere appreciation to Professors John F. Meyer, William A. Porter, Norman R. Scott and Bernard P. Zeigler for serving on his doctoral committee. Special gratitude is due his committee chairman Professor John F. Meyer for his inspiring guidance, counsel and constant encouragement through the period of this research.

He also wishes to thank the Product Engineering Management of Burroughs Corporation at the Plymouth Plant for the opportunity of employment while pursuing this doctoral program.

This work was performed in part for the Jet Propulsion Laboratory, California Institute of Technology, sponsored by the National Aeronautics and Space Administration under contract NAS7-100 and for the National Aeronautics and Space Administration under research grant NGR23-005-463 [35], [36].

The author also wishes to thank Miss Joyce Doneth for her excellent typing on early drafts and most of the final manuscript and to Mrs. Shirley Bretting and Mr. Thomas Hadfield for their help in final typing and corrections.

Finally, the author is very grateful to his wife Betty and his son Christopher for their patience and understanding throughout this research period.

TABLE OF CONTENTS

	Acknowledgements	<u>Page</u> ii
	List of Tables	v
	List of Illustrations	vi
	<u>Chapter</u>	
I	Introduction	1
	1. 1 Review of Literature and Historic Backgrounds	3
	1. 2 Problem Statement and Research Objectives	6
II	Fundamental Concepts and Definitions	10
	2. 1 Definitely Homable and Definitely Diagnosable Machines	18
	2. 2 Sequence Generators and Linear Machines	27
	2. 3 Machine Classifications	40
III	Diagnosable Machine Realization of Sequential Behavior	42
	3. 1 Machine Augmentation as a Machine Realization Problem	43
	3. 2 Control Input Augmentation	47
	3. 3 Test Output Augmentation	54
	3. 4 State-Output Augmentation	73
	3. 5 Summary	115

<u>Chapter</u>	<u>Page</u>
IV Regular Expression Representation of Fault Detection Sets	117
4.1 Introduction	118
4.2 Memory Fault Detection	120
4.3 Regular Representation of q-detection Sets	126
4.4 Multiple Fault Test Sets	140
V Relations of Faults and Easily Testable Machines	151
5.1 Introduction	152
5.2 Relations of Faults	155
5.3 Conditions of Fault Detection and a Class of Easily Detectable Faults	175
5.4 Strongly Connected and Diagnosable Machines	187
5.5 Definite Machines	196
VI Summary and Conclusions	218
References	233

LIST OF TABLES

		<u>Page</u>
Table 3. 1	Machinè M_4' of Example 3. 2	66
Table 3. 2	Machine M_4 of Example 3. 2	70
Table 3. 3A	State diagrams of M' and M for $k=3$ to $k=8$	96
Table 3. 3B	State diagrams of M' and M for $k=9$ to $k=12$	97
Table 3. 4	Values of functions $I_k(p)$	107
Table 3. 5	Upper bounds on the number of states need to be increased for minimum ouput diagnosable realizations using state-output augmentation	111

LIST OF ILLUSTRATIONS

		<u>Page</u>
Figure 2. 1	Machine M_1 of Example 2. 1	16
Figure 2. 2	Successor State Pairs of $\{q, r\}$ Under x with Repeated Successor State Pair	20
Figure 2. 3	Machine Classification Diagram	41
Figure 3. 1	Machine M_1' and a Diagnosable Realization M_1	45
Figure 3. 2	Machine M_2' of Example 3. 1	48
Figure 3. 3	A Diagnosable Realization of M_2' of Example 3. 1	49
Figure 3. 4	An 8-state, Single Input and Binary Output Machine with a DS of Length 3	52
Figure 3. 5	Machine M_3' and a Diagnosable Realization M_3	53
Figure 3. 6	T_0 of Example 3. 2	67
Figure 3. 7	G_{o_1} and G_{o_2} After Step(3) of Example 3. 2	68
Figure 3. 8	G_{o_1} and G_{o_2} After Step(4) of Example 3. 2	69
Figure 3. 9	Machine M_5' of Example 3. 3	85
Figure 3. 10	A Diagnosable Realization of M_5' of Example 3. 3	87
Figure 3. 11	M_6' and One of Its Diagnosable Realizations M_6 of Example 3. 4	101
Figure 3. 12	Machine M_7' and a Diagnosable Realization M_7 of Example 3. 5	114

		<u>Page</u>
Figure 4. 1	Example of Memory Faults	124
Figure 4. 2	Machine N and Fault f of Example 4. 3	137
Figure 4. 3	Machines M and M^μ	143
Figure 5. 1	Repeated Successor State Pair of $(q, \mu(q))$ Under x	179
Figure 5. 2	Example of Proper Memory Faults in a Machine Which are Not q-detectable	186
Figure 5. 3	Flow Chart of Algorithm 5. 1	193
Figure 5. 4	Definite Machine M and Fault Set $F=\{\mu, \mu'\}$ of Example 5. 5	210
Figure 5. 5	A Non-definite Fault μ'' of M	212

Chapter I

INTRODUCTION

This dissertation is concerned with some theoretical aspects of the hardware fault diagnosis problem in digital switching systems. Traditionally, the study of this problem has been divided into separately considering combinational systems and sequential systems. It can be fairly said that, for the most part, difficulties in fault diagnosis of combinational systems are well understood and have been practically resolved. On the other hand, efforts of trying to extend results obtained in combinational systems to sequential systems have met only partial success and the problem of fault diagnosis in sequential systems remains essentially unsolved.

During the last few years, the use of large scale integrated circuits (LSIC) chips in digital switching systems has increased tremendously. Relative to the problem of fault diagnosis, the impact of this technology has been a mixed blessing. On the positive side, the need to determine a failure to a gate or flip-flop level has been completely eliminated. Furthermore, the cost of adding extra logic in an LSIC chip for the purpose of fault diagnosis has been relatively insignificant. However, several problems have arisen. One primary limitation on an LSIC chip is usually the number of pins (external terminals) which often severely restricts the ability of quickly determining the presence of a failure inside a chip. Since a formerly regarded subsystem may now

be just simply a component, almost all of the so called "random logic" chips are sequential in nature (i.e. containing memories and internal feedback lines). Thus any assumption that a purely combinational systems approach will satisfy most of the LSIC testing requirements is totally unrealistic. Furthermore, the yields of LSIC manufacturing are usually low (typically only 10% of the total units processed are usable) and any suggestion that no weird type faults can occur without analysis of individual circuit is obviously just a wishful thinking.

These facts and observations motivate this study of fault detection problem in sequential systems. Although the concept of fault diagnosis usually means fault detection and distinction, we will use "diagnosis" and "detection" interchangeably in this investigation. This somewhat abuse in terminology is intended to underlie the fact that results obtained here are applicable in general to fault diagnosis and to emphasize the increasingly important role of fault detection in the area of fault diagnosis of sequential systems. To put our research and contributions in a proper perspective, a review of literature and historic background is now presented.

Section 1.1 Review of Literature and Historic Backgrounds.

The most fundamental approach to the problem of fault diagnosis in combinational networks is a truth table method [28] in which all input combinations of the network are considered. An analysis procedure has also been developed which incorporates the network structure into an output Boolean expression [43] from which a fault table can be constructed. Although these methods give rise to optimum solutions, the amount of computation required is usually large so that their application is generally limited to small circuits. Armstrong [3] has used the concept of one-dimensional "Path Sensitizing " for analyzing a network and developed a procedure for deriving near optimal test sets for logical failures of stuck-at-1 and stuck-at-0. Roth [45] generalized this idea and formulated a procedure called D-algorithm which guarantees to generate a test for a fault if a test exists. More recently, Sellers et al [47] have used the concept of Boolean difference to derive test sets for combinational networks. Among these techniques, the D-algorithm has recently gained popularity and several successful implementations resulted in efficient computation have been reported [8], [46].

The more fundamental problem of determining properties of combinational systems' behavior and structure conducive to fault tolerance, detection and location has been investigated recently by F. G. Gray [21]. His major contributions relative to the fault diagnosis problem have been a classification of combinational behaviors and structures according to

their "inherent" fault detectability and a generalization of the usual notion of fault location to the concept of partitioning a system under test into a definitely faulty set, an indeterminate set and a definitely fault-free set [22] .

A natural attempt to solve the problem of fault diagnosis in sequential networks is the extension of results obtained in combinational networks. This was first done by Galey, Norby and Roth [16] where they proposed to break the feedback loops in a sequential network and derived test sequences using the path-sensitizing concept. The technique does not work well when the network becomes sophisticated. Extensions of D-algorithm to sequential networks have been reported by Kubo [33] , Putzulu and Roth [44] , and Breuer [10] . The basic approach they took here is that a sequential network can be regarded as a cascade connection of duplicated copies of a combinational network. The types of failures detected by these methods are limited to those whose detection do not depend on initial state.

Techniques widely practiced in industry involve randomly selecting test sets and simulating these test sets to determine which failures are detected by them. These methods are mostly based on the digital fault simulation work pioneered by the late Professor Seshu [48] . Another technique using physical fault simulation was first employed in the compilation of fault dictionary for the maintenance of Bell Telephone's No. 1 ESS central control as described by Tsiang and Ulrich [51] . In

the last technique, the test sets are manually derived by engineers who analyze each individual circuits.

The most fundamental technique in the diagnosis of sequential systems was first proposed by Hennie [26]. He used the concept of identifying initial state and final state at each step of test to verify the behavior of the network under test. The technique becomes very complicated if the network does not have a distinguishing sequence. This method was later improved by several researchers, most notably Kime [29] and Kohavi and Kohavi [31]. Another important work in this area is a "synthesis for diagnosability" point of view adopted by Kohavi and Lavallee [32] in which they proposed methods of modifying a given machine so that the modified machine has many distinguishing sequences.

The discussion presented above is not intended as an exhaustive survey of literature, but rather as a representative sampling of various contributions made in the area of fault diagnosis in digital switching systems. Extensive surveys of literature have been made by Short [50] and more recently by Bennetts and Lewin [4].

Section 1.2 Problem Statement and Research Objectives.

The purpose of this research is to determine fundamental properties of sequential systems which are conducive to easy testing and to consider how some of these properties can be incorporated into the design of the proposed system. To accomplish this goal, the approach to be taken is system theoretic in the sense that formal model of sequential machine (finite automaton) is used to represent the system and formal methods are used in studying this model. Specifically, the following questions are considered:

- i) Investigate properties of sequential machines that relate to "inherent" fault diagnosability in the sense that the behavior can be easily verified and classify these machine according to some measure of "easiness".
- ii) Determine methods of realizing (simulating) machines (or behavior) that are not diagnosable by diagnosable machines using augmentation to the specified input-output behavior.
By diagnosable, in this context, we mean the machine possesses a distinguishing sequence.
- iii) Given a known set of faults in a machine, determine conditions under which the given machine can be tested against the occurrence of any fault in this set and, if testable, determine an optimum test set.

- iv) Investigate properties of machine structure and behavior that are conducive to efficient fault detection when knowledge of the faulty machine structures is included.

Generally speaking, these questions fall into two categories. In the first category, questions i) and ii) are concerned with the problem of behavior checking as initiated by Hennie [26] and our results in this area can be regarded as extensions of work previously reported by Kohavi and Lavalley [32]. Chapter 2 is devoted to question i) where the properties of possessing distinguishing sequences and homing sequences in sequential machines are investigated. Using the abundance of such sequences as a basis of machine classification, the result obtained is a partially ordered set of machine classes where the partial ordering is simply the natural set containment. Such classification is useful in that it permits tradeoffs between hardware complexity and efficiency of diagnostic test during the design stage of a system. To answer question ii), the problem of diagnosable machine realizations is solved in Chapter 3 by considering augmentation to the input set, output set and state-output set, respectively. Our primary contributions here are considered to be 1) formalization of the notion of machine modification to obtain a distinguishing sequence to that of a diagnosable machine realization, 2) development of an input augmentation technique which can lead to optimal diagnosable realization, 3) development of an output augmentation method which results in a special diagnosable

realization using a relatively small number of output symbols, and 4) development of state-output augmentation techniques which allow potential tradeoffs between the number of test outputs and the number of states.

In the second category, questions iii) and iv) are concerned with the study of the effects of changes in machine structure (due to faults) on behavior relative to the problem of fault detection. Investigation of these questions is motivated by the fact that in practice, only more limited types of faults can occur in a physically realized system. To answer question iii), Chapter 4 discusses the problem of representation and minimization of test sets in sequential systems. The class of faults considered here is restricted to faults which represent permanent changes in the memory structure of the system. This restriction is made primarily to simplify discussion and the results obtained can be generalized to other classes of faults. Chapter 5 is devoted to question iv) of the problem statement and its development is essentially applications of the fault detection concept and regular representation of fault detection sets developed in Chapter 4. The important contributions in this category are considered to be the following:

- 1) A concept of fault detection in terms of an initial state.
- 2) A representation method of fault detection set in sequential system in terms of regular expressions. This provides a

means of computing test sets using mechanical manipulation of regular expressions.

- 3) A method of computing optimal test set where an upper bound on the length of fault detection sequences that need to be considered can be determined prior to the computation of a test set.
- 4) Methods of determining fault equivalence and fault dominance relations of faults without explicitly computing all fault detection sequences.
- 5) Development of illustrative applications of the regular representation of fault detection sets to the study of fault classes and machine classes which are conducive to easy testing.

Chapter 6 summarizes the results obtained in each of the questions studied, and discusses open problems for future study.

Chapter II

FUNDAMENTAL CONCEPTS AND DEFINITIONS

This chapter first reviews several basic notions of sequential machines related to the fault detection problems informally introduced in the last chapter in order to precisely establish the terminology and notation used in this dissertation. Machine properties conducive to testing and classes of machines having these properties are then discussed with some detail.

Definition 2.1 A Mealy sequential machine is a system

$M = (I, Q, Z, \delta, \omega)$ where

- i) I is a finite set of input symbols,
- ii) Q is a finite set of states,
- iii) Z is a finite set of output symbols,
- iv) $\delta: Q \times I \rightarrow Q$, the transition function of M ,
- v) $\omega: Q \times I \rightarrow Z$, the output function of M .

A Moore sequential machine is as above except that

- v') $\omega: Q \rightarrow Z$.

Since a Moore machine can be regarded as a special type of Mealy machine and the transformation between a Moore model and a Mealy model is well known [39], we will consider only Mealy sequential machines in all the discussions unless explicitly stated otherwise.

To describe the behavior of a sequential machine $M = (I, Q, Z, \delta, \omega)$, let I^+ denote the set of all finite length nonnull sequences of elements from I and let $\bar{\delta}$ denote the extension of δ to $Q \times I^*$ where $I^* = I^+ \cup \{\Lambda\}$ (Λ is the null sequence).

Definition 2.2 If $M = (I, Q, Z, \delta, \omega)$ is a sequential machine and $q \in Q$, the behavior of M for initial state q is the function

$$\beta_q: I^+ \rightarrow Z$$

where, if $x = a_1 a_2 \dots a_n$,

$$\beta_q(x) = \omega(\bar{\delta}(q, a_1 a_2 \dots a_{n-1}), a_n).$$

Definition 2.3 The behavior of a sequential machine M with states Q is the set of functions

$$B_M = \{\beta_q \mid q \in Q\}.$$

Thus, regarding the usual notions of state and machine "equivalence", q is equivalent to r ($q \equiv r$) if $\beta_q = \beta_r$; M is equivalent to M' ($M \equiv M'$) if $B_M = B_{M'}$. A machine M is reduced if $\forall q, r \in Q$, whenever $\beta_q = \beta_r$ then $q = r$.

When considering procedures for diagnosing faults in sequential systems, such procedures can often be simplified if it is possible to infer the initial state of the system, given the output response to some

distinguished input sequence. Input sequences with this property were first considered by Moore [40] and are defined as follows. Let $\hat{\beta}_q$ be the sequence to sequence behavior of M for initial state q, that is

$$\hat{\beta}_q: I^+ \rightarrow Z^+$$

where

$$\hat{\beta}_q(a_1 a_2 \dots a_n) = \beta_q(a_1) \beta_q(a_1 a_2) \dots \beta_q(a_1 a_2 \dots a_n),$$

then

Definition 2.4 If M is a sequential machine, an input sequence x is a distinguishing sequence (DS) of M if, for all $q, r \in Q$

$$\hat{\beta}_q(x) = \hat{\beta}_r(x) \text{ implies } q = r.$$

Although possession of a distinguishing sequence may be only one of several properties required to solve some given diagnosis problem, it is a major property of interest in the discussion that follows and accordingly, with some abuse of terminology, we will say that a machine M is diagnosable if, for some input sequence x, x is a DS of M. The order of diagnosability of a diagnosable machine is the length of a shortest distinguishing sequence. If we let

$$\lg(x)$$

denote the length of $x \in I^*$, then we say M is k-diagnosable if M is diagnosable and the order of diagnosability is k, i. e.

$$k = \min\{\lg(x) \mid x \text{ is a DS of } M\}.$$

If M is k -diagnosable, an upper bound on the order of diagnosability has been given by Gill [18], i. e.

$$k \leq (n-1)n^n \quad (2.1)$$

where n is the number of states of M . Although it is possible to obtain a smaller bound by using a more refined argument, the least upper bound is still yet to be found. Since we will discuss methods of reducing these upper bounds in a latter chapter, we turn now, instead to the other problem of establishing the greatest lower bound of the order of diagnosability. If ρ is a real number, let $\lceil \rho \rceil$ denote the least integer greater than or equal to ρ .

Lemma 2.1 If M is a reduced machine with n states and p outputs and $x \in I^+$ is a distinguishing sequence of M , then

$$\lg(x) \geq \lceil \log_p n \rceil. \quad (2.2)$$

Proof: Consider any $x \in I^+$ with $\lg(x) = m < \lceil \log_p n \rceil$. It follows that $p^m < n$. Since $\lg(\hat{\beta}_q(x)) = \lg(x) = m$ for any $q \in Q$, the number of different output sequences under x is at most $p^m < n$. Thus there exist $q, r \in Q$ such that $\hat{\beta}_q(x) = \hat{\beta}_r(x)$ but $q \neq r$. x cannot be a DS of M and this completes the proof.

The fact that the bound given in Lemma 2.1 is the best (the greatest) will be shown later by constructing machine having DS of this length. A machine satisfying Lemma 2.1 will be called optimally

diagnosable. The utility of optimally diagnosable machines will be discussed in a later chapter. Let us turn now to a more general type of input sequences in which final state of a machine can be determined by observing output responses to these sequences.

Definition 2.5 If M is a sequential machine, an input sequence x is a homing sequence (HS) of M if for all $q, r \in Q$

$$\hat{\beta}_q(x) = \hat{\beta}_r(x) \text{ implies } \bar{\delta}(q, x) = \bar{\delta}(r, x)$$

We will say a machine M is homable if, for some input sequence x , x is a HS of M . A homable machine is k-homable if a shortest homing sequence is of length k . In this case k is the order of homability.

It is well known that every reduced machine is homable and every diagnosable machine must be reduced. If M is an n -state reduced machine, then the least upper bound on the order of homability is $n(n-1)/2$ and the shortest possible length of a homing sequence is 1.

Distinguishing sequences and homing sequences are closely related. It is easy to see that every DS is also a HS but the converse is not true. We will precisely establish their relationship after the following definition.

Definition 2.6 If M is a sequential machine with states Q and $q, r \in Q$ ($q \neq r$), then q and r merge under x ($x \in I^+$) if

$$i) \quad \bar{\delta}(q, x) = \bar{\delta}(r, x) .$$

If in addition to i) ,

$$ii) \quad \hat{\beta}_q(x) = \hat{\beta}_r(x)$$

then q and r converge under x .

In words, two states q and r merge under an input sequence x , if when M is started in q or r , and x is applied, M goes to the same final state. If q and r merge under x and, furthermore, the output responses under x with initial states q or r are identical, then q and r converge under x . A pair of states converge if they converge under some input sequence and M is convergence free (CF) if no pair of distinct states in Q converge. With these definitions, we can now formally state the relationship between a DS and a HS which has been informally described by Hennie [25].

Theorem 2.1 An input sequence x of a machine M is a distinguishing sequence if and only if it is a homing sequence and no pair of distinct states converge under x .

Proof: Let x be a DS of M . Then, by Definition 2.4

$$\hat{\beta}_q(x) = \hat{\beta}_r(x) \implies q = r \quad \forall q, r \in Q$$

But

$$q = r \implies \bar{\delta}(q, x) = \bar{\delta}(r, x)$$

Therefore x is a HS of M by Definition 2.5. Moreover, no distinct pair of states converge under x , since by Definition 2.4 $q \neq r \implies \hat{\beta}_q(x) \neq \hat{\beta}_r(x)$. Conversely, suppose x is a HS of M so that no distinct pair of states converge under x . Suppose there are states q and r such that

$$\hat{\beta}_q(x) = \hat{\beta}_r(x).$$

Then $q = r$, for if $q \neq r$ then, as q and r cannot converge under x ,

$$\bar{\delta}(q, x) \neq \bar{\delta}(r, x)$$

contradicting the fact that x is a HS. Thus x is a DS of M and the proof is completed.

Example 2.1

Consider the machine M_1 whose state table and transition graph are shown below.

	a	b
1	1/0	4/1
2	3/1	5/1
3	4/1	1/0
4	2/0	4/0
5	1/1	5/1

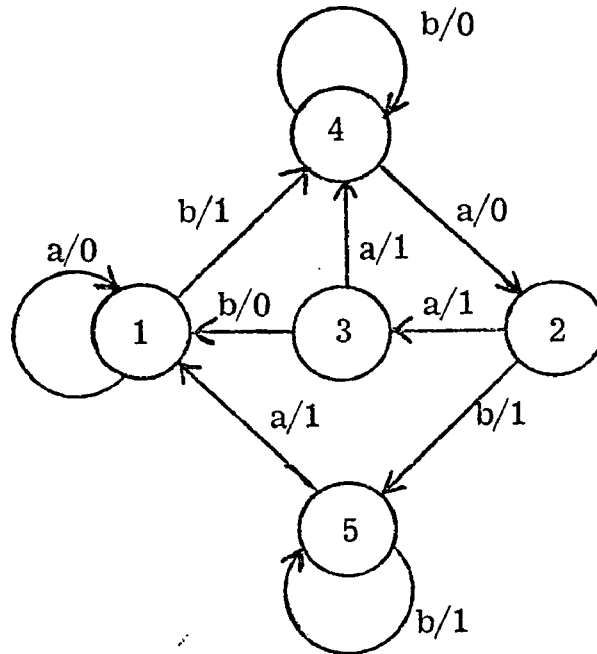


Figure 2.1 Machine M_1

aaa is a DS and bb is a HS but not a DS due to the fact that states 2 and 5 converge under b. Since no sequence shorter than 3 is a DS, M is 3-diagnosable. Similarly M_1 is 2-homable. States 1 and 5 merge under a and states 1 and 4 merge under b.

Section 2.1 Definitely Homable and Definitely Diagnosable Machines

Diagnosable machines and homable machines are of interest in designing fault detection and diagnosing experiments because of the ability to determine initial state and final state with some proper choice of input sequences. In order to have a more profound understanding of these classes of machines let us first study subsets of these machines where almost all sequences are DS or HS. The class of "definitely diagnosable" machines was first suggested by Kohavi and Lavallee [32] in their now well-known paper of 1967. We will review some of their results here and put them in a better perspective encompassing a spectrum of machines with various "degrees" of diagnosability.

Definition 2.7 A sequential machine M is definitely homable (DH) if there is an integer k such that every input sequence of length k is a homing sequence. The least such integer k is called the order of definite homability.

A definitely homable machine is also known as a finite-memory machine [30]. By the deterministic property of a machine, if x is an HS and y is any input sequence, then xy is also an HS. Thus if a machine is definitely homable of order k , any sequence of length equal to or greater than k must also be a homing sequence. Consequently, all but a finite set of input sequences are

homing sequences. If M is definitely homable, then an upper bound on its order can be easily determined as shown in the next theorem. If M is definitely homable of order k , let us say M is k -definitely homable.

Theorem 2.2 If $M = (I, Q, Z, \delta, \omega)$ is a k -definitely homable machine with $|Q| = n$, then

$$k \leq \frac{n(n-1)}{2}. \quad (2.3)$$

Proof: Suppose to the contrary, i. e. M is DH and yet $\exists x \in I^+$ such that $\lg(x) \geq \binom{n}{2}$ and x is not an HS, i. e. $\exists q, r \in Q$ such that $\bar{\delta}(q, x) \neq \bar{\delta}(r, x)$ and $\hat{\beta}_q(x) = \hat{\beta}_r(x)$. Then, for any prefix y of x , $\bar{\delta}(q, y) \neq \bar{\delta}(r, y)$. We first claim that for any two prefixes y and z of x

$$\{\bar{\delta}(q, y), \bar{\delta}(r, y)\} \neq \{\bar{\delta}(q, z), \bar{\delta}(r, z)\}.$$

Suppose that this is not so, i. e.

$$\{\bar{\delta}(q, y), \bar{\delta}(r, y)\} = \{\bar{\delta}(q, z), \bar{\delta}(r, z)\}.$$

Let $\lg(y) > \lg(z)$, i. e. z is a proper prefix of y and let w be the suffix of y with z deleted. Then the sequence consisting of z followed by an arbitrary iteration of w , zw^+ , cannot be a HS of M due to the fact that $\hat{\beta}_{\bar{\delta}(q, z)}(w^+) = \hat{\beta}_{\bar{\delta}(r, z)}(w^+)$ and yet $\bar{\delta}(q, zw^+) \neq \bar{\delta}(r, zw^+)$ - contradicting the assumption that M is DH. This is illustrated in Figure 2.2.

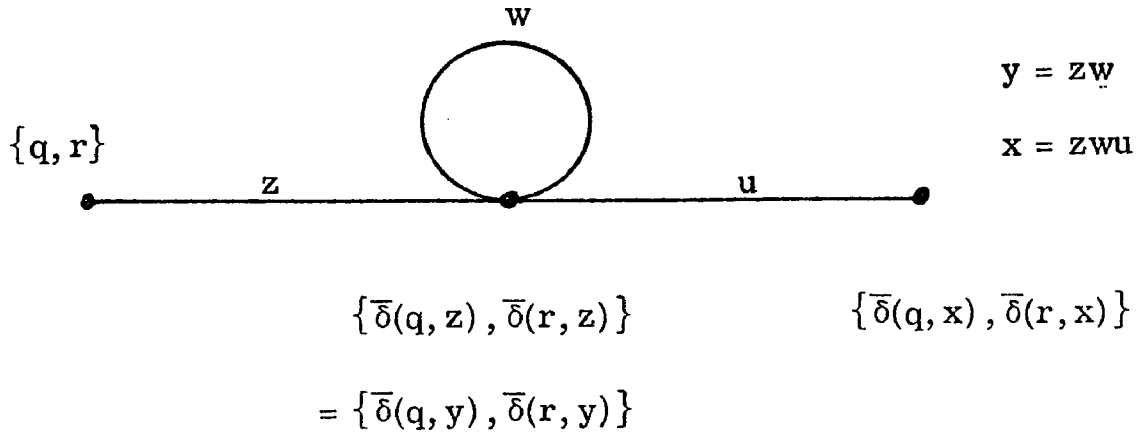


Figure 2.2 Successor State Pairs of $\{q, r\}$ Under x with a Repeated Successor State Pair

Thus we must conclude that there cannot be any repeated successor state pair of $\{q, r\}$ under x . On the other hand $\ell g(x) \geq \binom{n}{2}$ implies at least $\binom{n}{2} + 1$ distinct state pairs are determined by all possible prefixes - an impossibility. This completes the proof.

As a consequence of Theorem 2.2, we can state the following characterization of definitely homable machines.

Corollary 2.2.1 If M is an n -state machine, then M is definitely homable if and only if every input sequence of length greater than or equal to $n(n-1)/2$ is a homing sequence of M .

Proof: The "only if" part has been shown in Theorem 2.2. To show the "if" part, let $x \in I^k \ni k \geq \binom{n}{2}$. Then x is a HS of M and

every sequence of length $\binom{n}{2}$ is a HS. By Definition 2.7, M is definitely homable.

The inequality (2.1) shows that even if a machine is diagnosable, the length of its shortest DS can be very large. We would like to investigate machine classes where the upper bounds of the order of diagnosability are much smaller. This motivates the study of another machine notion [32].

Definition 2.8 A sequential machine is definitely diagnosable (DD) if there is an integer k such that every input sequence of length k is a distinguishing sequence. The least such integer k is called the order of definite diagnosability.

Thus, again, if a machine is definitely diagnosable all but a finite number of input sequences are distinguishing sequences. If a machine M is definitely diagnosable of order k , we call M k -definitely diagnosable. Because of the fact that every DS is also an HS, it follows that every DD machine is DH. Thus the order of definite diagnosability and characterization of DD machine can be obtained in a manner similar to Theorem 2.2 and Corollary 2.2.1. Before we establish these results, let us investigate some necessary conditions for DD machines.

Theorem 2.3 If M is definitely diagnosable, then M is convergence free.

Proof: Suppose the contrary, i.e. M is DD but for some $q, r \in Q$ ($q \neq r$) $\exists x \in I^+$ such that $\hat{\beta}_q(x) = \hat{\beta}_r(x)$ and $\bar{\delta}(q, x) = \bar{\delta}(r, x)$. Let k be the order of definite diagnosability. Then the length of x cannot be equal to or greater than k otherwise x must be a DS. Suppose then that $\ell g(x) < k$ and let $y = xz$ where $\ell g(y) = k$. Now

$$\hat{\beta}_q(y) = \hat{\beta}_q(x) \hat{\beta}_{\bar{\delta}(q, x)}(z),$$

$$\hat{\beta}_r(y) = \hat{\beta}_r(x) \hat{\beta}_{\bar{\delta}(r, x)}(z)$$

Since $\bar{\delta}(q, x) = \bar{\delta}(r, x)$ it follows that

$$\hat{\beta}_q(y) = \hat{\beta}_r(y)$$

where $q \neq r$. But $\ell g(y) = k \Rightarrow y$ is a DS, a contradiction.

Although every distinguishing sequence is a homing sequence, the converse is not true as is shown in Theorem 2.1. However, if a machine is DD, then as a corollary of Theorem 2.3 we have:

Corollary 2.3.1 If M is a definitely diagnosable machine then every homing sequence is a distinguishing sequence.

Proof: If M is DD, then by Theorem 2.3, no pair of states converge under any sequence and thus none will converge under a homing sequence. Thus by Theorem 2.1, every HS of M is a DS of M .

Recall that if a machine is definitely diagnosable then it is also definitely homable but the converse need not hold. However, if the convergence free condition is added, then as a second corollary of the last theorem, we obtain the following characterization of definite diagnosability.

Corollary 2.3.2 A machine M is definitely diagnosable of order k if and only if M is both convergence free and definitely homable of order k .

Proof: If M is DD of order k then from Corollary 2.3.1 M is obviously DH of order k and by Theorem 2.3 M is also convergence free. Conversely, if M is DH of order k and CF, then $x \in I^k \Rightarrow x$ is an HS and by Theorem 2.1, x is an HS $\Rightarrow x$ is a DS. Consequently, $x \in I^k \Rightarrow x$ is a DS and by Definition 2.8, M is DD.

Thus an upper bound for the order of definite diagnosability can be seen to be identical to the order of definite homability as an immediate result of Corollary 2.3.2.

Corollary 2.3.3 If M is k -diagnosable and has n states, then

$$k \leq \frac{n(n-1)}{2} \quad (2.4)$$

Thus, summarizing these developments of DD machines, another characterization of the DD machines follows immediately.

Corollary 2.3.4 If M is an n -state machine, then M is definitely diagnosable if and only if every input sequence of length greater than or equal to $n(n-1)/2$ is a distinguishing sequence of M .

Corollary 2.3.2 characterizes the DD property of a machine by means of its being convergence free and definitely homable. From a practical point of view, we have found it more convenient to characterize a machine by its "submachines" if possible. This is the third characterization of DD machines to be introduced below. If a machine M has the property that its input set contains a single element, then M is a single-input machine, a sequence generator or an autonomous machine.

Definition 2.9 Let $M = (I, Q, Z, \delta, \omega)$ be a sequential machine. A single-input submachine M_a of M is defined as $M_a = (\{a\}, Q, Z, \delta|_{Q \times \{a\}}, \omega|_{Q \times \{a\}})$ where $a \in I$.

Lemma 2.2 If every single-input submachine of a sequential machine M is reduced, then M is convergence free.

Proof: Suppose M is not CF. Then $\exists q, r \in Q$ and $a \in I \ni q \neq r$ but $\omega(q, a) = \omega(r, a)$ and $\delta(q, a) = \delta(r, a)$. Thus for these q, r and a

$$\beta_q(a^n) = \beta_r(a^n) \quad \forall n \geq 1$$

This means q and r are equivalent in M_a and M_a cannot be reduced.

This completes the proof.

The converse of the above lemma is not true; in particular, a convergence free autonomous machine needs not be reduced.

Theorem 2.4 A sequential machine is definitely diagnosable if and only if

(1) M is definitely homable

and

(2) every single-input submachine is reduced.

Proof: First assume M is definitely diagnosable, then it is obvious that (1) holds. If (2) does not hold, then there is some $a \in I$ such that any repeated symbol sequence formed by a is not a DS. Thus M cannot be definitely diagnosable.

Conversely if both (1) and (2) hold, then from Lemma 2.2, (2) guarantees that M is convergence free. (1) and the convergence free condition say that M is definitely diagnosable (Corollary 2.3.2). Thus, the proof is complete.

This theorem can be viewed as a stronger and more practical version of Corollary 2.3.2. It is stronger because condition (2) is stronger than the convergence free property as pointed out by Lemma 2.2 and the remarks following it. Interestingly, (2) and DH is equivalent to CF and DH.

Let us call a distinguishing sequence (homing sequence) minimal if no proper prefix of it is also a distinguishing sequence (homing sequence). Then we can define yet another class of machines between the classes of DH and DD machines. If a definitely homable machine is diagnosable, then the following theorem shows that every minimal length DS has the same upper bound as that of the order of definite diagnosability.

Theorem 2.5 Let M be an n -state definitely homable machine. If M is diagnosable then every minimal distinguishing sequence x of M has the property that

$$\ell g(x) \leq \frac{n(n-1)}{2}$$

Proof: Assume M is diagnosable and suppose there is a minimal DS x such that $\ell g(x) > \frac{n(n-1)}{2}$. Now x is an HS and moreover must be minimal as an HS because any proper prefix of x that is an HS must be a DS, contradicting the minimality of x . However by Theorem 2.2, M is DH, a minimal HS must have length $\leq \frac{n(n-1)}{2}$.

Section 2.2 Sequence Generators and Linear Machines

Two classes of machines which have close relationships with those studied in the last section will be discussed below relative to their ability in providing short distinguishing sequences. We have observed previously that the single-input submachines of a sequential machine determine some important properties of the complete machine. For example, definite diagnosability can be characterized by the property of definite homability and that each single-input submachine is reduced. Independent study of this class of machines is therefore justified in order to learn more about the diagnosis problem of general sequential machines. Similarly, the class of reduced "linear" machines can be shown to be a subclass of definitely diagnosable machines where the order of definite diagnosability is bounded by the "dimension" of the state space thus providing the machine with short distinguishing sequences. We begin by first revealing some interesting properties of sequence generators.

Lemma 2.3 A sequence generator M is definitely diagnosable if and only if it is reduced. Moreover, M is diagnosable $\iff M$ is $n-1$ DD where n is the number of states of M .

Proof: We have already noted that every diagnosable machine is reduced. Suppose then that $M = (\{a\}, Q, Z, \delta, \omega)$ is reduced. Then $q \neq r$ implies $\beta_q \neq \beta_r$ and if $|Q| = n$, we know that q and r are distinguishable by a sequence of length $n-1$ in this case is a^{n-1} we have

$$\hat{\beta}_q(a^{n-1}) \neq \hat{\beta}_r(a^{n-1})$$

i. e. a^{n-1} is a DS of M and M is therefore DD.

Thus a reduced sequence generator of n-state is definitely diagnosable of order at most n-1. Therefore being reduced is synonymous with being diagnosable or definitely diagnosable in a sequence generator. This property will be found useful later on when we consider machine augmentation for realizing a given behavior by a diagnosable machine. Let us turn now to the problem of finding the relationship between state structure and the order of diagnosability in a reduced sequence generator. First, the review of a basic machine notion.

Definition 2.10 Two states $q, r \in Q$ in a sequential machine are k-equivalent if whenever the length of input sequence x is less than or equal to k , $\beta_q(x) = \beta_r(x)$. The partition on Q induced by the k-equivalence relation (denoted π_k) is called the k-equivalence partition.

Recall that the lower bound of the length of a distinguishing sequence in an n-state, p-output machine is $\lceil \log_p n \rceil$. Thus an optimally diagnosable machine has a shortest possible DS. The next lemma relates the length of the shortest DS in a sequence generator to the state equivalence partition.

Lemma 2.4 If M is a reduced sequence generator, then M is k-diagnosable iff k is the least integer such that $\pi_k = \pi_{k+1}$.

Proof: Suppose M is k -diagnosable, then for any $x \in I^k$ of length k , $\hat{\beta}_q(x) = \hat{\beta}_r(x) \Rightarrow q = r$.

$$\therefore \pi_k = 0 = \pi_{k+1}$$

But if $lg(x) = k-1$, x is not a DS of M and $\exists q, r \in Q \ni \hat{\beta}_q(x) = \hat{\beta}_r(x)$ yet $q \neq r$.

$$\therefore \pi_{k-1} \neq 0 = \pi_k$$

Conversely, if k is the least integer such that $\pi_k = \pi_{k+1}$, then since M is reduced and $\pi_k \geq \pi_{k+1}$, $\pi_k = \pi_{k+1} = 0$. $\pi_{k-1} \geq \pi_k$ and $\pi_{k-1} \neq \pi_k$, then $\exists q, r \in Q \ni q$ and r are $k-1$ equivalent. Therefore, the length of the shortest distinguishing sequence is k and M is k -diagnosable.

With this lemma, the following characterization of an optimally diagnosable sequence generator is obtained naturally.

Theorem 2.6 Let M be a reduced p -ary sequence generator (i.e. there are p output symbols) with n states, where $n = p^m$. Then M is optimally diagnosable iff $p|\pi_k| = |\pi_{k+1}| \forall 1 \leq k < m$.

Proof: We first observe that since M is autonomous and $|\mathcal{R}(\omega)| = p$, it follows that $|\pi_1| = p$ and $|\pi_{k+1}| \leq p|\pi_k|$ for $1 \leq k$. Now suppose M is optimally diagnosable of order m but $\exists k (1 \leq k < m) \ni |\pi_{k+1}| \neq p|\pi_k|$ where $|\pi_{i+1}| = p|\pi_i|$ for $1 \leq i < k$. If $|\pi_{k+1}| = |\pi_k|$, then since $\pi_{k+1} \leq \pi_k$, we have $\pi_{k+1} = \pi_k$ and it follows that M is not

reduced, contrary to our hypothesis that M is reduced. So, let us assume that $|\pi_{k+1}| > |\pi_k|$. Then from our previous observation and the assumption that $|\pi_{k+1}| \neq |\pi_k|$, we have

$$p^{k+1} > |\pi_{k+1}| > p^k$$

Then at least $\exists$ one block B_{k+1} of π_{k+1} $\ni \lceil \frac{p^{m-k}}{p-1} \rceil \leq |B_{k+1}| \leq p^{m-k}$.

The shortest sequence of p -ary partitions that can partition this block to singleton sets is of length $m-k$. Therefore, the shortest DS is of length $k+1+m-k = m+1$, contrary to our assumption that M has a DS of length m .

Conversely, if $|\pi_{k+1}| = p|\pi_k| \forall k \leq m$. Then when $k = m-1$,

$$|\pi_m| = p|\pi_{m-1}| = pp^{m-1} = p^m$$

which is the total number of states. Thus, M has a DS of length m .

For the case where n is not a power of p , we have the following theorem.

Theorem 2.7 Let M be a reduced p -ary sequence generator with n states and B_k be a largest k -equivalence class. Then M is optimally diagnosable iff $|B_k| \leq p^{m-k} \forall k \leq m$ where $m = \lceil \log_p n \rceil$.

Proof: If there exists B_k in π_k such that $|B_k| > p^{m-k}$, then the shortest possible DS that will partition B_k into singleton states is of length $> m-k$. Consequently, the shortest DS for M would be $> m-k+k$ and M cannot have a DS of length m .

Conversely, when $k = m$

$$|B_k| \leq p^0 = 1$$

and the sequence of length m is a DS. This completes the proof.

Linear sequential machines are generally known for their ease in analysis and network realizations and their properties and limitations have been well explored (see, for example, [15], [38] and [7]). However, properties of linear machines relating to the fault detection problem of behavior verification are still yet to be documented. The purpose of the following development is to bridge this gap. It has been found that the linear machines have many properties similar to those of sequence generators relating to machine diagnosis as to be seen in the following development. To make this development precise, let us first formally state the definition of a linear machine.

Definition 2.11 A sequential machine $M = (I, Q, Z, \delta, \omega)$ is said to be linear over a finite field F if there exist integers n, k , and ℓ such that

$$Q = V^n(F), I = V^k(F), Z = V^\ell(F)$$

and linear transformations

$$A: Q \rightarrow Q$$

$$B: I \rightarrow Q$$

$$C: Q \rightarrow Z$$

$$D: I \rightarrow Z$$

such that

$$\delta(q, a) = Aq + Ba$$

$$\omega(q, a) = Cq + Da$$

where $V^n(F)$ is an n -dimensional linear space over F .

In words, a sequential machine is said to be linear if its next state vector and output vector can be represented as linear combinations of the present state and present input vectors. The input-output behavior of a linear machine can be defined recursively in terms of the linear transformations A, B, C and D as follows (for a proof and a more detailed discussion see [7] or [15], for example).

Lemma 2.5 Let M be the linear machine defined in Definition 2.11 and $x \in I^n$. Then $\forall q \in Q$

$$\hat{\beta}_q(x) = K_n q + Q_n x$$

for linear transformations $K_n: Q \rightarrow Z^n$ and $Q_n: I^n \rightarrow Z^n$ where

$$K_n = \begin{bmatrix} C \\ CA \\ CA^2 \\ \vdots \\ CA^{n-1} \end{bmatrix} \quad Q_n = \begin{bmatrix} D & 0 & \dots & 0 & 0 \\ CB & D & \dots & 0 & 0 \\ CAB & CB & \dots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ CA^{n-2}B & CA^{n-3}B & \dots & CB & D \end{bmatrix}$$

Based on the above lemma, we have the following alternative characterizations of reduced linear machines.

Theorem 2.8 If M is a reduced linear machine and $Q = V^n(F)$, then the following statements are equivalent

- i) M is definitely diagnosable of order i .
- ii) i is the least integer such that $\text{rank}(K_i) = n$
- iii) i is the least integer such that $\pi_i = \pi_{i+1}$

Proof: i) $\Rightarrow$ ii) Suppose M is definitely diagnosable of order i , then $\forall x \in I^i$, we have

$$\hat{\beta}_q(x) = \hat{\beta}_r(x) \Rightarrow q = r, \forall q, r \in Q.$$

Recall that

$$\hat{\beta}_q(x) = K_i q + Q_i x$$

where

$$K_i: Q \rightarrow Z^i$$

$$Q_i: I^i \rightarrow Z^i$$

First we show that $\hat{\beta}_q(x) = \hat{\beta}_r(x) \Leftrightarrow K_i q = K_i r$. Suppose $\hat{\beta}_q(x) = \hat{\beta}_r(x)$, then $K_i q + Q_i x = K_i r + Q_i x \forall x \in I^i$. Subtracting $Q_i x$ from both sides, we have $K_i q = K_i r$. Conversely, if $K_i q = K_i r$, then $K_i q + Q_i x = K_i r + Q_i x$ and we have $\hat{\beta}_q(x) = \hat{\beta}_r(x)$. Since $\forall x \in I^i$

$$\hat{\beta}_q(x) = \hat{\beta}_r(x) \Rightarrow q = r$$

we have

$$K_i q = K_i r \Rightarrow q = r$$

But this says that K_i is a 1-1 linear transformation from Q to Z^i and since $\dim Q = n$, it follows then

$$\text{rank}(K_i) = n$$

By definition of the order of definite diagnosability i is the least such integer.

$$\text{ii)} \Rightarrow \text{iii)}$$

$$\text{Suppose } \text{rank}(K_i) = n$$

$$K_i: Q \rightarrow Z^i$$

then K_i is a 1-1 linear transformation

$$\therefore K_i q = K_i r \Rightarrow q = r, \forall q, r \in Q$$

$$\text{But } K_i q = K_i r \Leftrightarrow \hat{\beta}_q(x) = \hat{\beta}_r(x), \forall x \in I^i$$

$$\therefore \hat{\beta}_q(x) = \hat{\beta}_r(x) \Rightarrow q = r, \forall x \in I^i$$

$$\text{But } \hat{\beta}_q(x) = \hat{\beta}_r(x) \forall x \in I^i \Leftrightarrow q \equiv r (\pi_i)$$

$$\therefore q \equiv r (\pi_i) \Rightarrow q = r$$

$$\therefore \pi_i = 0$$

Since $\pi_i \geq \pi_{i+1}$, it follows then $\pi_i = \pi_{i+1}$.

$$\text{iii)} \Rightarrow \text{i)}$$

Suppose i is the least integer such that $\pi_i = \pi_{i+1}$, then since M is reduced, $\pi_i = \pi_{i+1} = 0$. Then $\forall$ pair $q, r \in Q$, $q \neq r$, $\exists x \in I^i \ni \hat{\beta}_q(x) \neq \hat{\beta}_r(x)$ which in turn implies $K_i q \neq K_i r$. Thus K_i is a 1-1 linear transformation and any $x \in I^i$ is a DS. Therefore, M is DD of order i .

Corollary 2.8.1 Every reduced linear sequential machine is definitely diagnosable and the maximum order of the definite diagnosability is n , where $n = \dim Q$.

Proof: If M is a reduced linear machine, then $\exists i$ such that $\pi_i = \pi_{i+1} = 0$. Now by iii) of Theorem 2.8, M is definitely diagnosable of order i if i is the least integer such that $\pi_i = \pi_{i+1}$. Then since K_i is a 1-1 linear transformation, $\text{rank}(K_i) = n$. Since the rank of A is $\leq n$ and by definition of K_i , it follows that $i \leq n$. Thus the least integer i s.t. $\text{rank}(K_i) = n$ is at most n .

In other words, every input sequence of length n in a reduced linear machine is a DS where n is the dimension of the state space. Thus in the case of linear machines, we have a reduced upper bound on the length of DS. Note that in a linear machine the concept of being i -diagnosable is equivalent to that of being definitely diagnosable of order i . Since the minimum length of DS in a linear machine can be characterized by the least integer i such that $\text{rank}(K_i) = n$, we can characterize the optimally diagnosable linear machine with the following corollary of Theorem 2.8.

Corollary 2.8.2 Let M be a reduced linear machine with $n = \dim Q$, $\ell = \dim \mathcal{R}(\omega) = \dim Z$ and $k = \dim I$. Then M is optimally diagnosable iff $\text{rank}(K_{\lfloor \frac{n}{\ell} \rfloor}) = n$.

Recall that a linear machine is reduced if and only if it is definitely diagnosable. This result leads to the observation that the state set is partitioned evenly by each input symbol. Since the state space can be considered as an additive abelian group and the linear transformation $K_i: Q \rightarrow Z^i$ [see Lemma 2.5] induces a congruence relation on Q , it follows that the partition corresponding to this congruence relation is a coset partition. More precisely,

Lemma 2.6 If M is a linear machine, then every i -equivalence relation partitions the state set into cosets when the state set is considered as an additive abelian group.

The cardinality of these cosets can be shown to be a power of a prime number. Thus, we can obtain a recursive relation on the i -equivalence relation of a linear machine. Denoting the i -equivalence partition on Q as π_i , we have

Theorem 2.9 Let M be a linear machine over a finite field F of characteristic p and $|F| = p^m$, $n = \dim Q$ and $\ell = \dim Z$. Then $\forall i, \exists k_i, 0 \leq k_i \leq \ell m$ such that $|\pi_{i+1}| = p^{k_i} |\pi_i|$.

Proof: From Lemma 2.6 we know that π_i partitions Q into cosets. Let H_i be the set of states which are i -equivalent to $\bar{0}$. Then H_i is a subgroup of Q . The order of H_i divides that of Q . Now the

cardinality of Q is a power of p , i.e. Q is a p -group, it follows that H_i is also a p -group or $H_i = \{\bar{0}\}$. If $H_i = \{\bar{0}\}$ or $H_i = H_{i+1}$ then clearly $k_i = 0$. If $H_i \neq \{\bar{0}\}$, then $|H_i| = p^{j_i}$

$$|\pi_i| = |Q/H_i| = p^{mn-j_i}$$

$$|\pi_{i+1}| = |Q/H_{i+1}| = p^{mn-j_{i+1}}$$

Therefore

$$|\pi_{i+1}| = p^{j_i-j_{i+1}} |\pi_i|.$$

Since $H_{i+1} \subseteq H_i$, it can be shown that $0 \leq j_i - j_{i+1} < \ell m$. Let $k_i = j_i - j_{i+1}$ and the theorem is proved.

Theorem 2.9 says that in a linear machine the i -equivalence classes of the state set always "grow" as a power of the field characteristic p . By the coset structure, each i -equivalence class has the same cardinality which is also a power of p . In case the dimension of the output space divides that of the state space, we can characterize an optimally diagnosable linear machine in the following way.

Theorem 2.10 Let M be a reduced linear machine with $q = p^m$, ℓ and n given as in Theorem 2.9 and $\ell \mid n$. Then M is optimally diagnosable iff $|\pi_{i+1}| = q^\ell |\pi_i| \forall i, 1 \leq i < \frac{n}{\ell}$.

Proof: Assume M is optimally diagnosable, then $\forall x \in \left[\frac{n}{\ell}\right]$, x is a DS of M . Since $\ell \mid n$, $\left[\frac{n}{\ell}\right] = \frac{n}{\ell}$, we claim that $|\pi_{i+1}| = q^\ell |\pi_i| \forall 1 \leq i < \frac{n}{\ell}$. Suppose there exists some i such that $|\pi_{i+1}| \neq q^\ell |\pi_i|$.

From Theorem 2.9, we have $|\pi_{i+1}| = p^{k_i} |\pi_i|$, and our last assumption says $k_i \neq \ell m$, i.e. $k_i < \ell m$. But this says in turn that $|\pi_i| < p^{i\ell m}$ and $|\pi_{\frac{n}{\ell}}| < p^{mn}$. Thus $x \in I^{\frac{n}{\ell}}$ cannot be a DS, contrary to our assumption that M is optimally diagnosable. Conversely, if $|\pi_{i+1}| = q^\ell |\pi_i|$, then $\forall x \in I^{\frac{n}{\ell}}$, x is a DS, i.e. M is optimally diagnosable.

The result of Theorem 2.9 can be generalized to nonlinear sequential machines. We first introduce a concept of "generalized equivalence relation" under some input sequence.

Definition 2.12 Let $M = (I, Q, Z, \delta, \omega)$ be a sequential machine and let $x \in I^+$. Then $q R_x r$ if $\hat{\beta}_q(x) = \hat{\beta}_r(x)$. The partition induced by R_x is denoted π_x .

In other words, $q R_x r$ if the output sequence for input sequence x is the same for initial states q and r .

Theorem 2.11 If $M = (I, Q, Z, \delta, \omega)$ is a sequential machine, $|Q| = p^n$, $|Z| = p$ (p is an integer). Then M is optimally diagnosable iff $\exists x = a_1 a_2 \dots a_n$ such that $|\pi_{x_{i+1}}| = p |\pi_{x_i}| \forall 1 \leq i < n$ where $x_i = a_1 a_2 \dots a_i$ and $|\pi_{x_1}| = p$.

Proof: To prove necessity, suppose there is no $x_n \in I^n$ such that $|\pi_{x_{i+1}}| = p |\pi_{x_i}|$ for $1 \leq i < n$. Then $\forall x_n \in I^n$, x_n cannot be a DS of M because $|\pi_{x_n}| \neq p^n$ implies $\pi_{x_n} \neq 0$. Thus by definition, M is not

optimally diagnosable. To show sufficiency, suppose M is not optimally diagnosable. Then every sequence of length n cannot be a DS.

This says that $\exists q \neq r \text{ in } Q \ni \forall x_n \in I^n, \hat{\beta}_q(x) = \hat{\beta}_r(x) \text{ i.e. } q \equiv_n r$.

This means that $\forall x_n \in I^n, \exists i, 1 \leq i < n$ (depending on x_n), such that $|\pi_{x_{i+1}}| \neq p |\pi_{x_i}|$.

Theorem 2.11 provides a useful means of finding an optimal distinguishing sequence. Any input symbol which does not partition the state set into p equivalence classes can be excluded as the starting symbol of an optimal DS. On each i -equivalence class of states any input symbol which does not partition it into p equivalence subclasses is excluded from being the next symbol of an optimal DS. The process is then iterated until an optimal DS of length n is found or no optimal DS can be found. In the case of linear machines, the same input symbol can be examined at each step since each input symbol has an "equivalent" effect on the partitioning process.

Section 2.3 Machine Classifications

We have discussed several classes of machines relating to their ability of possessing distinguishing sequences or homing sequences, the ability of providing many such sequences and the ability of providing these sequences of small length. A partially ordered set of these classes of machines using set containment as the partial ordering is depicted in the following Hass diagram of Figure 2.3.

From Figure 2.3 it is clear that if a machine is definitely homable then it is also homable and every diagnosable machine is also homable. The third characterization of DD machine as stated in Theorem 2.7 is clearly depicted in the diagram. Many other classes of machines which can be generated from this diagram are not shown but they can be easily obtained if so desired. For example, the class of machines stated in Theorem 2.5 can be obtained from the intersection of the set of diagnosable machines and the set of DH machines.

In summary, this chapter begins with the review of some basic sequential machine theory and establishes precisely the terminology and notation to be used throughout this thesis. Several machine concepts and machine classes relating to behavior checking are then introduced and studied. Some of these concepts are to be used extensively in the following chapters while the others are introduced for completeness or indications of possible generalization that may be applied to the results obtained in this thesis.

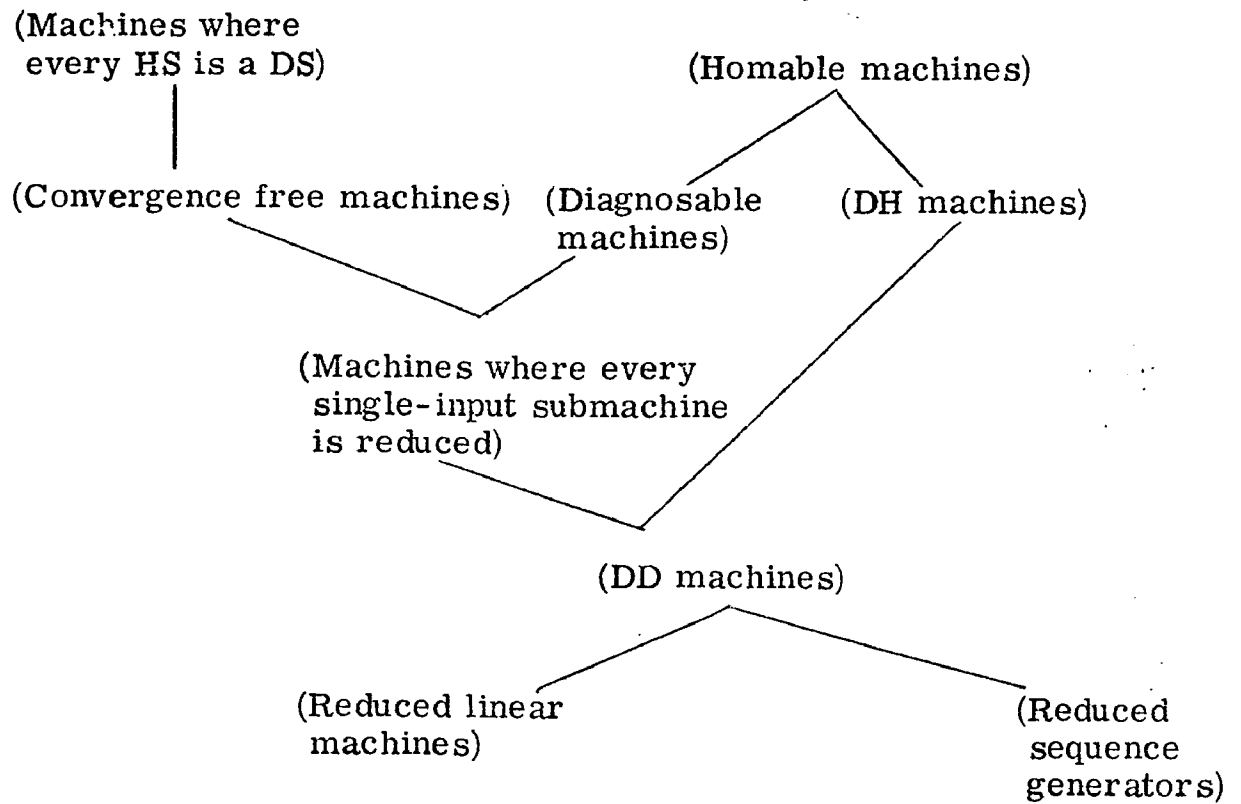


Figure 2.3 Machine Classification Diagram

Chapter III

DIAGNOSABLE MACHINE REALIZATIONS OF SEQUENTIAL BEHAVIOR[†]

This chapter is concerned with the design of a sequential machine M which "realizes" some given sequential machine behavior B and M possesses some distinguishing sequences of "reasonable" length. The application of such sequences in the design of diagnosing algorithms is illustrated by the investigations of Hennie [26], Kime [29], and Kohavi and Lavalley [32]. In particular, three types of realizations are considered using control-input augmentation, test-output augmentation and state-output augmentation, respectively. Such realizations are studied from a machine-theoretic point of view and tradeoff between time (length of distinguishing sequence) and space (alphabet size and state size) is investigated.

[†]Part of the work in this chapter was reported at the 1971 International Conference on Fault-Tolerant Computing, Pasadena, California [37].

Section 3.1 Machine Augmentation as a Machine Realization Problem

Although the problem of designing diagnosable machines has been studied previously [26] [32], it is usually stated as addition of test points or modification of state table to the given network or machine. This notion is restrictive in the sense that the same or similar physical realization is usually implied. In this section we will formalize this notion in terms of machine "realization" where the only restriction is that the designed machine be able to mimic the given behavior while at the same time possesses a desired property. With this new notion in mind, many new solutions can be obtained.

From the definition of distinguishing sequence, it is immediate that every diagnosable machine is reduced but, as is well known, not every reduced machine is diagnosable. The problem we wish to consider then is the following:

Given some reduced machine M' , (or equivalently, some sequential behavior B where M' is a reduced machine such that $B_{M'} = B$), design a diagnosable machine M that "realizes" M' .

Note that in stating the problem, no generality is lost by requiring that M' be reduced for if M' is not reduced, any realization of a reduced machine equivalent to M' is also a realization of M' . A more specific

statement of the above problem depends, of course, on what is meant by "realizes". To insure adequate generality the formal notion of machine "realization" [24] (or "simulation" [1]) appears to be the most appropriate starting point, that is:

Definition 3.1 Let $M = (I, Q, Z, \delta, \omega)$ and $M' = (I', Q', Z', \delta', \omega')$ be two (Mealy) sequential machines. Then M realizes M' if there are three functions h_1, h_2 and h_3 , where

$h_1: (I')^+ \rightarrow I^+$ is a semigroup homomorphism

such that $h_1(I') \subseteq I$,

$h_2: Q' \rightarrow Q$, and

$h_3: Z \rightarrow Z'$

such that

$$\beta_{q'}(x) = h_3(\beta_{h_2(q')} (h_1(x)))$$

for $q' \in Q'$ and $x \in (I')^+$.

Thus M realizes M' if each state q' of M' can be realized by state $h_2(q')$ of M under appropriate input encoding h_1 and output decoding h_3 . Note that the restriction $h_1(I') \subseteq I$ requires that the encoding be symbol-to-symbol. If M realizes M' , M is said to be a realization of M' and therefore, paraphrasing the problem just stated, given any reduced machine M' , we seek machines M that are diagnosable realizations of M' . Such a realization is illustrated in

M_1' :

Q \ I	a	b
1	1/1	4/1
2	3/0	5/1
3	4/0	1/0
4	2/0	4/0
5	1/1	5/1

 M_1 :

Q' \ I'	a	b
1	1/A	4/A
2	3/C	5/A
3	4/C	1/C
4	2/C	4/C
5	1/A	5/B

$h_1: I_1' = e_I: I' \longrightarrow I$ (Input identity mapping)

$h_2 = e_Q: Q' \longrightarrow Q$ (State identity mapping)

$h_3: Z \longrightarrow Z'$ whose mapping rule is given below:

Z	$h_3(Z)$
A	1
B	1
C	0

Figure 3.1 Machine M_1' and a Diagnosable Realization M_1

Figure 3. 1 where M_1 is a diagnosable realization of M_1' . One can verify that M_1' is reduced but not diagnosable and yet, under functions h_1, h_2 , and h_3 , M_1 realizes M_1' and the sequence bb , for example, is a distinguishing sequence of M_1 .

In order to determine what properties affect the complexity of diagnosable realizations, three special cases of the general problem are considered in the discussion that follows:

1. Find a diagnosable machine M which realizes M' with $|Q| = |Q'|$ and $|Z| = |Z'|$. This is the "control input" augmentation problem.
2. Find a diagnosable realization M of M' with $|Q| = |Q'|$ and $|I| = |I'|$. This is the "test output" augmentation problem.
3. Find a diagnosable realization M of M' with $|I| = |I'|$.

This is the "state-output" augmentation problem.

To preclude the possibility of exploiting any input redundancy in the reduced machine M' we will assume throughout the discussion that M' is transition-distinct, that is, for all $a, b \in I'$ such that $a \neq b$, there is some state q for which $\delta'(q, a) \neq \delta'(q, b)$. This results in no loss of generality since every reduced machine M'' is realizable by some transition-distinct reduced machine M' .

Section 3.2 Control Input Augmentation

Given a reduced machine M' , let us consider first the class of diagnosable realizations of M' restricted such that each realization has the same number of states and output symbols as M' . In this case we will show that diagnosable realizations can always be obtained where the realizing machine has at most one more input symbol than the realized machine. Moreover, in many cases one can obtain realizations which are optimal in the sense that they have the shortest possible distinguishing sequences.

We begin by recalling from Lemma 2.3 that every single-input machine is diagnosable if and only if it is reduced. Applying this lemma, a nondiagnosable machine can be "combined" with a single-input reduced machine to obtain a diagnosable realization. More precisely,

Theorem 3.1 If M' is a machine then there is a diagnosable realization M of M' such that $|I| = |I'| + 1$, $|Q| = |Q'|$ and $|Z| = |Z'|$.

Proof: Let $M'' = (\{d\}, Q', Z', \delta'', \omega'')$ be any reduced single-input machine ($d \notin I'$) with state set and output alphabet equal to those of the given machine M' . Consider now the machine M defined in terms of M' and M'' as follows:

$$M = (I' \cup \{d\}, Q', Z', \delta, \omega)$$

where

$$\delta(q, a) = \begin{cases} \delta'(q, a) & \text{if } a \neq d \\ \delta''(q, a) & \text{if } a = d \end{cases}$$

and

$$\omega(q, a) = \begin{cases} \omega'(q, a) & \text{if } a \neq d \\ \omega''(q, a) & \text{if } a = d. \end{cases}$$

Then if we let

$$h_1(x) = x, \text{ for all } x \in (I')^+$$

$$h_2(q) = q, \text{ for all } q \in Q'$$

and

$$h_3(z) = z, \text{ for all } z \in Z$$

it follows that M realizes M' under h_1, h_2 , and h_3 ; and M is diagnosable with distinguishing sequence d^{n-1} , where $n = |Q|$.

Example 3.1

To illustrate Theorem 3.1, let us consider the machine M_2' whose description is shown in Figure 3.2. Note that M_1' does not have any distinguishing sequence.

$M_2' =$		a	b	$M_2' = (I_2', Q_2', Z_2', \delta_2', \omega_2')$ $I_2' = \{a, b\}$ $Q_2' = \{1, 2, 3, 4\}$ $Z_2' = \{0, 1\}$
	1	1/0	2/0	
	2	1/0	3/0	
	3	1/0	4/0	
	4	1/1	1/0	

Figure 3.2 The Machine M_2'

Let us next construct a reduced 4-state machine and append it to M_2' in the manner described by the proof of Theorem 3.1. The resultant machine M_2 is diagnosable with cc as a DS as shown in Figure 3.3.

Note that M_1 realizes M_2' under h_1, h_2 and h_3 where

$$h_1(x) = x \text{ for all } x \in (I_2')^+,$$

$$h_2(q) = q \text{ for all } q \in Q_2'$$

and

$$h_3(z) = z \text{ for all } z \in Z_2.$$

		a	b	c	$M_2 = (I_2, Q_2, Z_2, \delta_2, \omega_2)$ $I_2 = I_2' \cup \{c\} = \{a, b, c\}$ $Q_2 = Q_2' = \{1, 2, 3\}$ $Z_2 = Z_2' = \{0, 1\}$
M_2	1	1/0	2/0	2/0	
	2	1/0	3/0	4/1	
	3	1/0	4/0	3/0	
	4	1/1	1/0	1/1	

Figure 3.3 A Diagnosable Realization of M_2'

Thus from a machine-theoretic point of view, diagnosable realizations with input augmentation are rather easily obtained. Aside from questions regarding the complexity of the corresponding networks, a remaining question of interest for this class of realizations is the required complexity of a distinguishing sequence, i.e. its length $lg(x)$. From the construction of Theorem 3.1, it follows that there exist $(n-1)$ -diagnosable realizations of any given n -state reduced machine.

It is possible, however, to obtain diagnosable realizations of lower order and, interestingly, it is always possible to obtain an optimally diagnosable realization for any machine by augmenting at most one input symbol. Furthermore, if the number of output symbols is a power of a prime, then it is possible to obtain a strongly connected optimally diagnosable realization. To this end, we recall from Lemma 2.1 that a machine $M = (I, Q, Z, \delta, \omega)$ is optimally diagnosable if M has a distinguishing sequence of length $\lceil \log_p n \rceil$ where $|Q| = n$ and $|Z| = p$. The fact that these can be achieved is primarily based on the following result of single-input machines, that is,

Lemma 3.1 For any given integers $n > 1$ and $p > 1$, there is an n -state, p -output and single-input sequential machine M which is optimally diagnosable. Moreover, if p is a power of a prime, then M can be chosen such that it is strongly connected.

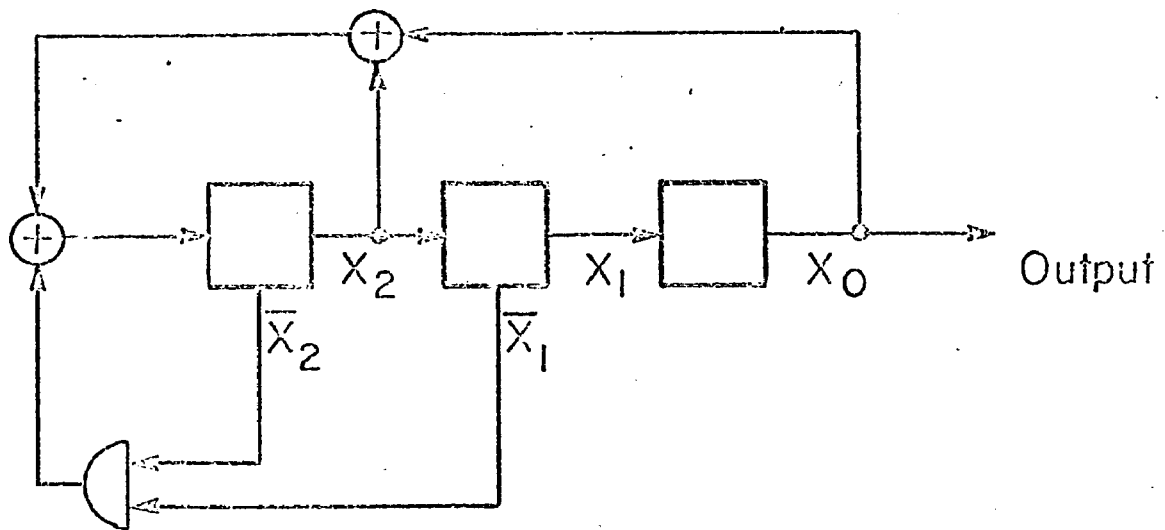
Proof: Let $m = \lceil \log_p n \rceil$ and consider an m -stage p -ary loop free shift register with the output derived from the last stage. Thus to determine the initial state of this machine, it is only necessary to shift the register m times and such a machine is obviously optimally diagnosable. If p is a prime and $\lceil \log_p n \rceil = m$, consider an m -stage p -ary shift register with a single output line from its last stage and a cycle in its state-graph of length n (where $p^{m-1} < n \leq p^m$). That such registers always exist is shown in [20], for example. If we now let M be the submachine defined by the cycle of length n , it follows that each state q in the cycle can be

identified after m shifts, i. e., M is an m -diagnosable single-input machine. If p is a power of a prime q , say $p = q^s$, the same reasoning applies to an ms -stage q -ary shift register with s output lines from stages $ms, m(s-1), \dots, m$.

An example of a strongly connected and optimally diagnosable single-input machine is given in Figure 3.4 for $n = 8$ and $p = 2$. If we now apply the construction used in the proof of Theorem 3.1 to single-input machines guaranteed by Lemma 3.1, we obtain

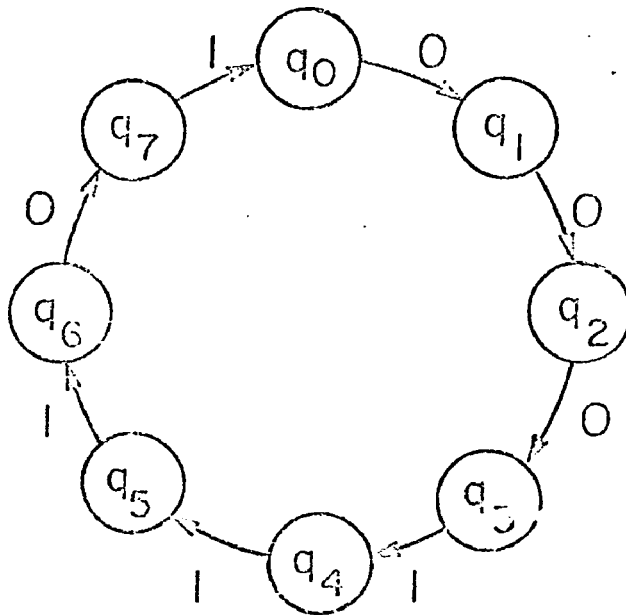
Theorem 3.2 If $M' = (I', Q', Z', \delta', \omega')$ is a machine, then there is an optimally diagnosable realization $M = (I, Q, Z, \delta, \omega)$ of M' such that $|I| = |I'| + 1$, $|Q| = |Q'|$ and $|Z| = |Z'|$. Moreover, if $|Z'|$ is a prime power, then M can be chosen such that it is strongly connected.

An application of Theorem 3.2 is illustrated in Figure 3.5. Recently, a similar approach of input augmentation for designing diagnosable machines has been proposed by Murakami, et al [41]. The length of distinguishing sequence obtained there is n for an n -state machine where we have shown here that optimal length of distinguishing sequence is generally obtainable using our method. In any case, we see that by allowing input augmentation diagnosable machine realizations are easily obtained. From a network point of view, however, such realizations may require greater network complexity than desired or than required by some other realization technique. This motivates the examination of realizations wherein input augmentation is not permitted, the subject of the section that follows.



The generator is obtained by modifying the max. length binary linear sequence generator which corresponds to a primitive polynomial $h(x) = x^3 + x^2 + 1$. [42].

(a) An 8-State shift register generator



(b) State diagram generated by (a)

Figure 3.4 An 8-State, Single Input and Binary Output Machine with a DS of Length 3

M_3' :

$Q' \backslash I'$	a	b
1	1/0	2/0
2	1/0	3/0
3	1/0	4/0
4	1/1	1/0

M_3 :

$Q \backslash I$	a	b	c
1	1/0	2/0	2/0
2	1/0	3/0	4/1
3	1/0	4/0	3/0
4	1/1	1/0	1/1

cc is a DS of M_3

$$h_1 \mid I' = e_I: I' \longrightarrow I$$

$$h_2 = e_Q: Q' \longrightarrow Q$$

$$h_3 = e_Z: Z \longrightarrow Z'$$

Figure 3.5 Machine M_3' and a Diagnosable Realization M_3

Section 3.3 Test Output Augmentation

Suppose once again that M' is a reduced machine but consider now the class of diagnosable realizations of M' restricted such that each realization has the same number of input symbols and states as M' . In other words only the output alphabet can be augmented in realizing M' . That such realizations always exist is established by the following theorem.

Theorem 3.3 If $M' = (I', Q', Z', \delta', \omega')$ is a reduced machine, then there exists a diagnosable realization $M = (I, Q, Z, \delta, \omega)$ of M' such that $|I| = |I'|$ and $|Q| = |Q'|$.

Proof: Given $M' = (I', Q', Z', \delta', \omega')$, to obtain the desired realization consider the machine $M = (I', Q', Z, \delta', \omega)$ where $Z = Q' \times I'$ and $\omega(q, a) = (q, a)$, for all $q \in Q'$ and $a \in I'$. Then under functions h_1, h_2 and h_3 where

$$h_1 = \text{identity function on } (I')^+$$

$$h_2 = \text{identity function on } Q'$$

and
$$h_3(q, a) = \omega'(q, a)$$

it follows that M realizes M' . Moreover, any sequence a ($a \in I'$) is a DS of M and hence M is diagnosable.

It is interesting to note that the proof of Theorem 3.3 demonstrates not only the existence of diagnosable realizations for any

given reduced machine using output augmentation but also the existence of 1-diagnosable realizations. In other words, with unbounded output augmentation it is always possible to obtain a diagnosable realization with a distinguishing sequence of length 1. This suggests that there is a tradeoff between time (i. e., length of shortest distinguishing sequence) and space (i. e., number of output symbols) in the realizing machine. To investigate the extremes of this tradeoff, let us first consider the minimum time case, i. e., let us require that the realization be 1-diagnosable and determine the minimum size output alphabet that will suffice for such a realization. This can be accomplished as follows.

Given a reduced machine $M' = (I', Q', Z', \delta', \omega')$, define, for each $a \in I'$, the function $\omega_a': Q' \rightarrow Z'$ where $\omega_a'(q) = \omega'(q, a)$, for all $q \in Q'$. If further we let

$$p = |\mathcal{R}(\omega')| \quad (\mathcal{R}(\omega') \text{ is the range of } \omega')$$

and
$$t = \max\{|\mathcal{R}(\omega_a')| \mid a \in I'\}$$

then the least upper bound on the size of the output alphabet of the realizing machine is given by:

Theorem 3.4 If M' is a reduced machine, then there is a 1-diagnosable realization $M = (I, Q, Z, \delta, \omega)$ of M' such that $|I| = |I'|$, $|Q| = |Q'|$ and $|Z| = |Q'| + p - t$. Moreover, there is no such 1-diagnosable realization of M' with fewer output symbols.

Proof: Let $M' = (I', Q', Z', \delta', \omega')$ where without loss of generality, we can assume that $Q' \cap Z' = \phi$, and let $d \in I'$ such that $t = |\mathcal{R}(\omega_d')|$.

To obtain the desired realization, consider now the machine

$$M = (I', Q', Z, \delta', \omega)$$

where

$$Z = Q' \cup (\mathcal{R}(\omega') - \mathcal{R}(\omega_d'))$$

and

$$\omega(q, a) = \begin{cases} q & \text{if } a = d \\ r & \text{if } \omega'(q, a) = \omega'(r, d) \text{ for some } r \in Q' \\ \omega'(q, a) & \text{otherwise} \end{cases}$$

Then if we let

$$h_1 = \text{identity function on } (I')^+$$

$$h_2 = \text{identity function on } Q'$$

$$h_3(z) = \begin{cases} z & \text{if } z \in \mathcal{R}(\omega') - \mathcal{R}(\omega_d') \\ \omega'(z, d) & \text{if } z \in Q' \end{cases}$$

it can be shown that M realizes M' . Moreover, the sequence d is obviously a DS of M and hence M is a 1-diagnosable.

To see that $|Q'| + p - t$ is the least upper bound on the size of the output alphabet for such a 1-diagnosable realization, suppose to the contrary, i.e. there exists a 1-diagnosable realization M of M' such that $|Z| < |Q'| + p - t$ and M realizes M' under h_1, h_2 and h_3 . Then $\exists d \in I$ such that $\omega(q, d) = \omega(r, d) \iff q = r$ for all $q, r \in Q$ which implies that

$|\mathcal{R}(\omega_d)| = |Q| = |Q'|$. Therefore $|Z| < |\mathcal{R}(\omega_d)| + p-t$ or equivalently, since $\mathcal{R}(\omega_d) \subseteq Z$, $|Z| - |\mathcal{R}(\omega_d)| = |Z - \mathcal{R}(\omega_d)| < p-t$. By the general properties of functions we have

$$|h_3(Z - \mathcal{R}(\omega_d))| \leq |Z - \mathcal{R}(\omega_d)|$$

and

$$h_3(Z) - h_3(\mathcal{R}(\omega_d)) \subseteq h_3(Z - \mathcal{R}(\omega_d)).$$

Hence, from the above inequality, it follows that

$$|h_3(Z) - h_3(\mathcal{R}(\omega_d))| < p-t$$

or, equivalently, since $h_3(\mathcal{R}(\omega_d)) \subseteq h_3(Z)$,

$$|h_3(Z)| - |h_3(\mathcal{R}(\omega_d))| < p-t$$

But $h_3(Z) \supseteq \mathcal{R}(\omega')$ since M realizes M' . Therefore $|h_3(Z)| \geq p$ and substituting in the above inequality

$$|h_3(\mathcal{R}(\omega_d))| > t \tag{1}$$

Moreover, since M' is transition distinct and h_2 must be 1-1, it can be shown that h_1 restricted to I' is 1-1 and hence onto. Accordingly, there is an input $d' \in I'$ such that $h_1(d') = d$ and as M realizes M' we have

$$h_3(\omega(h_2(q), d)) = \omega'(q, d') \text{ for all } q \in Q'.$$

Since h_2 is onto, it follows that

$$|h_3(\mathcal{R}(\omega_d))| = |\mathcal{R}(\omega_{d'})| \quad (2)$$

and hence by (1) and (2)

$$|\mathcal{R}(\omega_{d'})| > t$$

This contradicts the definition of t , thereby proving the theorem.

Interpreting Theorem 3.4 in network terms, it is interesting to note that in order to obtain a 1-diagnosable network realization, it is never necessary to use the output of every memory element as a test output. The latter would correspond to an augmented output alphabet of $n + p$ symbols whereas only $n+p-t$ are required (where $t \geq 2$ if M' has at least two states).

Turning to the other extreme of the space-time tradeoff problem, suppose that no limit is placed on the length of the shortest distinguishing sequence and let us consider the output complexity required, that is, the minimum size output alphabet required for a diagnosable realization.

Given some input sequence $x \in I^+$ it has been shown by Theorem 2.1 that x is a distinguishing sequence if and only if x is a homing sequence of M and no pair of states converge under x . This characterization of DS will be found useful later on in constructing output augmented diagnosable realizations. Using this characterization along with the fact that every reduced machine is homable it is also immediate that

Theorem 3.5 Every reduced, convergence free machine is diagnosable.

Thus, applying Theorem 3.5, one approach to obtaining a diagnosable realization M of M' would be to eliminate (in M) all the state pair convergences in M' , that is, for all $q, r \in Q'$ such that $q \neq r$, $\delta'(q, a) = \delta'(r, a)$ and $\omega'(q, a) = \omega'(r, a)$, require that ω be such that $\omega(h_2(q), h_1(a)) \neq \omega(h_2(r), h_1(a))$. This approach, however, may not yield a realization with fewest output symbols since a reduced machine need not be convergence free to be diagnosable.

A second approach, which can result in realizations requiring fewer output symbols than convergence free realizations, is to consider a homing sequence x of M' and realize M' in such a way that $h_1(x)$ is a homing sequence of M and for every state pair $\{q, r\}$ that converges under x , the corresponding pair $\{h_2(q), h_2(r)\}$ does not converge under $h_1(x)$. If no new state pair convergences are introduced in the process, $h_1(x)$ is a DS of M , i.e., M is a diagnosable realization of M' . The question that remains open using this approach is how to choose a homing sequence of M' that results in a minimum size output alphabet for the realizing machine M . One could, of course, consider all minimal homing sequences (minimal in the sense that no subsequence is a homing sequence) and choose one requiring minimum output augmentation. However, this procedure

appears impractical from a computational point of view unless the number of states of the machine is relatively small.

A third approach is to consider a restricted class of distinguishing sequences where the restriction is not directly related to the length of the sequences. In particular, one such class which has been studied in connection with fault detection experiments [32] is the set of distinguishing sequences which consist of repetitions of a single input symbol. More precisely, let us say that a sequence $x \in I^+$ is a repeated symbol distinguishing sequence (RDS) if x is a distinguishing sequence and, for some $a \in I$ and some integer k , $x = a^k$. Then to obtain diagnosable machine realizations with an RDS we observe first of all that

Theorem 3.6 A sequential machine M has an RDS if and only if there exists a single input submachine of M that is reduced.

Proof: Suppose $M = (I, Q, Z, \delta, \omega)$ has an RDS a^k , $a \in I$. Then a^k is obviously a DS of the single-input submachine $M' = (\{a\}, Q, Z, \delta', \omega')$ where δ' and ω' are δ and ω restricted to $Q \times \{a\}$. Thus M' is diagnosable and, by Lemma 2.3, M' is reduced. Conversely, if M contains a reduced single-input submachine M' with $I' = \{a\}$ then, by Lemma 2.3, M' is diagnosable and hence any DS of M' is of the form a^k . As this sequence is also a DS of M , M has an RDS.

In view of Theorem 3.6, to obtain a diagnosable realization with an RDS it suffices to imbed a reduced single-input submachine in the realization. Since this condition is also necessary, the minimum size output alphabet required is the size below which no such submachine can be imbedded. Relative to the problem of imbedding a reduced single-input submachine in the realization, we consider first the special case where M' is a (nonreduced) single-input machine and we desire a reduced realization M of M' where $|Q| = |Q'|$. This can be achieved by a procedure that uses the "testing graph" [32] of a machine to determine homing sequences and a "distinguishing graph" for book-keeping.

Before we define these terms more precisely and describe the procedure, it will be helpful to review some basics in graph theory. A graph G consists of a finite nonempty set V of points together with a prescribed set X , called lines, of unordered pairs of distinct points of V . Two points $\{u, v\}$ of V are said to be adjacent if $\{u, v\} \in X$. A directed graph G is a graph whose lines are ordered pairs of distinct points, called directed lines.

Definition 3.2 A testing graph of a sequential machine

$M = (I, Q, Z, \delta, \omega)$ is a directed graph (allowing self loops) which is constructed as follows: Each point of the graph corresponds to a pair

of distinct states which are either indistinguishable under some input or is a state pair successor of the former. A directed line is drawn from point $\{q_i, q_j\}$ to point $\{q_m, q_n\}$ iff $\exists a \in I \ni$

$$\omega(q_i, a) = \omega(q_j, a)$$

$$\delta(q_i, a) = q_m$$

$$\delta(q_j, a) = q_n$$

where $q_i, q_j, q_m, q_n \in Q$ and, m and n need not be distinct from i and j , but $i \neq j$ and $m \neq n$.

It is obvious that each component of the testing graph of a single-input machine is either unicyclic (containing only one cycle) or a tree. A testing graph is said to be acyclic if it does not contain any cycle. In the case of single-input machines, it can be shown that a machine has a HS if and only if its testing graph is acyclic. Since a single-input machine is reduced if and only if it is both homable and convergence free, the concept of testing graph can be incorporated into the characterization of the realizing machine.

Definition 3.3 Let $M = (\{a\}, Q, Z, \delta, \omega)$ be a single-input sequential machine and $z \in Z$. A z -distinguishability graph of M is a graph G_z whose points are states of M and which satisfies the following conditions:

- i) For every $q \in V(G_z)$, $\omega(q, a) = z$.
- ii) $\{q, r\} \in X(G_z)$ if $\delta(q, a) = \delta(r, a)$.
- iii) $\{q, r\} \in X(G_z)$ if $\{\delta(q, a), \delta(r, a)\} = \{q, r\}$.
- iv) Choose a pair of states $\{q, r\}$ from a cycle of the testing graph $\ni \omega(q, a) = \omega(r, a) = z$ and put $\{q, r\} \in X(G_z)$. The corresponding cycle in the testing graph is then eliminated from further consideration.
- v) Step iv) is iterated until either all cycles in the testing graph are eliminated or no more cycle can be eliminated by considering z .
- vi) Trivial components are excluded.

We recall that a coloring of a graph is an assignment of colors to its points so that no two adjacent points have the same color. An n-coloring of a graph G uses n colors. The chromatic number $\chi(G)$ is defined as the minimum n for which G has n -coloring [23]. Techniques of computing chromatic number and minimum coloring of a graph have been discussed in Berge [6]. The problem of finding a minimum size output diagnosable realization can be seen to be equivalent to that of constructing a set of z -distinguishability graphs for each z so that the sum of the chromatic numbers of G_z 's is minimum. Although the following technique does not guarantee a minimum solution, it does not require an exhaustive construction of all possible z -distinguishability graphs and the results obtained appear to be satisfactory.

Let $M' = (\{a\}, Q', Z', \delta', \omega')$ be the given single-input machine and let $M = (\{a\}, Q, Z, \delta, \omega)$ be the desired realization where for simplicity we let $Q = Q'$ and $\delta = \delta'$. Also let $Z' = \{o_1, o_2, \dots, o_p\}$ and $Z = \{o_{1,1}, o_{1,2}, \dots, o_{1,i_1}, o_{2,1}, o_{2,2}, \dots, o_{2,i_2}, \dots, o_{p,1}, o_{p,2}, \dots, o_{p,i_p}\}$ where each i_j is to be determined and $i_j \geq 1$. Then to design M ,

Procedure 3.1

- (1) Construct the cycles of the testing graph of M' and denote them T_0 .
- (2) For each self loop of T_0 with output o_i and each state pair convergence in M' with output o_i , add a line to the o_i -distinguishability graph G_{o_i} using conditions i), ii), and iii) of Definition 3.3. Removing all self loops from T_0 and call the remaining cycles T_1 .
- (3) Compute the chromatic number of each G_{o_j} constructed in step (2), $\chi(G_{o_j})$, and set $i_j = \chi(G_{o_j})$. Let $Z_s' = \{o_i \in Z' \mid \text{there is a } G_{o_i} \neq \phi \text{ constructed in step (2)}\}$. It is clear that $i_j \geq 2$ for each $o_j \in Z_s'$. Let T_k be the cycles of T_0 left after k iterations and set $k = 1$.
- (4) Let $Z_k' = \{o_i \in Z' \mid o_i \text{ is an output of } T_k\}$. If $Z_s' \cap Z_k' = \phi$, go to step (5). Otherwise, for each $o_j \in Z_s' \cap Z_k'$, select a state pair $\{q, r\}$ from a cycle of T_k (i.e. a point of that cycle) with output o_j such that addition of the line $\{q, r\}$ to G_{o_j} does not increase its chromatic number. If this is successful, remove that cycle from

T_k and increment k by 1. This step is iterated until $T_k = \phi$, $Z_s' \cap Z_k' = \phi$ or increasing the chromatic number of some G_{o_j} becomes necessary.

- (5) Let k_i be the maximum number of cycles in T_k such that each of these cycles has a point with output o_i and each pair of these points have no state in common.

Choose $o_j \in Z_k'$ $k_j = \max_{o_i \in Z_k'} k_i$ and select these k_j state pairs. Add these k_j lines to G_{o_j} , remove the k_j cycles from T_k and increment k by 1. This process is iterated until for some integer n , $T_n = \phi$.

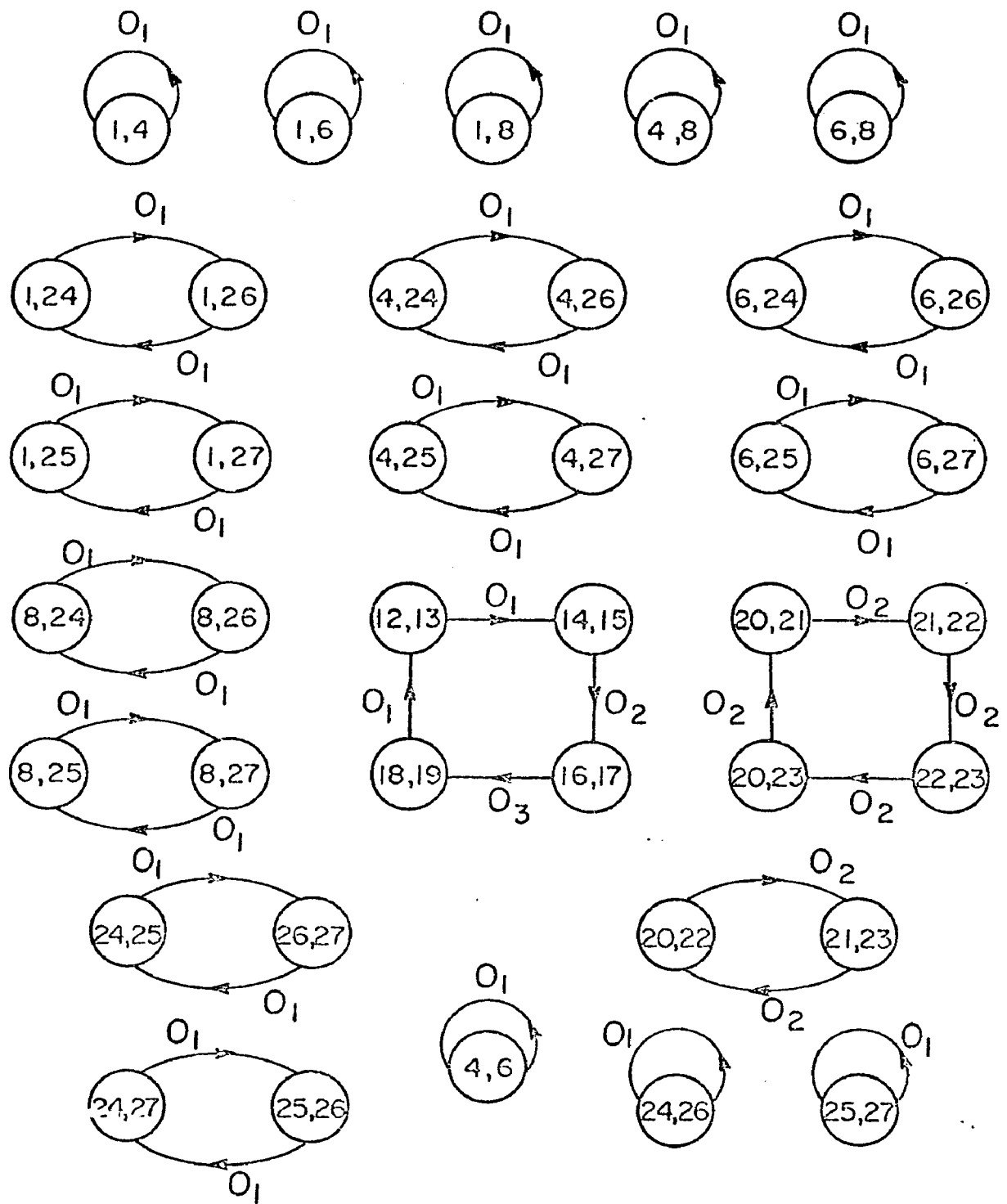
- (6) For each G_{o_j} constructed, assign appropriate symbol from Z to each point of G_{o_j} using $i_j = \chi(G_{o_j})$ so that no two adjacent points of G_{o_j} have the same symbol. The size of the realizing output alphabet = $\sum_{o_i \in Z'} \chi(G_{o_i})$ where $\chi(G_{o_i}) = 1$ if $G_{o_i} = \phi$.

Example 3.2

To illustrate Procedure 3.1, let us consider the single-input machine M_4' given in Table 3.1. Note that no reduction of the machine M_4' should be made since it is implicitly understood that M_4' is a single-input submachine of some other machine. T_o of M_4' is shown in Figure 3.6. The nonempty distinguishability graphs obtained using step (2) are shown in Figure 3.7. It can be easily found that

Q	a
1	1/o ₁
2	1/o ₁
3	1/o ₁
4	4/o ₁
5	4/o ₁
6	6/o ₁
7	6/o ₁
8	8/o ₁
9	8/o ₁
10	12/o ₂
11	12/o ₂
12	14/o ₁
13	15/o ₁
14	16/o ₂
15	17/o ₂
16	18/o ₃
17	19/o ₃
18	12/o ₁
19	13/o ₁
20	21/o ₂
21	22/o ₂
22	23/o ₂
23	20/o ₂
24	26/o ₁
25	27/o ₁
26	24/o ₁
27	25/o ₁

Table 3.1 Machine M₄'

Figure 3.6 T_0

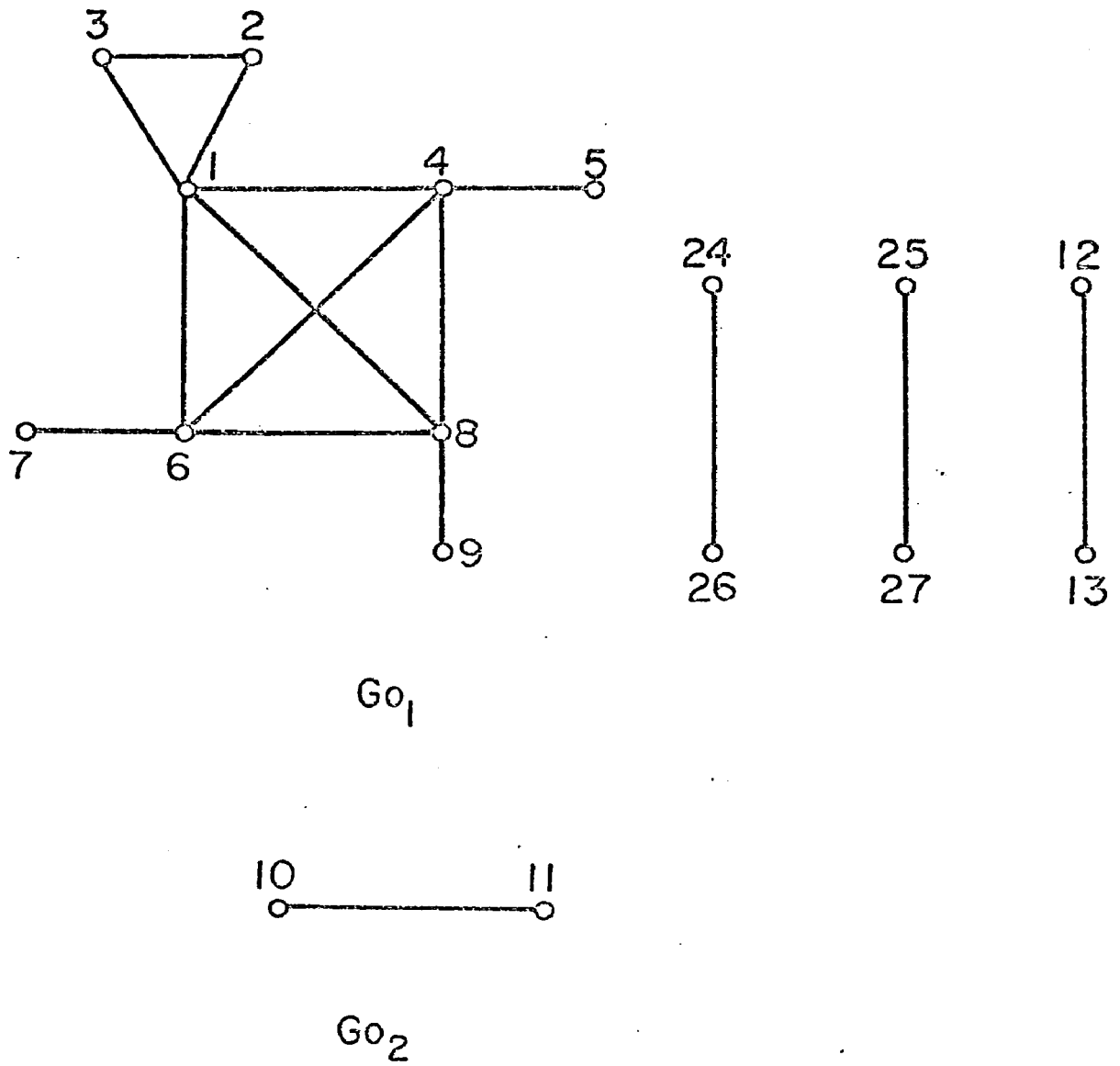


Figure 3.7 G_{o_1} and G_{o_2} After Step (3)

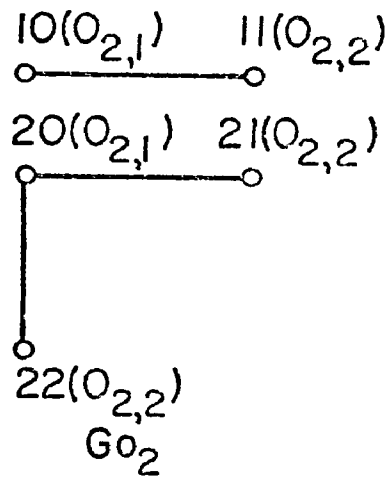
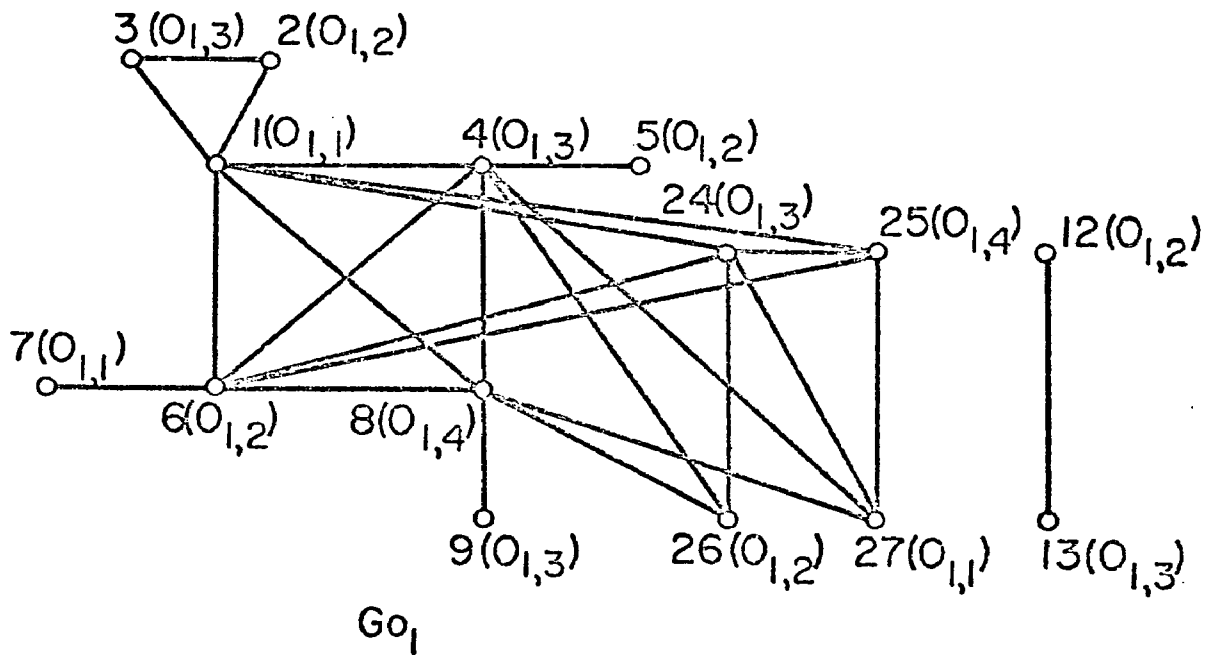


Figure 3.8 G_{o_1} and G_{o_2} After Step (4)

Q	a
1	$1/o_{1,1}$
2	$1/o_{1,2}$
3	$1/o_{1,3}$
4	$4/o_{1,3}$
5	$4/o_{1,2}$
6	$6/o_{1,2}$
7	$6/o_{1,1}$
8	$8/o_{1,4}$
9	$8/o_{1,3}$
10	$12/o_{2,1}$
11	$12/o_{2,2}$
12	$14/o_{1,2}$
13	$15/o_{1,3}$
14	$16/h_3^{-1}(o_2)$
15	$17/h_3^{-1}(o_2)$
16	$18/o_{3,1}$
17	$19/o_{3,1}$
18	$12/h_3^{-1}(o_1)$
19	$13/h_3^{-1}(o_1)$
20	$21/o_{2,1}$
21	$22/o_{2,2}$
22	$23/o_{2,2}$
23	$20/h_3^{-1}(o_2)$
24	$26/o_{1,3}$
25	$27/o_{1,4}$
26	$24/o_{1,2}$
27	$25/o_{1,1}$

Table 3.2 Machine M_4

$\chi(G_{o_1}) = 4$ and $\chi(G_{o_2}) = 2$ and we set $i_1 = 4$ and $i_2 = 2$. Using step (4), the constructed G_{o_1} and G_{o_2} are shown in Figure 3.8. Note that in executing step (4) we should bear in mind not to increase the maximum degree of the graph since the chromatic number is bounded by the maximum degree of the graph plus 1 [23]. Step (5) is not needed in this example. The assignment of output symbols in step (6) to G_{o_1} and G_{o_2} is also shown in Figure 3.8, and the size of the realizing output set is $= 4+2+1 = 7$. Table 3.2 shows M_4 as a collection of diagnosable machines which realize M_4' .

After solving the problem of obtaining a diagnosable realization of a single-input machine, the problem of seeking a diagnosable realization with an RDS for a given machine involves only a straightforward process of imbedding. The first step of this process requires the selection of an input symbol d from the machine $M' = (I', Q', Z', \delta', \omega')$. Then the single-input submachine $M_d' = (\{d\}, Q', Z', \delta_d', \omega_d')$ is considered for diagnosable realization using the procedure stated earlier. Finally the imbedding involves the assignment of appropriate new output symbols to M' to obtain a diagnosable realization with RDS, $M = (I', Q', Z, \delta', \omega)$. This procedure will be stated below. Let Sc_a be the sum of chromatic numbers of the distinguishability graphs and k_a be cycles of T_1 of the single-input submachine of M', M_a' , after steps (1) and (2) of Procedure 3.1 are applied.

Procedure 3.2

- (1) Choose $R \subseteq I' \ni R = \{a \in I' \mid (Sc_a + k_a) \text{ is minimum}\}$.
- (2) Choose $d \in R \ni |\mathcal{R}(\omega_d')| \leq |\mathcal{R}(\omega_a')| \quad \forall a \in R$.
- (3) Use steps (1) through (6) of Procedure 3.1 to obtain a diagnosable realization of M_d' , denoted as $M_d = (\{d\}, Q', Z, \delta_d', \omega_d')$.
- (4) Construct M using the following ω

$$\omega(q, a) = \begin{cases} \omega(q, d) & \text{if } a = d \\ o_{i,j} & \text{if } a \neq d \text{ and } \omega'(q, a) = o_i \in \mathcal{R}(\omega_d') \text{ for } 1 \leq j \leq i_i \\ o_{i,1} & \text{if } \omega'(q, a) \notin \mathcal{R}(\omega_d') \end{cases}$$

In this section, we have presented several methods of constructing diagnosable machine realizations of a given reduced machine using output recoding while permitting increases in the size of output alphabet. These methods are by no means inclusive. However, they serve to illustrate some basic approaches that may be taken. Using the general concept of a diagnosable realization introduced in Section 3.1, other feasible techniques can also be investigated. For example, in using the output augmentation technique, if we do not restrict the size of state set in the realizing machine to be the same as that of the realized machine, then in many cases it is possible to further reduce the size of output alphabet in the realizing machine. This serves to motivate, in the next section, the study of realizations where increase in the number of states is allowed.

Section 3.4 State-Output Augmentation

A natural question which we would like to ask next is whether it is possible to obtain a diagnosable realization of any given machine with only state augmentation. If the answer is affirmative, such a method of realization will be very useful in many cases where no input-output terminals can be added to the design. Unfortunately, as to be shown in the following, this is impossible. Nevertheless, we will also show in the succeeding development that when it is used in conjunction with the output augmentation methods of last section, reduction in the size of augmented output set can be obtained.

To simplify our discussion, let us assume that the machines to be considered have onto output functions, i. e. if $M = (I, Q, Z, \delta, \omega)$ is a machine, then

$$\mathcal{R}(\omega) = Z.$$

Lemma 3.2 Let M' be a transition-distinct and reduced machine. If machine M realizes M' under (h_1, h_2, h_3) , then

- 1) h_1 is 1-1, and
- 2) h_3 is onto.

Proof: To prove 1), let us suppose the contrary, i. e. $\exists a, b \in I', \ni a \neq b$ but $h_1(a) = h_1(b)$. Since h_1 is a semigroup homomorphism, $\forall x \in (I')^*$, $h_1(ax) = h_1(bx)$. Now M realizes M' and by Definition 3.1, $\forall q' \in Q'$ and $x \in (I')^*$

$$\begin{aligned}
\beta_{q'}(ax) &= h_3(\beta_{h_2(q')}(h_1(ax))) \\
&= h_3(\beta_{h_2(q')}(h_1(bx))) \\
&= \beta_{q'}(bx).
\end{aligned}$$

It follows that $\delta'(q', a) \equiv \delta'(q', b)$. But M' is reduced, thus

$$\delta'(q', a) = \delta'(q', b) \quad \forall q' \in Q'$$

contrary to the assumption that M' is transition distinct.

To show 2), we also suppose the contrary, i.e. $\exists z' \in Z' \ni \forall z \in Z, h_3(z) \neq z'$. Since we assume ω' is onto Z' , $\exists q' \in Q'$ and $x \in (I')^+ \ni$

$$\beta_{q'}(x) = z' \neq h_3(\beta_{h_2(q')}(h_1(x))).$$

Thus M cannot realize M' , a contradiction to our hypothesis and the proof of the theorem is now complete.

With the help of this lemma, we can now show that if no input-augmentation is permitted, in order to design a diagnosable realization of a given nondiagnosable reduced machine, it is necessary to augment the output alphabet. More precisely,

Theorem 3.7 Let $M' = (I', Q', Z', \delta', \omega')$ be a transition-distinct nondiagnosable reduced machine. If $M = (I, Q, Z, \delta, \omega)$ is a diagnosable realization of M' and $|I| = |I'|$, then

$$|Z| > |Z'|.$$

Proof: Let us assume that the hypothesis is false, i. e.

$|Z| \leq |Z'|$. From Lemma 3.2, h_3 is onto, it follows that $|Z'| = |h_3(Z)|$. Furthermore, by the general properties of functions, $|h_3(Z)| \leq |Z|$, we have $|Z'| \leq |Z|$. Thus this contrary assumption leads to the only case where $|Z| = |Z'|$. It is clear then that h_3 is 1-1 and onto. Similarly, since h_1 is 1-1 and $|I| = |I'|$, it must be the case that h_1 is onto. Now since M is diagnosable, let $x \in (I')^+$ be such that $h_1(x)$ is a DS of M . Let $q, r \in Q'$ and if

$$\hat{\beta}_q(x) = \hat{\beta}_r(x)$$

then by Definition 3.1, for every prefix y of x

$$\beta_q(y) = h_3(\beta_{h_2(q)}(h_1(y))) = \beta_r(y) = h_3(\beta_{h_2(r)}(h_1(y))).$$

It follows that

$$\hat{\beta}_{h_2(q)}(h_1(x)) = \hat{\beta}_{h_2(r)}(h_1(x))$$

But since $h_1(x)$ is a DS of M , it is immediate that $h_2(q) = h_2(r)$. We claim if $h_2(q) = h_2(r)$, then $q = r$. Suppose $q \neq r$ but $h_2(q) = h_2(r)$

$$\begin{aligned} \beta_q(x) &= h_3(\beta_{h_2(q)}(h_1(x))) = h_3(\beta_{h_2(r)}(h_1(x))) \\ &= \beta_r(x) \quad \forall x \in (I')^+ \end{aligned}$$

i. e.

$$q \equiv r$$

But since M' is reduced, it must be that $q = r$. This is to say that x is a DS of M' , a contradiction to our hypothesis of M' being nondiagnosable. Thus $|Z| > |Z'|$.

Interpreting Theorem 3.7 in a slightly different way, it says that given a reduced nondiagnosable machine, it is impossible to obtain a diagnosable realization by just augmenting the state set alone. Thus input or output augmentation is necessary for obtaining a diagnosable realization. However, we have shown in Theorem 3.1 that augmenting one input symbol is sufficient for obtaining a diagnosable realization of any machine, and as such the minimum number of input symbols required has been achieved. Nevertheless, in the case of output augmentation the question of whether the number of augmented output symbols can be further reduced by state augmentation has not been answered. Toward obtaining an affirmative answer to this question, let us next consider the case where the only restriction placed on the realization is that the input alphabet size of the realizing machine remains unchanged compared to the given machine.

Recall that a reduced machine is not diagnosable due to the condition that there are state set convergences under every homing sequence of the machine. As also discussed earlier, one technique of obtaining a diagnosable realization (for a given machine) is to eliminate (in the realizing machine) all state set convergences under a homing sequence. Thus we will first consider the problem of eliminating state set convergences under a particular input symbol by increasing, relative to a given machine, both the number of output symbols and number of states in the realizing machine.

To minimize the amount of information required to eliminate some state set convergences (in the realizing machine) of some given machine, it is often found to be convenient to treat only parts of the machine at a time. Since we are dealing with parts of the machine, the realizations of these parts will have to preserve the structure of the original complete machine. In this respect, the type of machine realization in Definition 3.1 is found inadequate because it deals only with the input-output behavior of the machine. Thus a stronger type of machine realization preserving machine structure is needed.

Let $M = (I, Q, Z, \delta, \omega)$ be a sequential machine, then, the state behavior of M for initial state q ($q \in Q$) is the function

$$\alpha_q: I^* \rightarrow Q$$

where

$$\alpha_q(x) = \bar{\delta}(q, x)$$

for all $x \in I^*$. Then the type of realization we desire is that of "homomorphic" realization which simulates state behavior as well as input-output behavior [38].

Definition 3.4 M homomorphically realizes M' if there is a triple of functions (η_1, η_2, η_3) , where

$\eta_1: (I')^+ \rightarrow I^+$ is a semigroup homomorphism such that

$$\eta_1(I') \subseteq I$$

$$\eta_2: Q \rightarrow Q' \text{ (onto)}$$

$$\eta_3: Z \rightarrow Z'$$

such that, for all $q \in Q$ and $a \in I'$,

$$\text{i) } \alpha'_{\eta_2(q)}(a) = \eta_2(\alpha_q(\eta_1(a))),$$

and

$$\text{ii) } \beta'_{\eta_2(q)}(a) = \eta_3(\beta_q(\eta_1(a))).$$

From the above definition and Definition 3.1, it follows that if M homomorphically realizes M' then M realizes M' . However, the converse is not true. For considering any machine M and its reduced version M_R , M and M_R mutually realizes one another. On the other hand, although M homomorphically realizes M_R , M_R need not homomorphically realize M . Thus the homomorphic requirement is indeed a proper restriction. In case M realizes M' and M' is reduced, then M realizes M' if and only if M homomorphically realizes M' [38].

Returning now to the problem of eliminating state set convergences by state-output augmentation, let $M' = (I', Q', Z', \delta', \omega')$ be a machine, $S \subseteq Q'$, and for any $s, s' \in S$, $\delta(s, a) = \delta(s', a)$ and $\omega'(s, a) = \omega'(s', a) = z$ for some $a \in I'$ and $z \in Z'$. We can subdivide the treatment of this problem into the following three cases:

- 1) $\delta'(s, a) = q \in S \quad \forall s \in S.$
- 2) $\delta'(s, a) = q, q \notin S$
and $\omega'(q, a) \neq \omega'(s, a) \quad \forall s \in S.$
- 3) $\delta'(s, a) = q, q \notin S$
and $\omega'(q, a) = \omega'(s, a) \quad \forall s \in S.$

These three cases will be discussed separately in the following.

Case 1 Given a machine M' , let $S \subseteq Q'$, $a \in I$ and

$$\left. \begin{array}{l} \delta'(s, a) = q \in S \\ \omega'(s, a) = z \in Z' \end{array} \right\} \quad \forall s \in S$$

In order to eliminate this state set convergence, the minimum number of output symbols in the realizing machine is $|S|$ if methods of output augmentation are used. We will show in the following that it is possible to reduce this bound if state augmentation is permitted.

Theorem 3.8 Let $M' = (I', Q', Z', \delta', \omega')$, $S \subseteq Q'$, $|S| = k$, $\delta'(s, a) = q$ and $\omega'(s, a) = z$ for all $s \in S$, some $a \in I'$, $z \in Z'$ and $q \in S$. Then the submachine of M' with states S , input $\{a\}$ can be homomorphically realized by a diagnosable machine $M_a = (\{a\}, Q, Z, \delta, \omega)$ with

$$|Z| \leq \lfloor \frac{k}{2} \rfloor + 1$$

and

$$|Q| \leq k + \lceil \frac{k}{2} \rceil - 1$$

where $\lfloor \frac{k}{2} \rfloor$ is the largest integer not greater than $\frac{k}{2}$.

Proof: Let $M'_a = (\{a\}, S, \{z\}, \delta | Sx\{a\}, \omega | Sx\{a\})$ be the submachine of M' which contains the state set convergence under consideration.

Without loss of generality assume M'_z has the following state table.

	a
1	1/z
2	1/z
3	1/z
$\vdots$	$\vdots$
k	1/z

$$S = \{1, 2, \dots, k\}$$

Let us construct a reduced machine M_a which homomorphically realizes M'_a by splitting state 1 and creating an output set which distinguishes each state pair. Such a machine is shown below:

	a
1	q_1/z_1
2	q_2/z_1
3	q_3/z_1
$\vdots$	$\vdots$
$\lceil \frac{k}{2} \rceil - 1$	$q_{\lceil \frac{k}{2} \rceil - 1}/z_1$
$\lceil \frac{k}{2} \rceil$	$1/z_1$
$\vdots$	$\vdots$
k	$1/z_{\lceil \frac{k}{2} \rceil + 1}$
q_1	q_1/z_2
q_2	q_2/z_3
$\vdots$	$\vdots$
$q_{\lceil \frac{k}{2} \rceil - 1}$	$q_{\lceil \frac{k}{2} \rceil - 1}/z_{\lceil \frac{k}{2} \rceil}$

where

$$Z = \{z_i \mid i=1, 2, \dots, \lceil \frac{k}{2} \rceil + 1\}$$

$$Q = \{1, 2, \dots, k, q_1, q_2, \dots, q_{\lceil \frac{k}{2} \rceil - 1}\}$$

If we define the triple of functions (η_1, η_2, η_3) as the following:

η_1 is an identity function on $\{a\}^+$

$$\eta_2(t) = \begin{cases} t & \text{if } t \in S - \{1\} \\ 1 & \text{if } t \in \{1, q_i \mid i=1, 2, \dots, \lceil \frac{k}{2} \rceil - 1\} \end{cases}$$

and

$$\eta_3(z_i) = z \text{ for all } z_i \in Z$$

Then we claim M_a homomorphically realizes M'_a . To show this, let $t \in Q$ and $t \in S - \{1\}$. Then $\delta'(\eta_2(t), a) = \delta'(t, a) = 1$. Now, from the state table of M_a , if $t \in S - \{1\}$ then $\delta(t, \eta_1(a)) = \delta(t, a) \in \{1, q_i \mid i=1, 2, \dots, \lceil \frac{k}{2} \rceil - 1\}$ and by the definition of η_2 , $\eta_2(\delta(t, \eta_1(a))) = \eta_2(\delta(t, a)) = 1$. If $t \in \{1, q_i \mid i=1, 2, \dots, \lceil \frac{k}{2} \rceil - 1\}$, then $\delta'(\eta_2(t), a) = \delta'(1, a) = 1$ and $\delta(t, a) \in \{1, q_i \mid i=1, 2, \dots, \lceil \frac{k}{2} \rceil - 1\}$. Thus $\eta_2(\delta(t, a)) = 1$. In either case, we have the following: if $t \in Q$, then $\delta'(\eta_2(t), a) = \eta_2(\delta(t, \eta_1(a)))$. To verify the second condition of homomorphic realization, we note that $\forall t \in Q$, $\beta'_{\eta_2(t)}(a) = z$ and since $\forall z_i \in Z$ $\eta_3(z_i) = z$, we have $\beta'_{\eta_2(t)}(a) = \eta_3(\beta_t(\eta_1(a)))$. This completes the proof of the theorem.

Note that in Theorem 3.8, in order to distinguish each state in Q , it requires the repetition of the corresponding input symbol $\eta_1(a)$ twice, i.e. the sequence $\eta_1(a) \eta_1(a)$, in the realizing machine. This suggests the investigation of the extreme case where the minimum size output set can be obtained in the realizing machine if length of the input sequence required to distinguish Q (and thus the number of augmented states) is unlimited. This is accomplished as follows:

Theorem 3.9 Let $M' = (I', Q', Z', \delta', \omega')$, $S \subseteq Q'$, $|S| = k$, $\delta'(s, a) = q$ and $\omega'(s, a) = z$ for all $s \in S$, some $a \in I'$, $z \in Z'$ and $q \in S$. Then the submachine of M' with states S , input $\{a\}$ can be homomorphically realized by a diagnosable machine

$$M_a = (\{a\}, Q, Z, \delta, \omega) \text{ with}$$

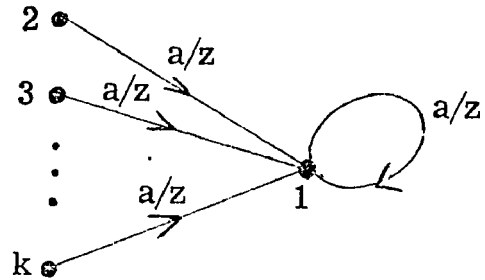
$$|Z| = 2 \text{ and}$$

$$|Q| \leq 2k - 2.$$

Moreover, M_a is ℓ -diagnosable with $\ell \leq k$.

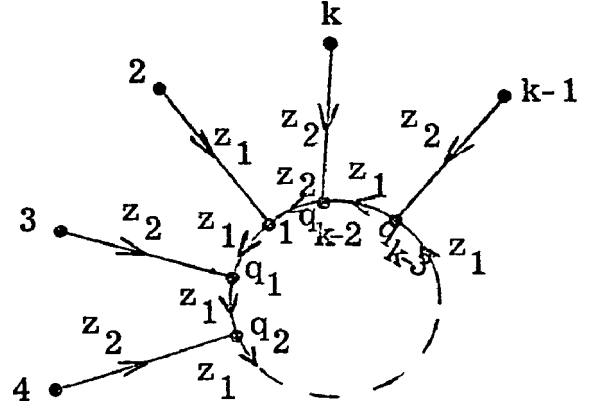
Proof: For $k \leq 2$, the theorem is trivially satisfied since no state augmentation is necessary. For $k \geq 3$, let M'_a be the single-input submachine of M' having states $S = \{1, 2, \dots, k\}$ and input $\{a\}$ as shown below:

	a
1	1/z
2	1/z
3	1/z
$\vdots$	$\vdots$
k	1/z



Let us construct a reduced single-input machine M_a which homomorphically realizes M'_a by splitting state 1 and creating a two symbol output set which distinguishes each state pair in M'_a . Such a machine M_a is shown below:

	a
1	q_1/z_1
2	$1/z_1$
3	q_1/z_2
$\vdots$	$\vdots$
k-1	q_{k-3}/z_2
k	q_{k-2}/z_2
q_1	q_2/z_1
q_2	q_3/z_1
$\vdots$	$\vdots$
q_{k-3}	q_{k-2}/z_1
q_{k-2}	$1/z_2$



where

$$Z = \{z_1, z_2\}$$

$$Q = \{1, 2, \dots, k, q_1, q_2, \dots, q_{k-2}\}.$$

M_a homomorphically realizes M'_a under (η_1, η_2, η_3) where

$$\eta_1[\{a\}^+ \text{ is an identity function on } \{a\}^+$$

$$\eta_2(t) = \begin{cases} t & \text{if } t \in S - \{1\} \\ 1 & \text{if } t \in \{1, q_i \mid i=1, 2, \dots, k-2\} \end{cases}$$

and $\eta_3(z_i) = z \quad \text{for } i=1, 2.$

To see that M_a is ℓ -diagnosable for $\ell \leq k$, we note that the state diagram of M_a is unicyclic with a cycle of length $k-1$. Since any pair

of states on the cycle is distinguishable by a sequence of length $k-1$, it is clear that any pair of states not on the cycle are distinguishable by a sequence of length k .

It is interesting to note that Theorem 3.9 demonstrates the possibility of eliminating a state set convergence of any size by adding at most one more output symbol using state-output augmentation. However, to distinguish the augmented state set, a repetition of the corresponding input symbol $\eta_1(a)$ of at most k times is required where k is the size of the original state set in the convergence. Some complications may occur in designing a diagnosable realization due to this limitation but let us postpone their discussions until after the following example which illustrates the application of these theorems.

Example 3.3

Consider the machine M'_5 whose state table is given in Figure 3.9.

	a	b	
1	1/0	2/1	$I' = \{a, b\}$
2	1/0	3/0	$Z' = \{0, 1\}$
3	1/0	4/0	$Q' = \{1, 2, 3, 4, 5, 6\}$
4	5/0	2/1	
5	6/0	2/1	
6	1/1	2/1	

Figure 3.9 Machine M'_5

It can be easily verified that M'_5 is reduced but not diagnosable.

Using output-augmentation methods of Section 3.3, it can be shown that the minimum size output alphabet for a diagnosable realization is 4. Now consider the single input submachine of M'_5 :

$$M'_{5,a} =$$

	a
1	1/0
2	1/0
3	1/0

Employing the constructive procedure in the proof of Theorem 3.7, it is immediate that $M'_{5,a}$ is homomorphically realized by the following machine $M_{5,a}$

$$M_{5,a} =$$

	a
1	q_1/z_1
2	$1/z_1$
3	$1/z_2$
q_1	q_1/z_2

with $(\eta'_1, \eta'_2, \eta'_3)$ where

η'_1 is an identity function on $\{a\}^+$

$$\eta'_2(t) = \begin{cases} t & \text{if } t \in \{2, 3\} \\ 1 & \text{if } t \in \{1, q\} \end{cases}$$

$$\eta'_3(z_i) = 0 \quad \text{for } i=1, 2$$

Expanding $M_{5,a}$ we obtain the following diagnosable realization of M'_5 , M_5 as shown in Figure 3.10.

	a	b	
1	q_1/z_1	$2/z_3$	$I = \{a, b\}$
2	$1/z_1$	$3/z_1$	$Z = \{z_1, z_2, z_3\}$
3	$1/z_2$	$4/z_1$	
q_1	q_1/z_2	$2/z_3$	$Q = \{1, 2, 3, q_1, 4, 5, 6\}$
4	$5/z_1$	$2/z_3$	
5	$6/z_1$	$2/z_3$	
6	$1/z_3$	$2/z_3$	

Figure 3.10 A Diagnosable Realization of M'_5 , M_5

The three functions of realizations (η_1, η_2, η_3) relating M_5 and M'_5 are:

η_1 is an identity on I^+

$$\eta_2(t) = \begin{cases} t & \text{if } t \in \{2, 3, 4, 5, 6\} \\ 1 & \text{if } t \in \{1, q_1\} \end{cases}$$

$$\eta_3(z_i) = \begin{cases} 0 & \text{for } i=1, 2 \\ 1 & \text{for } i=3 \end{cases}$$

It can be shown that M_5 has a DS, aaa, and the realizing output set has 3 symbols comparing to 4 symbols required for the methods of the last section.

Note that M'_5 of Example 3.3 has a repeated symbol homing sequence (RHS) aaa and elimination of the state set convergence is sufficient for obtaining a diagnosable realization. However, in more general cases, this may not be as easy due to the fact that a state set converging under input symbol a may require the repetition of $\eta_1(a)$ many times to fully distinguish its corresponding state set in the realizing machine. Complications may happen in that either there are other state set convergences under the same input symbol a or that any repetition of a fails to be part of any HS in the given machine. Nevertheless, the first problem can be treated in a way similar to what has been done here or other cases of eliminating state set convergences to be presented in the subsequent discussions. The second problem can be treated by eliminating cycles of the testing graph of some single input submachine of the given machine and is also to be presented later in this section. Thus it will be seen that this limitation may not be as severe as it might have appeared. What we have accomplished here is a method of reducing the number of test outputs which is otherwise unattainable by the output augmentation methods of last section. Another point illustrated by Example 3.3 is the importance of homomorphic realization of Definition 3.4. In order to obtain a complete diagnosable realization of M'_5 , it is necessary to embed the diagnosable realization obtained from $M'_{5,a}, M_{5,a}$ into a machine realizing M'_5 . The homomorphic requirement serves to relate the partial realizing structure and the complete realization.

Case 2 Given a machine M' , let $S \subseteq Q'$, $a \in I'$,

$$\left. \begin{aligned} \delta'(s, a) &= q \notin S \\ \omega'(s, a) &= z \in Z' \end{aligned} \right\} \quad \forall s \in S,$$

$$\omega'(q, a) = z' \neq z$$

The problem here is to find a method of realization by increasing the number of states and output symbols in the realizing machine so that the corresponding state set of S in the realizing machine, $\eta_2^{-1}(S)$, can be distinguished by a sequence formed from the symbol $\eta_1(a)$. Before we present our results, let us first review several notions of sequential machines to be used in the discussion.

Definition 3.5 A sequential machine $M = (I, Q, Z, \delta, \omega)$ is incompletely specified if the transition function δ is a function from a proper subset by $Q \times I$ into Q and the output function ω is a function from a proper subset of $Q \times I$ onto Z .

Thus for any given state $q \in Q$ of an incompletely specified machine M , we can partition I^+ into two disjoint subsets of sequences A_q and $\bar{A}_q$ where

$$A_q = \{x \in I^+ \mid \hat{\beta}_q(x) \text{ is defined}\}$$

and $\bar{A}_q = I^+ - A_q$. A_q is called the applicable set of q in M . In case $A_q = \phi$, we say q is a degenerate state. An incompletely specified machine is diagnosable if when the machine is started from any

nondegenerate state, the machine is diagnosable. If $Q'' \subseteq Q$, and $x \in I^+$, then Q'' is said to be distinguishable by x if $\forall s, t \in Q''$

$$x \in A_s \cap A_t \text{ and } \hat{\beta}_s(x) = \hat{\beta}_t(x) \implies s = t.$$

Furthermore, if $M' = (I', Q', Z', \delta', \omega')$ and $M = (I, Q, Z, \delta, \omega)$ are two incompletely specified machines, we say M realizes M' if $\exists (h_1, h_2, h_3)$ such that whenever $\delta'(q, a)$ and $\omega'(q, a)$ are defined for any $q \in Q'$ and $a \in I'$, then $\omega(h_2(q), h_1(a))$ is also defined and the usual conditions of realization are satisfied. Similarly, we say M homomorphically realizes M' if $\exists (\eta_1, \eta_2, \eta_3)$ such that whenever $\delta'(q, a)$ and $\omega'(q, a)$ are defined for any $q \in Q'$ and $a \in I'$, then $\delta(\eta_2^{-1}(q), \eta_1(a))$ and $\omega(\eta_2^{-1}(q), \eta_1(a))$ are also defined and the usual conditions of homomorphic realization are satisfied. With the help of these definitions, we will first show that, in Case 2, it is possible to reduce the number of output symbols required for test augmentation if the number of states is increased in the realizing machine.

Theorem 3.10 Let $M' = (I', Q', Z', \delta', \omega')$, $S \subseteq Q'$, $|S| = k$, $\delta'(s, a) = q$, $\omega'(s, a) = z$ and $\omega'(q, a) = z' \neq z$, for all $s \in S$, some $a \in I'$, $z, z' \in Z'$ and $q \notin S$. Then $\exists$ a machine M realizing M' under (h_1, h_2, h_3) such that $h_2(S)$ is distinguishable by the sequence $h_1(a) h_1(a)$. Moreover,

$$\begin{aligned} |h_3^{-1}(\mathcal{R}(\omega' | S \times \{a\}))| &\leq 2 \\ |h_3^{-1}(\mathcal{R}(\omega' | \{q\} \times \{a\}))| &\leq \lfloor \frac{k}{2} \rfloor + 1 \end{aligned}$$

and

$$|Q| \leq |Q'| + \lfloor \frac{k}{2} \rfloor$$

Proof: The proof of this theorem is basically similar to that of Theorem 3.8. However, since a submachine must be closed, let us consider an incompletely specified single-input machine

$M'_a = (\{a\}, S \cup \{q, \delta'(q, a)\}, \{z, z'\}, \delta'_a, \omega'_a)$ where

$$\delta'_a = \delta' \mid \{S \cup \{q\}\} \times \{a\}$$

$$\omega'_a = \omega' \mid \{S \cup \{q\}\} \times \{a\}.$$

The state table of M'_a is shown below:

	a	
1	q/z	$S = \{1, 2, \dots, k\}$ and $r = \delta'(q, a).$
2	q/z	
$\vdots$	$\vdots$	
k	q/z	
q	r/z'	
r	-/-	

We note that r is a degenerate state in M'_a . To prove the theorem, it is sufficient to show that there is a single-input diagnosable realization $M_a = (\{a\}, Q_a, Z_a, \delta_a, \omega_a)$ of M'_a satisfying conditions specified in the theorem. Such a machine M_a is demonstrated by the following state table.

$M_a =$

	a
1	q_1/z_1
2	q_2/z_1
$\vdots$	$\vdots$
$\lfloor \frac{k}{2} \rfloor - 1$	$q_{\lfloor \frac{k}{2} \rfloor - 1} / z_1$
$\lfloor \frac{k}{2} \rfloor$	q / z_1
$\lfloor \frac{k}{2} \rfloor + 1$	q_1 / z_2
$\vdots$	$\vdots$
k	$q_{\lfloor \frac{k}{2} \rfloor} / z_2$
q	r / z'_1
q_1	r / z'_2
q_2	r / z'_3
$\vdots$	$\vdots$
$q_{\lfloor \frac{k}{2} \rfloor}$	$r / z'_{\lfloor \frac{k}{2} \rfloor + 1}$
r	-/-

It can be easily verified that M_a homomorphically realizes M'_a under (η_1, η_2, η_3) and has a DS $\eta_1(a) \eta_1(a)$, where

η_1 is an identity function on $\{a\}^+$

$$\eta_2(t) = \begin{cases} t & \text{if } t \in S \text{ or if } t = r \\ q & \text{if } t \in \{q, q_i \mid i=1, 2, \dots, \lfloor \frac{k}{2} \rfloor\} \end{cases}$$

$$\eta_3(w) = \begin{cases} z & \text{if } w \in \{z_1, z_2\} \\ z' & \text{if } w \in \{z'_i \mid i=1, 2, \dots, \lfloor \frac{k}{2} \rfloor + 1\} \end{cases}$$

To show that the bounds stated in the theorem can be achieved, it suffices to note that

$$|\eta_3^{-1}(z)| = 2$$

$$|\eta_3^{-1}(z')| = \lfloor \frac{k}{2} \rfloor + 1$$

and

$$\begin{aligned} |Q_a| &= k + 2 + \lfloor \frac{k}{2} \rfloor \\ &= |Q'_a| + \lfloor \frac{k}{2} \rfloor \end{aligned}$$

To construct the complete realization desired, it is sufficient to relate (η_1, η_2, η_3) and (h_1, h_2, h_3) as follows:

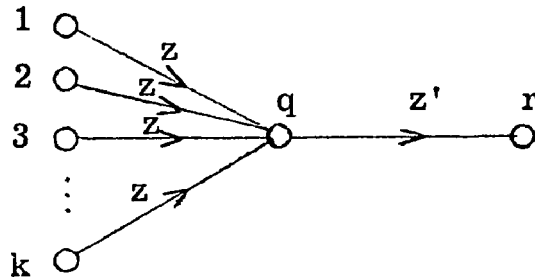
$$h_1 | \{a\}^+ = \eta_1$$

$$h_2 | \{a\} \times S \cup \{q, r\} = \eta_2^{-1}$$

$$h_3 | Z_a = \eta_3.$$

Note that in Theorem 3.10 we only consider the necessary information related to the state set convergence. If the knowledge of the complete machine structure is utilized, the bounds given may be further reduced but the amount of information required for analysis may be prohibitive for large machines. Although Theorem 3.10 demonstrates

possibility of reducing the number of augmented output symbols by increasing the number of states in the realizing machine, the bounds given are not the best even in the restricted sense of using only the necessary information related to the state set convergence. In general, our goal is to reduce the number of test output terminals needed while at the same time, trying to minimize the number of states to be added. To achieve this goal, it is generally desirable to minimize the total number of output symbols and the number of states required and to equalize the sizes of the pre-images of the original two output symbols under the realizing output function η_3 . More precisely, if M' is an incompletely specified single input machine with the following state diagram



where the label on each directed line represents the output under that transition, our goal here is to find a single input diagnosable machine M such that

- i) M homomorphically realizes M' under (η_1, η_2, η_3) ,
 - ii) $\text{Max} \{ |\eta_3^{-1}(z)|, |\eta_3^{-1}(z')| \}$ is minimized,
- and iii) $|Q| - |Q'|$ is minimized.

Note that the state diagram of M' given above is an in-tree of depth 2 [23]. Thus this problem can be restated as a problem in graph theory. First, let us review some more basics of graph theory. Let μ and ν be two adjacent points in a directed graph G . If the directed line goes from μ to ν then we say ν is adjacent from μ and μ is adjacent to ν . The outdegree $od(\nu)$ of a point ν is the number of points adjacent from it, and the indegree $id(\nu)$ is the number of points adjacent to it. A source in G is a point which can reach all others and a sink is a point which can be reached from all others.

The problem then can be stated as follows. Given an in-tree of depth 2, G' , with k sources and 1 sink, find another in-tree of depth 2, G , with k sources and 1 sink such that the maximum in-degree of any point in G is minimized and G' is a homomorphic image of G . A rather simple solution of this problem is obtained by splitting the point q in the above state diagram of M' into m points where m is an integer determined as follows:

$$m = \begin{cases} \lfloor \sqrt{k} \rfloor & \text{if } \lfloor \sqrt{k} \rfloor - \sqrt{k} > \sqrt{k} - \lfloor \sqrt{k} \rfloor \\ \lceil \sqrt{k} \rceil & \text{if } \lfloor \sqrt{k} \rfloor - \sqrt{k} < \sqrt{k} - \lfloor \sqrt{k} \rfloor \\ p & \text{if } k = p^2 \text{ for some integer } p \end{cases} \quad (3.1)$$

Tabulations of the state diagrams of M' and M for $k = 3$ to $k = 12$ are shown in Table 3.3A and Table 3.3B. The following procedure formally summarizes the solution method.

TABLE 3.3A

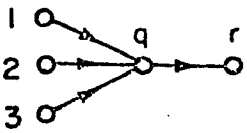
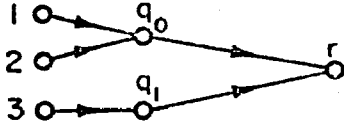
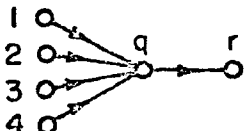
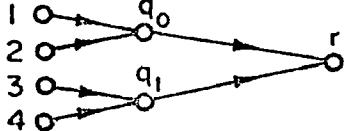
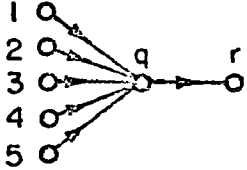
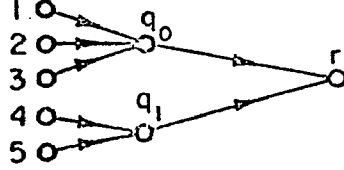
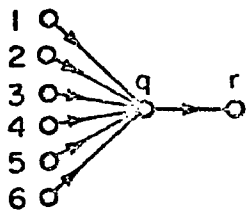
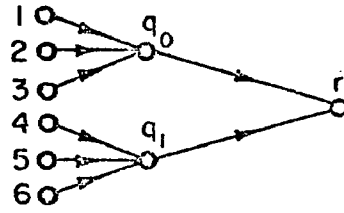
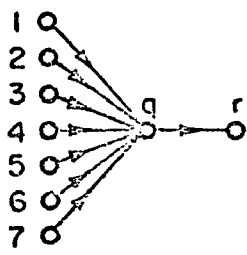
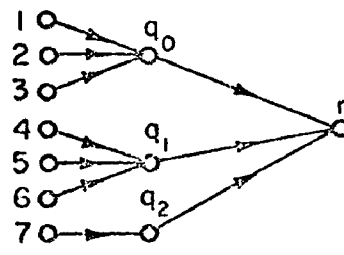
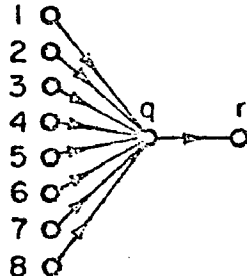
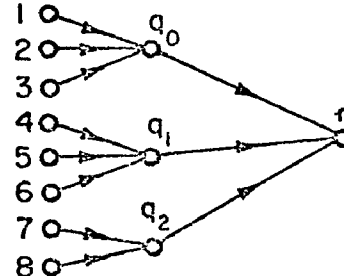
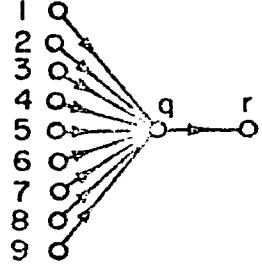
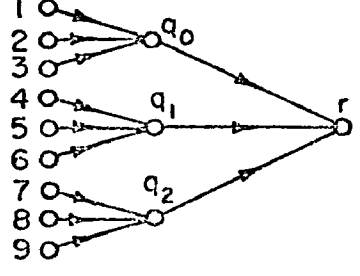
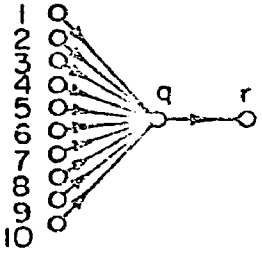
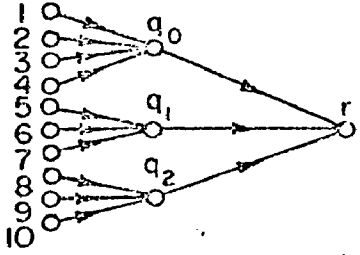
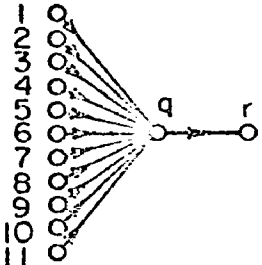
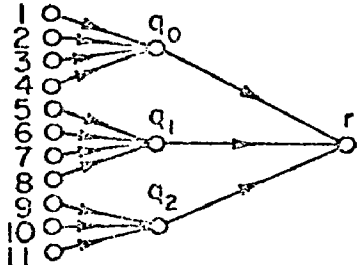
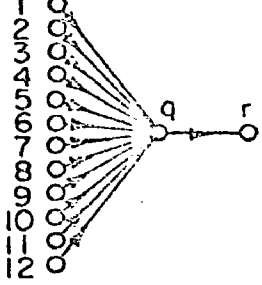
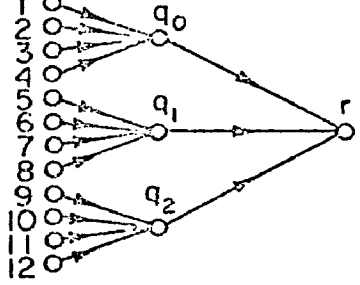
k	M'	M
3		
4		
5		
6		
7		
8		

TABLE 3.3B

k	M'	M
9		
10		
11		
12		

Procedure 3.3

- (1) Split the point q in the state diagram of M' into m points, labeled $q_0, q_1, \dots, q_{m-1}$ where m is determined according to Equation (3.1).
- (2) If $\lceil \sqrt{k} \rceil - \sqrt{k} > \sqrt{k} - \lfloor \sqrt{k} \rfloor$, then $m = \lfloor \sqrt{k} \rfloor$. Let $n = k - m^2$, then for $i=1, 2, \dots, k$

$$\omega(i, a) = \begin{cases} z_{(i-1) \bmod (m+1)} & \text{if } i \leq n \lceil \sqrt{k} \rceil \\ z_{(i-1-n) \bmod m} & \text{if } i > n \lceil \sqrt{k} \rceil \end{cases}$$

$$\delta(i, a) = \begin{cases} q_{\lfloor \frac{i}{m+1} \rfloor - 1} & \text{if } i \leq n \lceil \sqrt{k} \rceil \\ q_{\lfloor \frac{i-n}{m} \rfloor - 1} & \text{if } i > n \lceil \sqrt{k} \rceil \end{cases}$$

$$\left. \begin{aligned} \omega(q_i, a) &= z'_i \\ \delta(q_i, a) &= r \end{aligned} \right\} \quad \text{for } i=0, 1, \dots, m-1$$

- (3) If $\lceil \sqrt{k} \rceil - \sqrt{k} \leq \sqrt{k} - \lfloor \sqrt{k} \rfloor$, then $m = \lceil \sqrt{k} \rceil$ and for $i=1, 2, \dots, k$

$$\omega(i, a) = z_{(i-1) \bmod m},$$

$$\delta(i, a) = q_{\lfloor \frac{i}{m} \rfloor - 1},$$

and

$$\left. \begin{aligned} \omega(q_i, a) &= z'_i \\ \delta(q_i, a) &= r \end{aligned} \right\} \quad \text{for } i=0, 1, 2, \dots, m-1$$

- (4) The state diagram so constructed represents a machine M which homomorphically realizes M' under functions

(η_1, η_2, η_3) where

$\eta_1: \{a\}^+ \rightarrow \{a\}^+$ is an identity function

$$\eta_2(t) = \begin{cases} t & \text{if } t \in \{1, 2, \dots, k, r\} \\ q & \text{if } t \in \{q_0, q_1, \dots, q_{m-1}\} \end{cases}$$

$$\eta_3(w) = \begin{cases} z & \text{if } w = z_i \\ z' & \text{if } w = z'_i \end{cases}$$

Note that in Procedure 3.3 (2)

$$|\eta_3^{-1}(z)| = \lceil \sqrt{k} \rceil,$$

$$|\eta_3^{-1}(z')| = \lfloor \sqrt{k} \rfloor,$$

and

$$|\eta_2^{-1}(q)| = \lfloor \sqrt{k} \rfloor,$$

and in (3)

$$|\eta_3^{-1}(z)| = \lceil \sqrt{k} \rceil,$$

$$|\eta_3^{-1}(z')| = \lceil \sqrt{k} \rceil,$$

and

$$|\eta_2^{-1}(q)| = \lceil \sqrt{k} \rceil.$$

Thus the following theorem can be stated to summarize the above solutions.

Theorem 3.11 Let $M' = (I', Q', Z', \delta', \omega')$, $S \subseteq Q'$, $|S| = k$, $\delta'(s, a) = q$, $\omega'(s, a) = z$ and $\omega'(q, a) = z' \neq z$, for all $s \in S$, some $a \in I'$, $z, z' \in Z'$ and $z \notin S$. Then $\exists$ a machine M homomorphically realizing M' under (η_1, η_2, η_3) such that $\eta_2^{-1}(S)$ is distinguishable by the sequence $\eta_1(a) \eta_1(a)$. Moreover,

$$|\eta_3^{-1}(\mathcal{R}(\omega' | \eta_2(S) \times \{a\}))| \leq \lceil \sqrt{k} \rceil,$$

$$|\eta_3^{-1}(\mathcal{R}(\omega' | \{\eta_2(q)\} \times \{a\}))| \leq \lceil \sqrt{k} \rceil,$$

and $|Q| \leq |Q'| + \lceil \sqrt{k} \rceil - 1$.

Note that in Theorem 3.11 the size of realizing output set increases $2(\lceil \sqrt{k} \rceil - 1)$ over the original output set while if only output augmentation is used we need to increase by $k - 1$. Thus the saving on the number of test outputs that needs to be added can be quite significant for large k . Furthermore, since the added output symbols are evenly divided, the number of test points can be reduced. To pay for the reduction of the number of output test points, we have to increase the number of states by $\lceil \sqrt{k} \rceil - 1$. The following example illustrates some of these advantages.

Example 3.4

Let M'_6 be a seven state submachine of some machine having 6 of its states converging to the seventh state under some input a . In this case $k = 6$ and $r \in S$. If we use the output augmentation method,

5 additional output symbols will be needed to obtain a diagnosable realization of M'_6 . Using Procedure 3.3 and from Table 3.3A, a diagnosable realization can be obtained by increasing one more state and 3 more output symbols. M'_6 and a diagnosable realization M_6 of M'_6 are shown in Figure 3.11. It can be easily verified that M_6 has a DS aa and M_6 homomorphically realizes M'_6 under (η_1, η_2, η_3) where

η_1 is an identity function on $\{a\}^+$

$$\eta_2(t) = \begin{cases} t & \text{if } t \in \{1, 2, 3, 4, 5, 6\} \\ 7 & \text{if } t \in \{7, 8\} \end{cases}$$

$$\eta_3(\{00, 01, 02\}) = 0$$

and

$$\eta_3(\{10, 11\}) = 1$$

$M'_6 =$		a
	1	7/0
	2	7/0
	3	7/0
	4	7/0
	5	7/0
	6	7/0
	7	1/1

$M_6 =$		a
	1	7/00
	2	7/01
	3	7/02
	4	8/00
	5	8/01
	6	8/02
	7	1/10
	8	1/11

Figure 3.11 M'_6 and One of Its Diagnosable Realizations M_6

Case 3 Given a machine M' , let $S \subseteq Q'$, $a \in I'$

$$\left. \begin{aligned} \delta'(s, a) &= q \notin S \\ \omega'(s, a) &= \omega(q, a) = z \in Z' \end{aligned} \right\} \quad \forall s \in S$$

It is clear that case 3 is similar to case 2 except the output value of q under input a is the same as that of any state in S . Our results in this case follows directly from Theorem 3.11.

Theorem 3.12 Let $M' = (I', Q', Z', \delta', \omega')$, $S \subseteq Q'$, $|S| = k$, $\delta'(s, a) = q$, $\omega'(s, a) = \omega'(q, a) = z$ for all $s \in S$, some $a \in I'$ and $q \notin S$. Then there is a machine M homomorphically realizing M' under $\{\eta_1, \eta_2, \eta_3\}$ such that $\eta_2^{-1}(S)$ is distinguishable by the sequence $\eta_1(a) \eta_1(a)$. Moreover,

$$|\eta_3^{-1}(z)| \leq \lceil \sqrt{k} \rceil$$

and

$$|Q| \leq |Q'| + \lceil \sqrt{k} \rceil - 1$$

Summarizing the efforts made to eliminate state set convergences for obtaining a diagnosable realization, we have developed design techniques which allow reduction of the number of output symbols or terminals required, in cases that this is possible, by increasing the number of states in the realizing machine. In many cases it is possible to minimize the number of output symbols required by augmenting a sufficient number of states. Compromises

between the number of additional outputs and the number of additional states are usually desirable in practice. Such compromises can be easily derived from the techniques we have presented.

As noted previously, the elimination of state set convergences under some input by state-output augmentation may lead to complication where repetition of the corresponding input fails to be a part of any DS in the realizing machine. This difficulty is usually caused by the fact that the remaining states involved cannot be distinguished after the application of this repeated input sequence due to cycles of testing graph or additional state set convergences under some other input symbols. The elimination of cycles of testing graph can be treated by output augmentation but we will explore here situations where increasing the number of states in the realizing machine will also result in the reduction of realizing output set.

To study the problem of eliminating cycles of testing graph (or more formally, the problem of acyclic testing graph realization), let us begin by considering an n -state single input identity machine where all the outputs are the same. There are $\binom{n}{2}$ cycles of length 1 in the testing graph of this machine and if output augmentation is used to eliminate these cycles, a realizing output set of size n is required. Now consider the state diagram of the machine which has n cycles of length 1. The output augmentation involves labeling n distinct cycles

of length 1. The strategy here is to increase the length of some of the cycles in the state diagram so that the number of distinct labelings is less than n . To show that this is possible, let us first consider the following special case where the order of diagnosability is 2.

Theorem 3.13 Let $M' = (\{a\}, Q', \{z\}, \delta', \omega')$ be a single-input, single-output, n -state identity machine, i.e. $\delta'(q, a) = q$ and $\omega'(q, a) = z$ for all $q \in Q'$. There is a homomorphic realization of M' , $M = (I, Q, Z, \delta, \omega)$, such that M is 2-diagnosable and

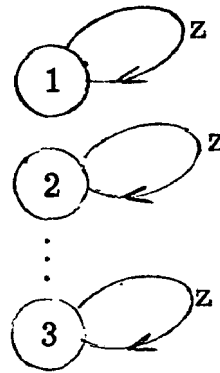
$$|Z| \leq \lfloor \frac{n}{2} \rfloor + 1$$

and

$$|Q| \leq n + \lceil \frac{n}{2} \rceil - 1$$

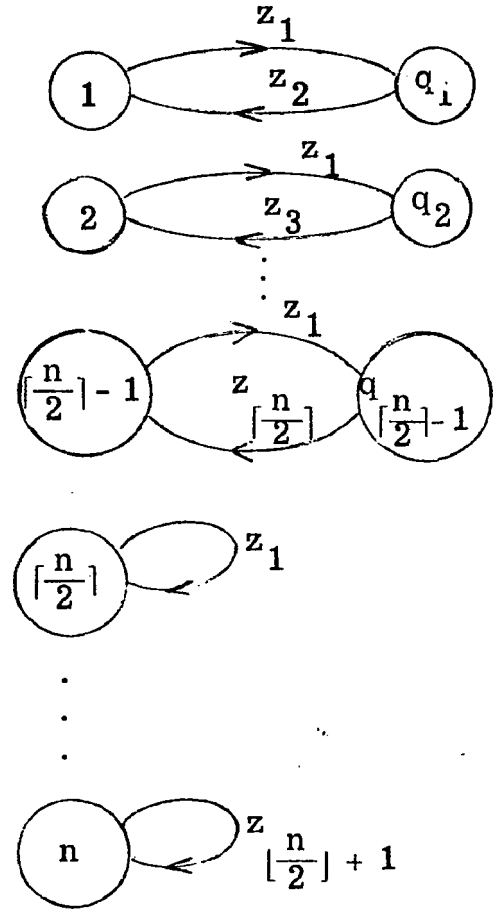
Proof: Let $Q' = \{1, 2, \dots, n\}$ and M' be the machine shown below:

	a
1	1/z
2	2/z
$\vdots$	$\vdots$
n	n/z



Now consider the machine M obtained from M' by increasing the cycle length of states $1, 2, \dots, \lfloor \frac{n}{2} \rfloor - 1$ to 2 and labeling the outputs with $\lfloor \frac{n}{2} \rfloor + 1$ distinct symbols as shown below:

	a
1	q_1/z_1
2	q_2/z_1
$\vdots$	$\vdots$
$\lceil \frac{n}{2} \rceil - 1$	$q_{\lceil \frac{n}{2} \rceil - 1}/z_1$
$\lceil \frac{n}{2} \rceil$	$\lceil \frac{n}{2} \rceil/z_1$
$\lceil \frac{n}{2} \rceil + 1$	$\lceil \frac{n}{2} \rceil + 1/z_2$
$\vdots$	$\vdots$
n	$n/z_{\lceil \frac{n}{2} \rceil + 1}$
q_1	$1/z_2$
q_2	$2/z_3$
$\vdots$	$\vdots$
$q_{\lceil \frac{n}{2} \rceil - 1}$	$\lceil \frac{n}{2} \rceil - 1/z_{\lceil \frac{n}{2} \rceil}$



It is clear that M homomorphically realizes M' under the triple of functions (η_1, η_2, η_3) where

$$\eta_1(x) = x \text{ for } x \in \{a\}^+$$

$$\eta_2(t) = \begin{cases} t & \text{if } t \in \{\lceil \frac{n}{2} \rceil, \lceil \frac{n}{2} \rceil + 1, \dots, n\} \\ i & \text{if } t \in \{i, q_i \mid i=1, 2, \dots, \lceil \frac{n}{2} \rceil - 1\} \end{cases}$$

$$\eta_3(z_i) = z \text{ for } i=1, 2, \dots, \lceil \frac{n}{2} \rceil + 1$$

It can be immediately verified that M has a DS of aa. To show that the bounds are satisfied, let $M = (\{a\}, Q, Z, \delta, \omega)$ then

$$Q = \{1, 2, \dots, n, q_1, q_2, \dots, q_{\lceil \frac{n}{2} \rceil - 1}\}$$

$$Z = \{z_1, z_2, \dots, z_{\lfloor \frac{n}{2} \rfloor + 1}\}$$

and that

$$\lceil \frac{n}{2} \rceil \leq \lfloor \frac{n}{2} \rfloor + 1.$$

Although Theorem 3.13 demonstrates the possibility of reducing the number of output symbols required in the output augmentation by increasing the number of states, it fails to provide a general scheme where a compromise between the number of output symbols and the number of states can be made. To devise such a scheme, we need some results of number theory which give the number of distinct p -ary sequences of period k for any integers p and k . One such result which is useful in our application here is the so called Mobius Inversion Formula [5] which is stated below without proof.

Lemma 3.3 Let p and k be two integers. Then the number of distinct p -ary sequences of period k is given by the function

$$I_k(p) = \frac{1}{k} \sum_{\substack{d \\ d|k}} \mu(d) p^{(k/d)}$$

where $\mu(d)$ is the Mobius function, defined by

$$\mu(d) = \begin{cases} 1 & \text{if } d = 1 \\ (-1)^k & \text{if } d \text{ is the product of } k \text{ distinct primes} \\ 0 & \text{if } d \text{ contains any repeated prime factors} \end{cases}$$

Thus $I_1(p) = p$, $I_2(p) = p(p-1)/2$, $I_3(p) = p(p^2-1)/3$, etc. Some values of the function $I_k(p)$ are compiled in Table 3.4.

Table 3.4 Values of the Function $I_k(p)$

$k \backslash p$	2	3	4	5	6	7
1	2	3	4	5	6	7
2	1	3	6	10	15	21
3	2	8	20	40	105	112
4	3	18	60	150	315	588
5	6	48	204	624	1554	3360
6	9	116	670	2580	7735	12215
7	18	312	2340	11160		
8	30	810	8160	48750		
9	56	2457				
10	99	5880				

Let us return now to the problem of obtaining an acyclic testing graph realization for any given single input identity machine such that for any integer p , the diagnosable realization has at most p output symbols. We will show that this is possible and will derive an upper-bound required on the number of states in the realizing machine.

Theorem 3.14 Let $M' = (\{a\}, Q', Z', \delta', \omega')$ be a single input, n -state identity machine. Then, for any integer p , there is a diagnosable realization $M = (I, Q, Z, \delta, \omega)$ of M' such that M homomorphically realizes M' and

$$1) \quad |Z| = p$$

$$\text{and } 2) \quad |Q| \leq \sum_{k=1}^{m-1} k I_k(p) + m\ell$$

where m is the least integer such that

$$n \leq \sum_{k=1}^m I_k(p)$$

$$\text{and } \ell = n - \sum_{k=1}^{m-1} I_k(p)$$

Proof: Let $Q' = \{1, 2, \dots, n\}$ and $Z' = \{z\}$. Construct $M = (I, Q, Z, \delta, \omega)$ as follows:

- i) Let $I = \{a\}$, $Z = \{z_1, z_2, \dots, z_p\}$ and $Q' \subseteq Q$
- ii) For $i=1, 2, \dots, p$, let

$$\omega(i, a) = z_i \quad \text{and} \quad \delta(i, a) = i$$

$$\text{iii) For } i = \sum_{k=1}^{s-1} I_k(p) + 1, \dots, \sum_{k=1}^s I_k(p)$$

such that $s \leq m-1$, let

$$\delta(i, a) = q_{i, 1}$$

$$\delta(q_{i, 1}, a) = q_{i, 2}$$

$$\vdots$$

$$\delta(q_{i, s-2}, a) = q_{i, s-1}$$

$$\delta(q_{i, s-1}, a) = i$$

and assign z_i 's to the outputs so that

$$\hat{\beta}_i(a^s) \neq \hat{\beta}_j(a^s) \quad \text{for } i \neq j$$

$$\text{and } \sum_{k=1}^{s-1} I_k(p) < j \leq \sum_{k=1}^s I_k(p)$$

This is possible as guaranteed by Lemma 3.3.

$$\text{iv) For } i = \sum_{k=1}^{m-1} I_k(p) + 1, \dots, n$$

$$\delta(i, a) = q_{i, 1}$$

$$\delta(q_{i, 1}, a) = q_{i, 2}$$

$$\vdots$$

$$\delta(q_{i, m-2}, a) = q_{i, m-1}$$

$$\delta(q_{i, m-1}, a) = i$$

and assign z_i 's to the outputs so that

$$\hat{\beta}_i(a^m) \neq \hat{\beta}_j(a^m) \quad \text{for } i \neq j$$

$$\text{and } \sum_{k=1}^{m-1} I_k(p) < j \leq n$$

The machine M so constructed has n p -ary cycles of periods m or less and has a DS a^{2m} . Furthermore, M homomorphically realizes M' under (η_1, η_2, η_3) where

$$\eta_1 \text{ is an identity function on } \{a\}^+$$

$$\eta_2(t) = \begin{cases} t & \text{if } 1 \leq t \leq p \\ i & \text{if } t \in \{i, q_{i,j} \mid j=1, \dots, s\} \end{cases}$$

for $s=2, 3, \dots, m$
and $i=p+1, \dots, n$

$$\eta_3(z_i) = z \text{ for } i=1, 2, \dots, p$$

To calculate the total number of states in M , we note that there are p states of length 1, $I_2(p)$ states of length 2, $\dots$, $I_{m-1}(p)$ states of length $m-1$ and ℓ states of length m . Thus

$$|Q| = \sum_{k=1}^{m-1} k I_k(p) + m\ell$$

The inequality holds for a more general case when $|Z'| > 1$. Therefore

$$|Q| \leq \sum_{k=1}^{m-1} k I_k(p) + m\ell.$$

Perhaps the formality of the proof of Theorem 3.14 may have obscured the simple rule of the design it represents. For a given single-input n -state identity machine, the rule simply elongates some of the cycles of the state diagram so that the new state diagram consists of n p -ary distinct cycles of length at most m where m is calculated from n and p based on the result of Lemma 3.3. A systematic procedure for constructing such realizations can be derived simply from the enumeration of distinct p -ary cycles of length at most m . It is interesting to note from Theorems 3.7 and

3. 14 that it is possible to obtain a minimum-output diagnosable realization (i. e. $p = 2$) by increasing sufficient number of states where the maximum number of states required is given in 2) of Theorem 3. 14.

Some values of this bound for the case of $p = 2$ is compiled in Table

3. 5. Example 3. 5 illustrates an application of Theorem 3. 14.

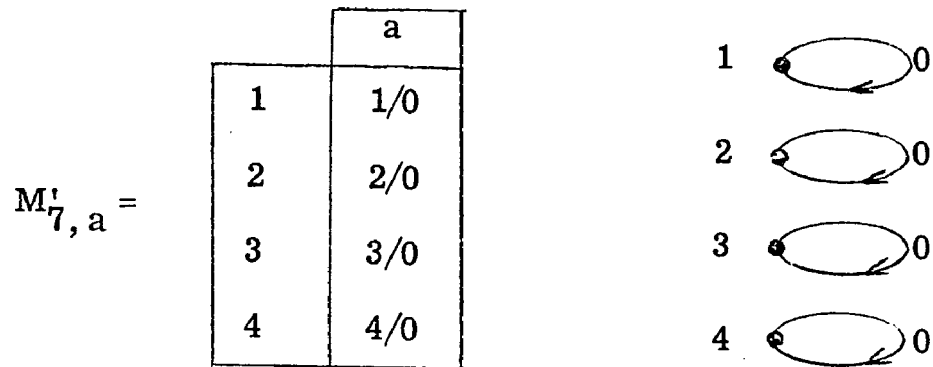
Table 3. 5

n	m	ℓ	$\sum_{k=1}^m I_k(2)$	$ Q $	$ Q - Q' $
3	2	1	3	4	1
4	3	1	5	7	3
5	3	2	5	10	5
6	4	1	8	14	8
7	4	2	8	18	11
8	4	3	8	22	14
9	5	1	14	27	18
10	5	2	14	32	22
11	5	3	14	37	26
12	5	4	14	42	30
13	5	5	14	47	34
14	5	6	14	52	38

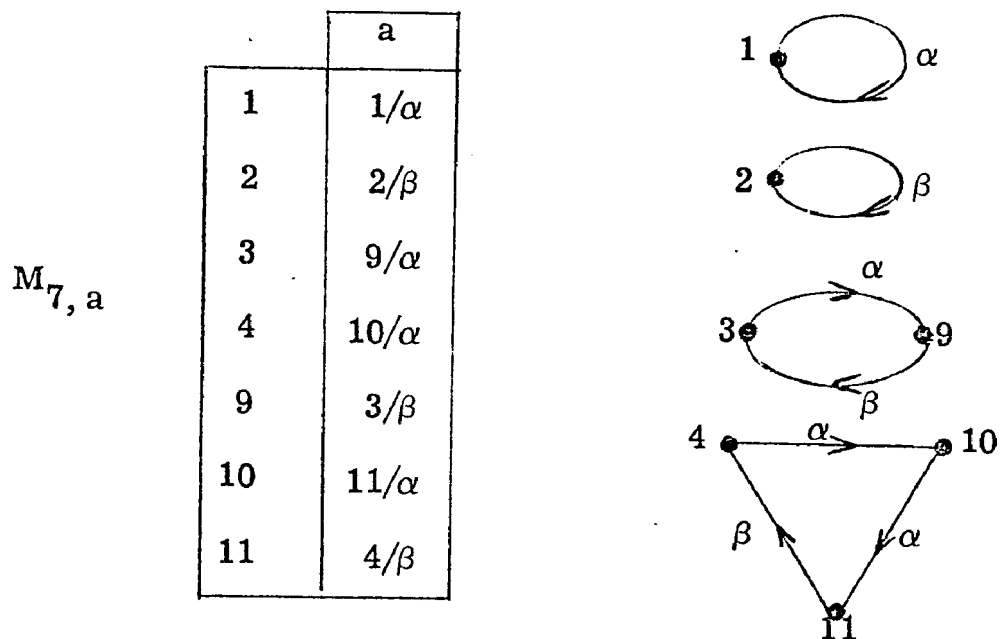
Example 3. 5

Consider an 8-state reduced non-diagnosable machine M_7' as shown in Figure 3. 12(a). Suppose it is desired to obtain a diagnosable realization of M_7' by increasing no more than 1 output symbol. If we

choose to eliminate the 5 states convergence under b using Theorem 3.9, we need to add 3 more states and the realizing machine will be 5-diagnosable. Employing Theorem 3.14, we first choose the 4-state identity submachine of $M'_{7,a}$ under a as shown below



Construct a homomorphically diagnosable realization of $M'_{7,a}$, $M_{7,a}$ whose descriptions are shown below:



If $M_{7,a}$ homomorphically realizes $M'_{7,a}$ under $(\eta'_1, \eta'_2, \eta'_3)$, then

η'_1 is an identity function on $\{a\}^+$

$$\eta'_2(t) = \begin{cases} t & \text{if } t \in \{1, 2\} \\ 3 & \text{if } t \in \{3, 9\} \\ 4 & \text{if } t \in \{4, 10, 11\} \end{cases}$$

$$\eta'_3(\{\alpha, \beta\}) = 0$$

To construct a diagnosable realization M_7 of M'_7 we need to embed $M_{7,a}$ into M_7 in a manner which preserves the homomorphic realization of $M'_{7,a}$ by $M_{7,a}$. One such machine M_7 is shown in Figure 3.12(b) where if M_7 realizes M'_7 under (η_1, η_2, η_3) then

η_1 is an identity function in $I^+ = (I')^+$

$$\eta_2(t) = \begin{cases} t & \text{if } t \in \{1, 2, 5, 6, 7, 8\} \\ 3 & \text{if } t \in \{3, 9\} \\ 4 & \text{if } t \in \{4, 10, 11\} \end{cases}$$

$$\eta_3(\{\alpha, \beta\}) = 0$$

$$\eta_3(\delta) = 1$$

Note that M_7 has a DS of a^4 .

	a	b
1	1/0	2/0
2	2/0	3/1
3	3/0	4/0
4	4/0	5/1
5	6/0	5/1
6	7/0	5/1
7	8/0	5/1
8	5/1	5/1

(a)

	a	b
1	$1/\alpha$	$2/\alpha$
2	$2/\beta$	$3/\delta$
3	$9/\alpha$	$4/\alpha$
4	$10/\alpha$	$5/\delta$
5	$6/\alpha$	$5/\delta$
6	$7/\alpha$	$5/\delta$
7	$8/\alpha$	$5/\delta$
8	$5/\delta$	$5/\delta$
9	$3/\beta$	$4/\alpha$
10	$11/\alpha$	$5/\delta$
11	$4/\beta$	$5/\delta$

(b)

Figure 3.12 Machine M_7^1 and a Diagnosable Realization M_7

Section 3.5 Summary

In this chapter we have developed three types of diagnosable realizations according to how the structure of the original machine is augmented to obtain the realization, that is, by i) input augmentation, ii) output augmentation and iii) state-output augmentation.

We have shown in Section 3.2 that it is possible to obtain a diagnosable realization by augmenting at most one input symbol. Furthermore, for any integers n and p , there is an optimally diagnosable single input machine with n states and p outputs. Thus optimally diagnosable realization of any machine satisfying the above requirements can be obtained by input augmentation of one input symbol. In Section 3.3 output augmentation was studied where tradeoffs between the order of diagnosability (time) and the number of output symbols (space) was investigated. First, the best bounds on the number of output symbols required for obtaining a 1-diagnosable realization of any machine was derived. Several methods of obtaining diagnosable realizations without regards to the length of distinguishing sequence were then proposed. In particular, a graphic method of obtaining a diagnosable realization with repeated symbol distinguishing sequences was described in detail.

Finally, the case of output augmentation was generalized in Section 3.4 where methods have been developed for obtaining diagnosable realizations which reduce the number of augmented output

symbols by increasing the number of states. This problem was divided in separate cases of eliminating state set convergences and cycles in machine's testing graph. Again, tradeoffs between the number of output symbols and the number of states in the realizing machine are considered and it has been shown that in many cases it is possible, with a sufficient increase in the number of states, to add at most one output symbol to obtain a diagnosable realization.

Chapter IV

REGULAR EXPRESSION REPRESENTATION OF FAULT DETECTION SETS

Previous chapters have been mainly concerned with fault detection properties of a sequential machine from a behavior checking viewpoint. In reality, only limited types of faults can occur in a system and detection of these faults is generally sufficient for all practical purposes. In the following chapters we will constrain ourselves to the study of a special class of faults and hopefully be able to derive some design criteria for detection of these faults.

Memory fault concept was first developed by Meyer [34] for the purpose of fault tolerance. The motivation for studying this type of fault comes from the observation that it is the memory that distinguishes a sequential network from a combinational network. While consideration of memory faults alone may be restrictive in appearances, it does underlie the basic difficult natures of faults in sequential machines. It is with this contention that we choose memory fault as the subject of our discussion that follows.

Section 4.1 Introduction

The problem of representing and minimizing test sets for combinational networks has been investigated from various points of view (c.f. [28], [16] and [13]; also the general discussion in [14]). Although the implementation of such procedures may be impractical for large networks, these results are nevertheless valuable in that they delimit the complexity of the problem. Such solutions may also indicate simpler, more practical methods of solving the problem at some sacrifice in optimality or completeness of the test set.

In the investigation that follows, we adopt a similar point of view relative to the problem of representing and minimizing test sets for sequential systems. The class of faults considered is restricted to faults which represent permanent changes in the memory structure of the system. This restriction is made primarily to simplify the discussion and the results obtained can be generalized to include any fault which i) does not increase the number of states and ii) does not affect the reset mechanism.

The problem of representing detection sequences is considered first and it is shown that if D is the set of all sequences that distinguish faulty behavior (for a given fault) from fault-free behavior (in a given initial state), then D is a regular set. Moreover, a regular expression

that denotes D can be obtained from expressions associated with the fault-free and faulty behaviors in much the same way that test sets are determined for combinational networks using Boolean differences [47].

The problem of obtaining a minimum cost test set (with cost measured in terms of testing time) is then considered where the primary difficulty lies in the fact that detection sets, although regular, are nevertheless infinite. However, we show that the cost of an optimum (minimum cost) test set is bounded from above by a quantity which depends only on the size of the fault-free machine and the number of faults to be detected. From this it follows that the length of the longest sequence in any minimum cost test set is also bounded by a known quantity. Thus only a finite subset of each fault detection set needs be considered in deriving an optimum test set. Employing some rather natural notions of fault equivalence and fault dominance, the problem of finding an optimum test set of a sequential machine, given a complete description of the fault set, can then be formulated as a covering problem. This parallels the solution suggested by [28] and others for obtaining optimum test sets for combinational networks.

Section 4.2 Memory Fault Detection

In studying the effects of changes in machine structure (due to faults) on machine behavior, much can be learned by restricting one's attention to faults which occur in the machine's memory. This is evidenced in a recent investigation of fault tolerance [34], and in the study that follows, we adopt a similar point of view with regard to the problem of fault detection. To review the basic notions of a memory fault and the resulting faulty machine [34], let $M = (I, Q, Z, \delta, \omega)$ be a finite state (Mealy) sequential machine with input alphabet I , states Q , output alphabet Z , transition function $\delta: Q \times I \rightarrow Z$.

Definition 4.1 If M is a sequential machine, a (memory) fault of M is a function on the states of M . If $M = (I, Q, Z, \delta, \omega)$ is a sequential machine and $\mu: Q \rightarrow Q$ is a fault of M , the result of μ is the sequential machine

$$M^\mu = (I, Q^\mu, Z, \delta^\mu, \omega^\mu)$$

where

- 1) $Q^\mu = \text{Im}(\mu)$, the image (range) of μ .
- 2) $\delta^\mu = \mu\delta$ restricted to $Q^\mu \times I$, where $\mu\delta$ is the composite of δ and μ , first applying δ .
- 3) $\omega^\mu = \omega$ restricted to $Q^\mu \times I$.

Given some machine M and a fault μ of M , one can then regard μ as "detectable" if the behavior of M^μ can be distinguished in some

way from the behavior of M , i. e. if $B_{M^\mu} \neq B_M$. Assuming that fault detection routines are to rely only on a knowledge of external behavior relative to one or more initial states of the faulty machine, the notion of a "state-detectable" fault can be made precise as follows. If μ is a fault of M then relative to some initial state $q \in Q$ and the corresponding initial state $\mu(q) \in Q^\mu$, μ is detectable if the behavior of M in q differs from the behavior of M^μ in $\mu(q)$. More precisely,

Definition 4.2 If μ is a fault of M and $q \in Q$ then μ is q-detectable in $\beta_q \neq \beta_{\mu(q)}^\mu$.

Implicit in applying this notion of q-detectability, of course, is the ability to "reset" M to state q in a manner such that, for any fault μ of M , M^μ can be reset to $\mu(q)$. However, any input symbol a that resets M to q will have this property for suppose $\delta(r, a) = q$, for all $r \in Q$. Then $\delta^\mu(r', a) = \mu(\delta(r', a)) = \mu(q)$, for all $r' \in Q^\mu$, i. e. a resets M^μ to $\mu(q)$. As the notion of q-detection, per se, does not require the existence of a reset input, we will generally leave such inputs unspecified.

If a fault μ of M is q-detectable then, by definition, there is at least one input sequence $x \in I^+$ that will detect μ in the sense that $\beta_{\mu(q)}^\mu(x) \neq \beta_q(x)$, i. e. the last output symbol distinguishes M^μ from M . We adopt the following notation and terminology for the set of all such sequences, including the case where none exist (i. e., μ is not q-detectable).

Definition 4.3 If μ is a fault of M and $q \in Q$ then the basic q-detection set of μ is the set

$$D(\mu, q) = \{x \in I^+ \mid \beta_{\mu(q)}^\mu(x) \neq \beta_q(x)\}.$$

Obviously, μ is q-detectable if and only if $D(\mu, q) \neq \phi$.

Although $D(\mu, q)$ suffices to characterize the detectability of faults μ relative to initial state q , in most testing applications, one is able to observe the complete output sequence as opposed to the last output symbol. This yields a general set of detection sequences which can be defined as follows.

Definition 4.4 If μ is a fault of M , $q \in Q$, and $x \in I^+$ then x is a (μ, q) -detection sequence if $\hat{\beta}_{\mu(q)}^\mu(x) \neq \hat{\beta}_q(x)$. The q-detection set of μ is the set

$$\hat{D}(\mu, q) = \{x \in I^+ \mid x \text{ is a } (\mu, q)\text{-detection sequence}\}.$$

Since β_q uniquely determines $\hat{\beta}_q$ it should be obvious that $D(\mu, q)$ uniquely determines $\hat{D}(\mu, q)$. The precise nature of the relationship between $D(\mu, q)$ and $\hat{D}(\mu, q)$ is given by the following theorem.

Theorem 4.1 If μ is a fault of M and $q \in Q$ then

$$\hat{D}(\mu, q) = D(\mu, q) I^*$$

where $D(\mu, q) I^*$ is the concatenation of $D(\mu, q)$ and I^* .

Proof: To prove $\hat{D}(\mu, q) \subseteq D(\mu, q) I^*$, let $x \in \hat{D}(\mu, q)$. By Definition 4.4 $\hat{\beta}_{\mu(q)}^{\mu}(x) \neq \hat{\beta}_q(x)$ and by the definition of $\hat{\beta}_q$, there is an initial segment y of x such that $\beta_{\mu(q)}^{\mu}(y) \neq \beta_q(y)$. Thus $y \in D(\mu, q)$ and as $x = yz$, for some $z \in I^*$, $x \in D(\mu, q) I^*$. Conversely, to show $D(\mu, q) I^* \subseteq \hat{D}(\mu, q)$, let $x \in D(\mu, q) I^*$. Then $x = yz$ where $y \in D(\mu, q)$ and $z \in I^*$. Since $y \in D(\mu, q)$, $\beta_{\mu(q)}^{\mu}(y) \neq \beta_q(y)$ which implies $\hat{\beta}_{\mu(q)}^{\mu}(x) \neq \hat{\beta}_q(x)$. Thus $x \in \hat{D}(\mu, q)$, completing the proof.

Let us illustrate these definitions and Theorem 4.1 with an example.

Example 4.1

Consider the 3-state, 2-input and 2-output machine M and faults μ shown in Figure 3.1. The fault μ is 1-detectable for if we let $x = 101$, then

$$\beta_1(x) = 0$$

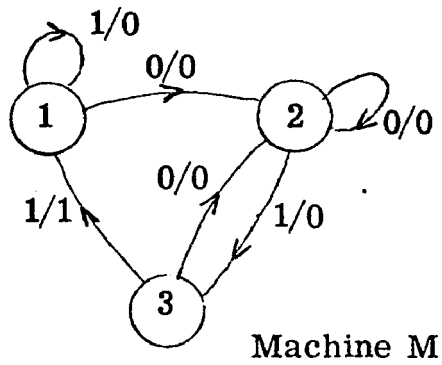
and

$$\beta_{\mu(1)}^{\mu} = 1$$

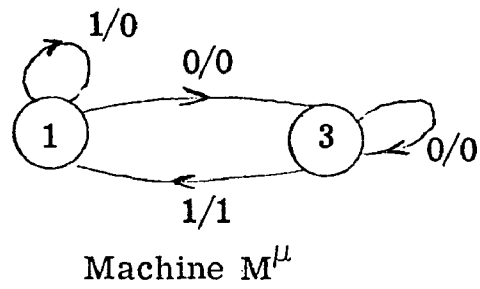
implying that $\beta_1 \neq \beta_{\mu(1)}^{\mu}$. To compute the 1-detection set of μ , $D(\mu, 1)$, let us compare directly the machines M and M^{μ} in which β_1 and $\beta_{\mu(1)}^{\mu}$ differ. We found that for any sequence x ending with 01 or 011 $\beta_1(x) \neq \beta_{\mu(1)}^{\mu}(x)$ and that no other sequence has this property. Thus

$$D(\mu, 1) = \{I^*01, I^*011\}$$

Using Theorem 4.1, we have



q	$\mu(q)$
1	1
2	3
3	3

Fault μ 

q	$\mu'(q)$
1	3
2	2
3	3

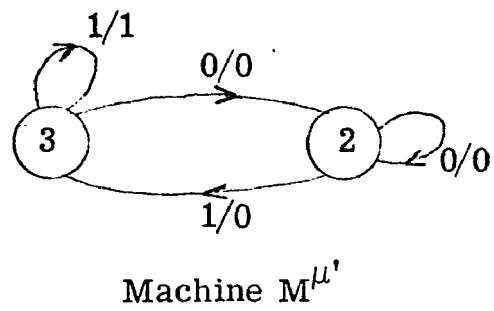
Fault μ' 

Figure 4.1 Example of Memory Faults

$$\hat{D}(\mu, 1) = D(\mu, 1) I^* = \{I^* 01 I^*, I^* 011 I^*\}$$

Since $I^* 011 I^* \subseteq I^* 01 I^*$, it follows that

$$\hat{D}(\mu, 1) = \{I^* 01 I^*\}$$

Thus by Definition 4.4, any input sequence containing 01 is a $(\mu, 1)$ -detection sequence.

As a consequence of Theorem 4.1, the discussion that follows will focus on the basic q -detection set $D(\mu, q)$ where most of what can be said about $D(\mu, q)$ will translate, via Theorem 4.1 to the q -detection set $\hat{D}(\mu, q)$.

Section 4.3 Regular Representation of q-detection Sets

The detection sets $D(\mu, q)$ and $\hat{D}(\mu, q)$ of Definitions 4.3 and 4.4 respectively are infinite set of sequences. Although Example 4.1 suggested that they can be compactly represented, such a result has not been formally established. In this section we will show that these detection sets can indeed be represented by regular expressions [27] and how these expressions can be computed.

A fundamental observation regarding basic q-detection sets is that they are regular and hence representable by regular expressions [11].

Theorem 4.2 If μ is a fault of M and $q \in Q$ then $D(\mu, q)$ is a regular subset of I^+ .

Proof: To prove $D(\mu, q)$ is regular, we prove that $D(\mu, q)$ is the language accepted by an appropriately determined finite state acceptor M' (from which regularity follows by Kleene's theorem). Given some machine $M = (I, Q, Z, \delta, \omega)$, a fault μ of M , and a state $q \in Q$, consider the machine $M' = (I, Q', \{0, 1\}, \delta', \omega')$ where

$$Q' = Q \times Q^\mu$$

$$\delta'((q, r), a) = (\delta(q, a), \delta^\mu(r, a))$$

and

$$\omega'((q, r), a) = \begin{cases} 1 & \text{if } \omega(q, a) \neq \omega^\mu(r, a) \\ 0 & \text{otherwise} \end{cases}$$

Then, using the definition of behavior, one can easily verify that for state $q' = (q, \mu(q))$,

$$\beta'_{q'}(x) = \begin{cases} 1 & \text{if } \beta_{\mu(q)}^\mu(x) \neq \beta_q(x) \\ 0 & \text{otherwise} \end{cases}$$

Thus, by Definition 4.3, $\beta'_{q'}(x) = 1$ if and only if $x \in D(\mu, q)$. Since Q' is finite, M' with initial state q' is a finite state acceptor for $D(\mu, q)$, thereby proving the theorem.

Corollary 4.2.1 $\hat{D}(\mu, q)$ is a regular subset of I^+ .

Proof: Since $D(\mu, q)$ and I^* are regular, by Theorem 4.1 and the fact that a concatenation of regular sets is regular, $\hat{D}(\mu, q)$ is regular.

Having determined that $D(\mu, q)$ is regular, an immediate question is whether a regular expression denoting $D(\mu, q)$ (or more precisely, an extended regular expression where we admit Boolean operations) can be determined directly from expressions relating to the behaviors β_q and $\beta_{\mu(q)}^\mu$. Toward obtaining an affirmative answer to this question, if M is a machine, q and r are states of M , and z is an output symbol, let

$$S_{q, r} = \{x \in I^* \mid \bar{\delta}(q, x) = r\},$$

and

$$T_{q, z} = \{x \in I^+ \mid \beta_q(x) = z\}.$$

To obtain regular expressions that denote the above sets, if A and B are expressions denoting sets A and B , let $A + B$ denote $A \cup B$, $A \cdot B$ denote $A \cap B$, $\bar{A}$ denote $I^* - A$ and AP denote the concatenation of A and B . As is well known, the sets $S_{q,r}$ are regular and expressions denoting them can be solved for by successive application of Arden's lemma (see [2], for example). Moreover, $T_{q,z}$ can be expressed in terms of the $S_{q,r}$ as follows:

$$T_{q,z} = \sum_{\substack{\text{all } r \in Q, a \in I \\ \omega(r,a) = z}} S_{q,r} a \quad (4.1)$$

Suppose now that M is a machine, μ is a fault of M , $q \in Q$ and let

$$\{T_{q,z} \mid z \in Z\}$$

be the set of expressions determined as in (4.1) by M and q . Similarly let

$$\{T_{q,z}^{\mu} \mid z \in Z\}$$

be the set of expressions determined as in (4.1) by M^{μ} and $\mu(q)$, i. e.

$T_{q,z}^{\mu} = T_{\mu(q),z}$. Then

Theorem 4.3 The basic q -detection set of μ is denoted by the regular expression

$$D(\mu, q) = \sum_{z \in Z} T_{q,z} \cdot \bar{T}_{q,z}^{\mu}.$$

Proof: If $x \in D(\mu, q)$ then, for some $z \in Z$, $\beta_q(x) = z$ and accordingly $\beta_{\mu(q)}^\mu(x) \neq z$. Thus $x \in T_{q,z} \cap \bar{T}_{q,z}^\mu$ and it follows that x is in the set denoted by the expression

$$\sum_{z \in Z} T_{q,z} \cdot \bar{T}_{q,z}^\mu.$$

Conversely, if x is in the set denoted by this expression then, for some $z \in Z$, $x \in T_{q,z} \cap \bar{T}_{q,z}^\mu$. By definition of these sets, $\beta_q(x) = z$ and $\beta_{\mu(q)}^\mu(x) \neq z$. Hence $x \in D(\mu, q)$.

Corollary 4.3.1 $\hat{D}(\mu, q) = \left(\sum_{z \in Z} T_{q,z} \cdot \bar{T}_{q,z}^\mu \right) I^*.$

Proof: Immediate from Theorems 4.1 and 4.3.

Let us illustrate these theorems with an example.

Example 4.2

Consider the machine M and fault μ shown in Figure 3.1. We first compute $S_{q,r}$'s as follows:

$$S_{1,1} = \Lambda + S_{1,1}^1 + S_{1,3}^1 \quad (4.2)$$

$$S_{1,2} = S_{1,1}^0 + S_{1,2}^0 + S_{1,3}^0 \quad (4.3)$$

$$S_{1,3} = S_{1,2}^1 \quad (4.4)$$

Now since $S_{1,1} + S_{1,2} + S_{1,3} = I^*$, it follows that Equations (4.3) and (4.4) become

$$S_{1,2} = I^*0 \quad (4.5)$$

$$S_{1,3} = I^*01 \quad (4.6)$$

Substituting (4.6) into (4.2), we have

$$S_{1,1} = \Lambda + S_{1,1} 1 + I^*011$$

Applying Arden's lemma and simplifying, we have

$$\begin{aligned} S_{1,1} &= (\Lambda + I^*011)1^* \\ &= \Lambda + 1 + I^*11 \end{aligned} \quad (4.7)$$

Now, to compute $T_{q,z}$'s, we use Equations (4.1), (4.5), (4.6) and (4.7)

$$\begin{aligned} T_{1,0} &= S_{1,1}I + S_{1,2}I + S_{1,3}0 \\ &= (\Lambda + 1 + I^*11)I + I^*0I + I^*010 \\ &= I + 1I + I^*11I + I^*0I + I^*010 \\ &= (1 + 11) + I^*(0 + 0I + 111) \end{aligned} \quad (4.8)$$

$$\begin{aligned} T_{1,1} &= S_{1,3}1 \\ &= I^*011 \end{aligned} \quad (4.9)$$

To compute $T_{q,z}^\mu$'s, first let

$$S_{q,r}^\mu = \{x \in I^* \mid \bar{\delta}^\mu(\mu(q), x) = r\} \quad (4.10)$$

Then

$$S_{1,1}^\mu = \Lambda + S_{1,1}^\mu 1 + S_{1,3}^\mu 1 \quad (4.11)$$

$$S_{1,3}^\mu = S_{1,1}^\mu 0 + S_{1,3}^\mu 0 \quad (4.12)$$

Again, since $S_{1,1}^\mu + S_{1,3}^\mu = I^*$, (4.11) and (4.12) can be immediately obtained

$$S_{1,1}^\mu = \Lambda + I^*1 \quad (4.13)$$

$$S_{1,3}^\mu = I^*0 \quad (4.14)$$

Using Equation (4.1) to compute $T_{q,z}^\mu$'s, we have

$$\begin{aligned} T_{1,0}^\mu &= S_{1,1}^\mu I + S_{1,3}^\mu 0 \\ &= (\Lambda + I^*1)I + I^*00 \\ &= I + I^*1I + I^*00 \\ &= I + (I^*1 + I^*0)0 + I^*11 \\ &= I + I^*I0 + I^*11 \\ &= 1 + (I^*I + \Lambda)0 + I^*11 \\ &= 1 + I^*0 + I^*11 \\ &= 1 + I^*(0 + 11) \end{aligned} \quad (4.15)$$

$$\begin{aligned} T_{1,1}^\mu &= S_{1,3}^\mu 1 \\ &= I^*01 \end{aligned} \quad (4.16)$$

Now, we can use Theorem 4.3 to calculate $D(\mu, 1)$

$$\begin{aligned}
D(\mu, 1) &= \sum_{z \in Z} T_{q, z} \cdot \bar{T}_{q, z}^{\mu} \\
&= T_{1, 0} \cdot T_{1, 1}^{\mu} + T_{1, 1} \cdot T_{1, 0}^{\mu} \\
&= [(1 + 11) + I^*(0 + 01 + 111)] \cdot [I^*01] \\
&\quad + [I^*011] \cdot [1 + I^*(0 + 11)] \\
&= I^*01 + I^*011 \\
&= I^*(01 + 011) \tag{4.17}
\end{aligned}$$

Employing Theorem 4.1, the q -detection set of fault μ can be immediately obtained

$$\begin{aligned}
\hat{D}(\mu, 1) &= D(\mu, 1) I^* \\
&= I^*(01 + 011) I^* \\
&= I^*01 I^* \tag{4.18}
\end{aligned}$$

In representing the fault detection sets $\hat{D}(\mu, q)$, we are quite often interested in the set of minimal (μ, q) -detection sequences; minimal in the sense that no proper subsequence is a (μ, q) -detection sequence. It may be expected that representation of such a set will be much more simplified because of possible reduction in the amount of information required to describe the detection set. Based on this observation, we define yet another type of fault detection set.

Definition 4.5 If μ is a fault of M and $q \in Q$, then the minimal q -detection set of μ is the set

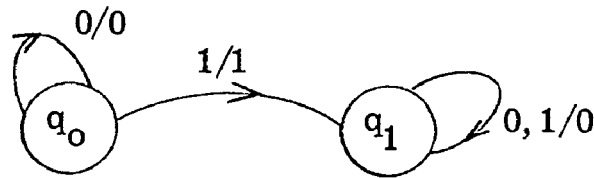
$$\hat{\hat{D}}(\mu, q) = \{ya \in I^+ \mid ya \in D(\mu, q), \text{ yet } y \notin \hat{D}(\mu, q)\}$$

In words, $\hat{\hat{D}}(\mu, q)$ is the set of all (μ, q) -detection sequences such that no proper subsequence in it is a (μ, q) -detection sequence. We show first that $\hat{\hat{D}}(\mu, q)$ is regular.

Theorem 4.4 If μ is a fault of M and $q \in Q$, then $\hat{\hat{D}}(\mu, q)$ is a regular subset of I^+ .

Proof: The proof is somewhat similar to that of Theorem 4.2.

Let M' be the finite state acceptor which accepts $D(\mu, q)$ as constructed in the proof of Theorem 4.2. Consider now the set Flip-Flop (SF) shown below:



If M' is connected in cascade in the front of SF, the composite machine $M'' = (I, Q'', \{0, 1\}, \delta'', \omega')$ is defined as

$$Q'' = Q \times Q^\mu \times \{q_0, q_1\}$$

$$\delta''((q, r, s), a) = (\delta(q, a), \delta^\mu(r, a), \delta^{\text{SF}}(s, \omega'((q, r), a)))$$

and

$$\omega'((q, r, s), a) = \begin{cases} 1 & \text{if } \omega'((q, r), a) = 1 \text{ and } s = q_0 \\ 0 & \text{otherwise} \end{cases}$$

where $q \in Q$, $r \in Q^\mu$, $s \in \{q_0, q_1\}$ and δ^{SF} is the state transition function of SF. Then, using the definition of behavior, one can easily verify that for state $q'' = \{q, \mu(q), q_0\}$ and $x = ya \in I^+$

$$\beta_{q''}^{\mu}(x) = \begin{cases} 1 & \text{if } \beta_{\mu(q)}^{\mu}(x) \neq \beta_q(x) \text{ and } \hat{\beta}_{\mu(q)}^{\mu}(y) = \hat{\beta}_q(y) \\ 0 & \text{otherwise} \end{cases}$$

Thus, by Definition 4.5, $\beta_{q''}^{\mu}(x) = 1$ if and only if $x \in \hat{D}(\mu, q)$. Since Q'' is finite, M'' with initial state q'' is a finite state acceptor for $\hat{D}(\mu, q)$, thereby completing the proof.

That $\hat{D}(\mu, q)$ is the smallest regular set sufficient to determine $\hat{D}(\mu, q)$ is established in the following theorem.

Theorem 4.5 If μ is a fault and $q \in Q$ then

$$\hat{D}(\mu, q) = \hat{\hat{D}}(\mu, q) I^*$$

Furthermore, if $\hat{D}(\mu, q) = DI^*$ for some regular set D , then

$$\hat{\hat{D}}(\mu, q) \subseteq D$$

Proof: To prove $\hat{D}(\mu, q) \subseteq \hat{\hat{D}}(\mu, q) I^*$, let $x \in \hat{D}(\mu, q)$. Then by

Definition 4.4

$$\hat{\beta}_{\mu(q)}^{\mu}(x) \neq \hat{\beta}_q(x)$$

and by the definition of sequence to sequence behavior there is an initial segment y of x such that

$$\beta_{\mu(q)}^{\mu}(y) \neq \beta_q(y).$$

Choose the shortest such y , called y_0 , i.e.

$$\beta_{\mu(q)}^{\mu}(y_0) \neq \beta_q(y_0)$$

and for every proper initial segment w of y_0

$$\hat{\beta}_{\mu(q)}^{\mu}(w) = \hat{\beta}_q(w)$$

Then clearly $y_0 \in \hat{\hat{D}}(\mu, q)$ by Definition 4.5 and as $x = y_0 z$ for some $z \in I^*$, $x \in \hat{\hat{D}}(\mu, q) I^*$. Conversely, to show $\hat{\hat{D}}(\mu, q) I^* \subseteq \hat{\hat{D}}(\mu, q)$, let $x \in \hat{\hat{D}}(\mu, q) I^*$. Then $x = yz$ where $y \in \hat{\hat{D}}(\mu, q)$ and $z \in I^*$. Since $y \in \hat{\hat{D}}(\mu, q)$, by Definition 4.5, $y \in D(\mu, q)$,

$$\beta_{\mu(q)}^{\mu}(y) \neq \beta_q(y)$$

which implies

$$\hat{\beta}_{\mu(q)}^{\mu}(x) \neq \hat{\beta}_q(x)$$

Thus $x \in \hat{\hat{D}}(\mu, q)$. To show that if $\hat{\hat{D}}(\mu, q) = DI^*$ then $\hat{\hat{D}}(\mu, q) \subseteq D$, suppose to the contrary that $\exists x \in \hat{\hat{D}}(\mu, q)$ but $x \notin D$. Since $x \in \hat{\hat{D}}(\mu, q)$

$$\beta_{\mu(q)}^{\mu}(x) \neq \beta_q(x).$$

Now $x \notin D$, it must be the case that either

$$\hat{\beta}_{\mu(q)}^{\mu}(x) = \hat{\beta}_q(x)$$

or that $x = yz$ for some $y \in D$ and $z \in I^*$. The first case is clearly impossible by definition of $\hat{\beta}_q$ and the second case holds if and only if $x = y \in D$ by the minimality of x . Thus $x \in D$, completing the proof.

From Theorems 4.1 and 4.5, it is obvious that $\hat{\hat{D}}(\mu, q) \subseteq D(\mu, q) \subseteq \hat{\hat{D}}(\mu, q)$ where $\hat{\hat{D}}(\mu, q)$ is the smallest characterizing set

which can completely determine the fault detection set $\hat{D}(\mu, q)$. A regular expression for $\hat{D}(\mu, q)$ can usually be obtained from that of $\hat{D}(\mu, q)$ by eliminating redundant terms. The following example illustrates how this can be carried out.

Example 4.3

Consider the machine N and a memory fault f of N shown in Figure 3.2. Using Equation 4.1, we have

$$T_{1,0} = (Ib*ab*a) * (I + Ib*I + Ib*ab*b) \quad (4.19)$$

$$T_{1,1} = (Ib*ab*a) * Ib*ab*a \quad (4.20)$$

$$T_{1,0}^f = I*b \quad (4.21)$$

$$T_{1,1}^f = I*a \quad (4.22)$$

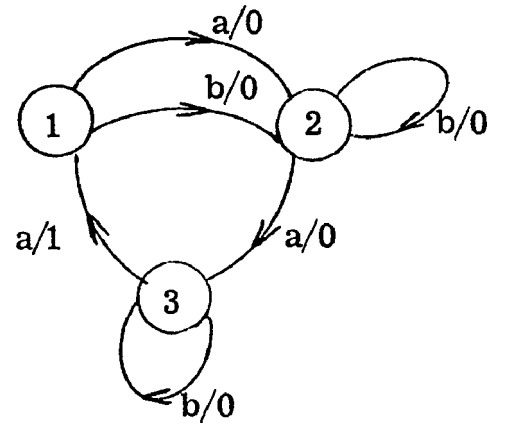
From Theorem 4.3, we can calculate $D(f, 1)$ from $T_{1,z}$'s and $T_{1,z}^f$'s as follows

$$\begin{aligned} D(f, 1) &= \sum_{z \in Z} T_{1,z} \cdot \bar{T}_{1,z}^f \\ &= T_{1,0} \cdot T_{1,1}^f + T_{1,1} \cdot T_{1,0}^f \\ &= (Ib*ab*a) * (I + Ib*I + Ib*ab*b) \cdot I*a \\ &\quad + (Ib*ab*a) * Ib*ab*a \cdot I*b \\ &= (Ib*ab*a) * (a + Ib*a) \end{aligned} \quad (4.23)$$

By employing Theorem 4.1, we obtain the following expression for $\hat{D}(f, 1)$

	a	b
1	2/0	2/0
2	3/0	2/0
3	1/1	3/0

Machine N



q	f(q)
1	3
2	3
3	3

Fault f

	a	b
3	3/1	3/0

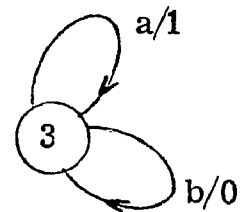
Result of f, M^f 

Figure 4.2 Machine N and Fault f

$$\hat{D}(f, 1) = D(f, 1) I^* = (Ib^*ab^*a)^*(a + Ib^*a) I^* \quad (4.24)$$

Using simplification rules of regular expressions [25] we note that

$(Ib^*ab^*a)^*$ is redundant in Equation (4.24). Thus

$$\hat{D}(f, 1) = (a + Ib^*a) I^* \quad (4.25)$$

Again, we found that ab^*aI^* is redundant and

$$\begin{aligned} \hat{D}(f, 1) &= (a + ab^*a + bb^*a) I^* \\ &= (a + bb^*a) I^* \end{aligned} \quad (4.26)$$

By Definition 4.5 and Theorem 4.5 an expression for $\hat{\hat{D}}(f, 1)$ is

$$\hat{\hat{D}}(f, 1) = a + bb^*a$$

The above example illustrates how a regular expression for $\hat{\hat{D}}(\mu, q)$ can be obtained from that of $\hat{D}(\mu, q)$ and results in a simpler representation than that of $D(\mu, q)$. In most cases we can expect a representation for $\hat{\hat{D}}(\mu, q)$ to be simpler than that of $D(\mu, q)$ but not necessarily the simplest possible. To illustrate this point, let us consider, as another example, $\hat{D}(\mu, 1)$ of Example 4.2

$$\hat{D}(\mu, 1) = I^*01I^* \quad (4.18)$$

yet by eliminating redundant sequences, we have

$$\begin{aligned} D(\mu, 1) &= (I^*- I^*01I^*) 01I^* \\ &= 1^*0^*01I^* \end{aligned} \quad (4.27)$$

Thus

$$\hat{\hat{D}}(\mu, 1) = 1^*0^*01 \quad (4.28)$$

which appears to be more complicated than the expression $D = I * 01$ where $\hat{D}(\mu, 1) = DI^*$. But Equation (4. 28) is considerably simpler than

$$D(\mu, 1) = I*(01 + 011) \quad (4. 23)$$

However, the major advantages of $\hat{D}(\mu, q)$ seems to lie in the amount of computation that may result in computing Boolean operation of detection sets where more than one fault is involved, the subject of discussion in the next section.

Section 4.4 Multiple Fault Test Sets

In devising a fault detection algorithm for a sequential system, a class of many faults is generally involved instead of just a single fault. This generalization to a set of faults is quite straightforward and can be made precise as follows.

Definition 4.6 If F is a set of faults of M , $q \in Q$, and $X \subseteq I^+$, then X is an (F, q) -test set if $\forall \mu \in F, \exists x \in X$ such that x is a (μ, q) -detection sequence. F is q -detectable if there is a non-empty (F, q) -test set.

In other words, X is an (F, q) -test set if, when each sequence in X (preceded by a reset) is applied and no output differences have been observed, it can be asserted that no fault in F has occurred in the system under test. When performing a test on a network, a measure of cost is often taken as the time required to apply a given test set. One such measure is the total length of sequences in the test set plus the number of sequences in the set, under the assumption that a reset need be applied before the application of each sequence. More precisely,

Definition 4.7 If $x \subseteq I^+$ is an (F, q) -test set, then the cost of X is the function

$$\varphi(X) = \sum_{x \in X} \lg(x) + |X|$$

where $\lg(x)$ is the length of x and $|X|$ is the cardinality of the set X .

Note that $\phi(X \cup Y) \leq \phi(X) + \phi(Y)$ and if $X \cap Y = \phi$, then $\phi(X \cup Y) = \phi(X) + \phi(Y)$. In case $X = \{x\}$, we write $\phi(X) = \phi(x) = \lg(x) + 1$. If X is a minimum cost (F, q) -test set, then we can show that the number of sequences in X need not be larger than the number of faults in F .

Theorem 4.6 If X is a minimum cost (F, q) -test set, then $|X| \leq |F|$.

Proof: Suppose to the contrary, i.e. $|X| > |F|$. Since X is an (F, q) -test set, by Definition 4.6, $\forall \mu \in F, \exists x \in X$ such that x is a (μ, q) -detection sequence. For each $\mu \in F$, choose one $x \in X$ such that x is a (μ, q) -detection sequence. The collection of such sequences, X' , is a proper subset of X since $|X'| \leq |F|$ and $|X| > |F|$. But X' , by definition, is an (F, q) -test set. By the linearity of the cost function, $X' \subset X$ implies that $\phi(X') < \phi(X)$, contrary to the assumption that X is of minimum cost. Thus $|X| \leq |F|$, completing the proof.

To derive a bound on the minimum cost of an (F, q) -test set, we first consider the case where $|F| = 1$.

Lemma 4.1 If μ is a q -detectable fault of M , and X is a minimum cost $(\{\mu\}, q)$ -test set then

$$\phi(X) \leq |Q| + |Q^\mu|.$$

Proof: Let M' be the direct sum [40] of machines M and M^μ . Since μ is q -detectable, $\beta'_q \neq \beta'_{\mu(q)}$, i.e. q and $\mu(q)$ are not equivalent in M' .

Recall that in any n -state machine if any two states are not equivalent they are distinguishable by a sequence of length at most $n-1$. Thus there is a sequence $y \in I^+$ such that $\hat{\beta}'_q(y) \neq \hat{\beta}'_{\mu(q)}(y)$ and $\lg(y) \leq |Q| + |Q^\mu| - 1$. But by the construction of direct sum machine, it follows that $\hat{\beta}_q(y) \neq \hat{\beta}_{\mu(q)}^\mu(y)$, i. e. $\{y\}$ is a $(\{\mu\}, q)$ -test set. From Definition 4.7

$$\begin{aligned} \phi(\{y\}) &= \lg(y) + 1 \\ &\leq |Q| + |Q^\mu| - 1 + 1 \\ &= |Q| + |Q^\mu|. \end{aligned}$$

Since X is of minimum cost,

$$\phi(X) \leq \phi(\{y\}) \leq |Q| + |Q^\mu|.$$

The bound given in Lemma 4.1 is best in the sense that, given any positive integer n , there is an n -state machine M and a fault μ of M such that there exists a $(\{\mu\}, q)$ -test set X having $\phi(X) = n + |Q^\mu|$. To show this, let $M = (\{a\}, Q, Z, \delta, \omega)$ be a mod n counter where $Q = \{0, 1, \dots, n-1\}$, $Z = \{0, 1\}$, $\delta(i, a) = i + 1 \pmod{n}$ for $i=0, 1, \dots, n-1$; $\omega(i, a) = 1$ for $i=n-1$ and 0 otherwise. Now consider the fault μ of M such that $\mu(0) = 1$ and $\mu(i) = i$ for $1 \leq i \leq n-1$. Then the shortest sequences which distinguishes state 1 of M and state $\mu(1)$ of M^μ is a^{2n-2} . Note that $|Q| = n$ and $|Q^\mu| = n-1$. Thus

$$\begin{aligned}
 \phi(a^{2n-2}) &= \lg(a^{2n-2}) + 1 \\
 &= 2n - 2 + 1 \\
 &= 2n - 1 \\
 &= |Q| + |Q^\mu|
 \end{aligned}$$

The state diagrams of M and M^μ are shown in Figure 4.3.

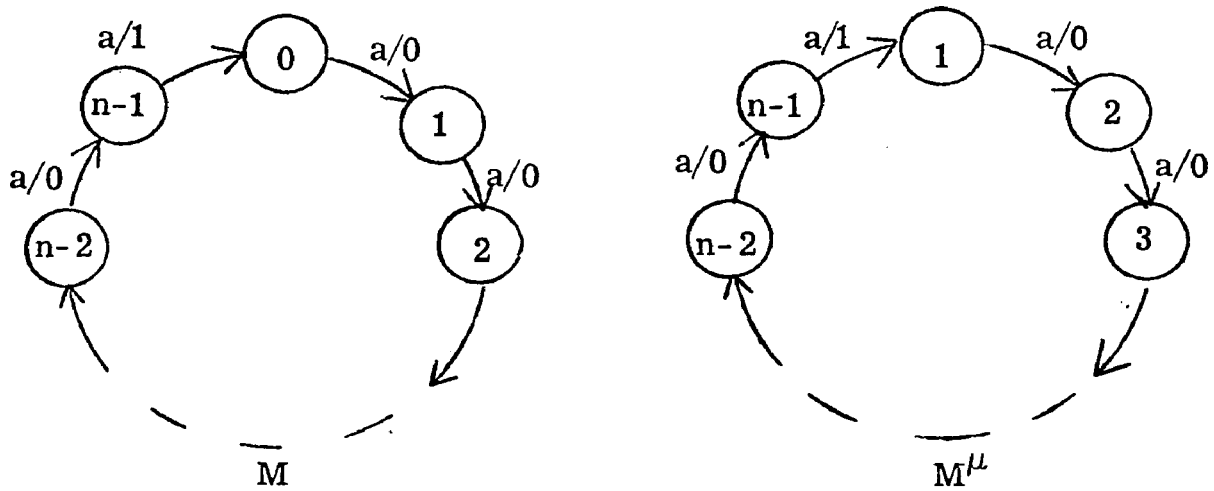


Figure 4.3 Machines M and M^μ

Applying Lemma 4.1 to the more general case of multiple faults, we have:

Theorem 4.7 If F is a set of q -detectable faults of M and X is a minimum cost (F, q) -test set, then

$$\phi(X) \leq |F| |Q| + \sum_{\mu \in F} |Q^\mu| \leq 2 |F| |Q|$$

Proof: To establish this bound, we construct an (F, q) -test set, Y , such that $\phi(Y)$ is no greater than $|F| |Q| + \sum_{\mu \in F} |Q^\mu|$. For each $\mu \in F$, choose an (μ, q) -detection sequence x_μ such that $\phi(x_\mu) \leq |Q| + |Q^\mu|$, which is possible as a consequence of Lemma 4.1. Since $|Q^\mu| \leq |Q|$ and the cost function is linear,

$$\begin{aligned}
 \phi(Y) &= \sum_{x \in Y} \phi(x) \\
 &\leq \sum_{\mu \in F} \phi(x_\mu) \\
 &\leq \sum_{\mu \in F} (|Q| + |Q^\mu|) \\
 &= |F| |Q| + \sum_{\mu \in F} |Q^\mu| \\
 &\leq 2|F| |Q|
 \end{aligned}$$

Since X is of minimum cost

$$\phi(X) \leq \phi(Y) \leq |F| |Q| + \sum_{\mu \in F} |Q^\mu| \leq 2|F| |Q|.$$

In most cases the actual cost of a test set is much smaller than the bound given above. Let us illustrate this observation and the above theorems.

Example 4.4

Consider the faults μ and μ' of machine M shown in Figure 4.1.

From Equation (4.27)

$$\hat{D}(\mu, 1) = 1*0*01 \text{ } I^*$$

Now, let us compute $\hat{D}(\mu', 1)$ using Equation (4.1) and Theorem 4.3

$$S_{1,3}^{\mu'} = \Lambda + I*1 \quad (4.29)$$

$$S_{1,2}^{\mu'} = I*0 \quad (4.30)$$

Thus

$$\begin{aligned} T_{1,0}^{\mu'} &= S_{1,3}^{\mu'} 0 + S_{1,2}^{\mu'} I \\ &= 0 + I*10 + I*0I \end{aligned} \quad (4.31)$$

$$T_{1,1}^{\mu'} = S_{1,3}^{\mu'} 1 = 1 + I*11 \quad (4.32)$$

and

$$\begin{aligned} D(\mu', 1) &= T_{1,0}^{\mu'} \cdot T_{1,1}^{\mu'} + T_{1,1}^{\mu'} \cdot T_{1,0}^{\mu'} \\ &= [(1 + 11) + I*(0 + 01 + 111)] \cdot [1 + I*11] \\ &\quad + [I*011] \cdot [0 + I*10 + I*0I] \\ &= (1 + 11) + I*111 \end{aligned} \quad (4.33)$$

Using Theorem 4.1, we have

$$\begin{aligned} \hat{D}(\mu', 1) &= [1 + 11 + I*111]I^* \\ &= 1I^* \end{aligned} \quad (4.34)$$

and

$$\hat{\hat{D}}(\mu', 1) = 1 \quad (4.35)$$

If we let $F = \{\mu, \mu'\}$, then since

$$\begin{aligned}
& \hat{D}(\mu, 1) \cdot \hat{D}(\mu', 1) \\
&= 1*0*011^* \cdot 11^* \\
&= 11*0*011^*
\end{aligned} \tag{4.36}$$

there is a set of single sequences which are $(F, 1)$ -test sets. The minimum cost $(F, 1)$ -test set is obviously $X = \{101\}$ which has a cost of $\phi(X) = 3 + 1 = 4$. This is much smaller than the bounds given in Theorem 4.6 which are

$$|F| |Q| + \sum_{\mu \in F} |Q^\mu| = 2 \times 3 + 2 + 2 = 10 \tag{4.37}$$

and

$$2|F| |Q| = 2 \times 2 \times 3 = 12 \tag{4.38}$$

respectively.

The bound given in Theorem 4.7 is very large when the number of states is large. However, it is apparent that many of these faults are equivalent in the sense that their corresponding faulty machines are equivalent. For fault detection, it suffices to consider a stronger fault-equivalence relation based on the q -detection sets, i. e. if

$\mu, \gamma \in F$

$$\mu \equiv_q \gamma \iff \hat{D}(\mu, q) = \hat{D}(\gamma, q) \tag{4.39}$$

If we now consider the equivalence classes of this relation i. e. the collection $\mathcal{F} = \{[\mu] \mid \mu \in F\}$, then the following relation is obviously a partial ordering of $\mathcal{F}$:

$$[\mu] \leq [\gamma] \iff \hat{D}(\gamma, q) \subseteq \hat{D}(\mu, q) \quad (4.40)$$

The relation " $\leq$ " can be regarded as a fault "dominance" where if $[\mu] \leq [\gamma]$, detection of any fault in $[\gamma]$ suffices to detect the presence of any fault in $[\mu]$. An element in $\mathcal{F}$ is said to be prime if it is not dominated by any other element in $\mathcal{F}$. Thus the first part of an algorithm to compute an (F, q) -test set would be to construct the partially ordered set $(\mathcal{F}, \leq)$ and then consider only the prime elements of this partially ordered set. We show next, as a corollary of Theorem 4.7, that to compute a minimum cost (F, q) -test set, we need to consider only a finite subset of $\hat{D}(\mu, q)$ for each prime element $[\mu] \in \mathcal{F}$.

Corollary 4.7.1 If F is a set of q -detectable faults of M and X is a minimum cost (F, q) -test set, then $\forall x \in X$,

$$\lg(x) \leq 2|F||Q| - 1.$$

Proof: From Theorem 4.7, we have

$$\phi(X) \leq 2|F||Q|. \quad (4.41)$$

Now if $x \in X$, then

$$\begin{aligned} \phi(X) &= \phi(x) + \sum_{\substack{y \neq x \\ y \in X}} \phi(y) \\ &= \lg(x) + 1 + \sum_{\substack{y \neq x \\ y \in X}} \phi(y) \end{aligned} \quad (4.42)$$

Subtracting $1 + \sum_{\substack{y \neq x \\ y \in X}} \phi(y)$ from both sides of (4.41) and using (4.42),

we have

$$\ell g(x) = \phi(X) - 1 - \sum_{\substack{y \neq x \\ y \in X}} \phi(y) \leq 2|F||Q| - 1. \quad (4.43)$$

Thus if X has minimum cost, the length of the longest sequence in X is bounded by a number which is known prior to the determination of X . Consequently, the problem of computing a minimum cost (F, q) -test set can be formulated as a finite covering problem in a manner similar to that previously accomplished for combinational networks [28]. To do this, let G be a set of representatives of the prime equivalence classes in $\mathcal{F}$ and let

$$W = \{x \in I^+ \mid x \in \bigcup_{\mu \in G} \hat{D}(\mu, q) \text{ and } \ell g(x) \leq 2|F||Q| - 1\}. \quad (4.44)$$

If further, for each $x \in W$, we let

$$H_x = \{\mu \in G \mid x \text{ is a } (\mu, q)\text{-detection sequence}\}, \quad (4.45)$$

then it follows that a cover of G with sets chosen from the class

$$\mathcal{H} = \{H_x \mid x \in W\} \quad (4.46)$$

corresponds to an (F, q) -test set. More precisely, if $\mathcal{C} \subseteq \mathcal{H}$ is a cover of G (i. e. $\bigcup_{H_x \in \mathcal{C}} H_x = G$), then the set

$$X(\mathcal{C}) = \{x \in W \mid H_x \in \mathcal{C}\} \quad (4.47)$$

is an (F, q) -test set. Moreover, if the cost of a cover $\mathcal{C}$ is given by the function

$$\bar{\phi}(\mathcal{C}) = \sum_{x \in X(\mathcal{C})} \phi(x) \quad (4.48)$$

then every minimum cost cover is a minimum cost (F, q) -test set.

As noted in Section 4.1, these results, although established for memory faults, apply in general to any fault which does not increase the number of states and which does not affect the reset mechanism. To formalize this observation, let $\mathcal{M}$ be the class of all finite state sequential machines and $M \in \mathcal{M}$. Let F be a set whose elements are the faults of M , then a sequential machine with faults is a system (M, F, ϕ) , $\phi: F \rightarrow \mathcal{M}$ and if $f \in F$, the machine $\phi(f) = M^f$ is the result of f . A machine with faults can be regarded as a model of an unreliable system where M represents the fault free system, F represents a set of potential system failures that are of concern to the user, and, for a given fault $f \in F$, $\phi(f)$ represents the resulting faulty system. Thus, our results apply in general to any machine with faults (M, F, ϕ) such that for all $f \in F$, $M^f = \phi(f)$ has no more states than M and when M is reset to q , then M^f is reset to q^f (the state of M^f corresponding to q). The first restriction is made primarily for using the bounds derived in Theorem 4.7 and Corollary 4.7.1 and can be relaxed to include fault

which does not increase the number of states more than a predetermined number. The second condition is required for deterministically distinguishing the good behavior and any faulty behavior of the system and can be regarded as a consequence of the assumption that only faults which permanently change the structure of the system are considered in this study.

The question of how one can best implement such a procedure requires further investigation. Nevertheless we feel that the procedure outlined above is indicative of the amount of information and computation required to determine optimum test sets for sequential machines.

Chapter V

RELATIONS OF FAULTS AND EASILY TESTABLE MACHINES

The purpose of this chapter is to explore applications of fault detection sets and their regular representations as derived in the last chapter. The representation of fault detection sets in terms of regular expressions of the faulty machine output behavior and the fault-free machine behavior will be used to determine possible fault equivalence or fault dominance relations among faults. To study easily testable machines, classes of fault detection sets which exhibit some special properties desirable for deriving test sets will be investigated to determine what machine classes might be conducive to such malfunctions. Emphasis is placed upon recognition of these detection sets by their expressions and derivation of sufficient conditions for faults and machines to have these properties by utilizing algebraic manipulation of the regular expressions.

Section 5.1 Introduction

An application of regular expression to the representation and derivation of test set for sequential machines has been previously investigated by Gelenbe [17]. His method mainly concerns the checking of machine behavior relative to a class of diagnosable machines. In this chapter, however, we will focus, instead, on the situation where only a known class of faults is of interest. Our approach here is to utilize some of the results obtained in the last chapter to the study of fault equivalence and fault dominance relations among these faults and to verify some known properties of some easily testable sequential machines.

The problem of determining fault equivalence and fault dominance relations among faults as defined in Equations (4.39) and (4.40) respectively, is first considered. The comparison of these faults is made in terms of componentwise output behavior representations of the faulty machines and the fault-free machine. Sufficient conditions for the existence of these relations have been derived but due to the fact that concatenation of regular expression is not distributive over the Boolean operation of set intersection, we are unable to obtain the corresponding necessary condition. Moreover, if F is a set of faults in a machine and $\mathcal{F}$ is the collection of equivalence classes, we are able to establish a sufficient condition for the existence of the greatest lower bound of any two elements in the partially ordered set $(\mathcal{F}, \leq)$.

These results are useful in that they provide shortcuts for computing test set without exhaustively computing all the fault detection sets in the fault set.

The problem of investigating properties of easily testable sequential machines is then considered. Section 5.3 discusses conditions and characterizations of memory fault detections in terms of machines structures. Moreover, a class of easily detectable faults has been introduced where the fault detection depends only on the length of the test sequences rather than the selection of sequences. A bound on the cost of an optimum test set for such class of faults independent of the size of the fault set has been obtained.

The class of strongly connected machines is then investigated. In this case, we have been able to establish an upperbound on the cost of an optimum test set smaller than that obtainable from Theorem 4.7. If the machine is also diagnosable and the type of faults occurred reduces the number of states in the machine, then it is possible to obtain a test set whose cost is independent of the size of the fault set.

Finally, the class of definite machines is then considered in Section 5.5. Due to the widely known property that definite machines can be realized by networks without feedback loop, it has been conjectured that this class of machines are easier for fault detection. It is the main purpose of this section to attempt formally verifying this conjecture. It has been first established that each output behavior of a definite machine can be represented by regular expression of the form $A + I^*B$

where A and B are finite expressions and I^* is the set of all possible input sequences to the machine. Moreover, it has been shown that if a fault is also definite, then the basic detection set of that fault can also be represented as a definite event. Such type of faults generally has the property that the common intersection of all its faults detection sets is non-empty and a test set so obtained either contains or has a non-empty intersection with any other fault detection set outside this given set of faults. Strongly connectedness has been found to be a sufficient condition for the definite machines to have this property when the fault set is definite. Later we have been able to generalize the class of definite faults to the class of faults which preserves some synchronizability of the fault-free machine and essentially obtain the same type of fault detection sets. Since almost all sequences of a reduced definite machine is a synchronizing sequence, it is reasonable to assume that any malfunction particularly of memory type will preserve some degree of synchronizability. With this assumption and the results obtained, it can be concluded that the class of definite machines is "easier" for fault detection.

Section 5.2 Relations of Faults

We have shown in the last chapter that fault equivalence and fault dominance relations as defined in Equations (4.39) and (4.40), respectively are of great interest in deriving a minimum cost test set for a given set of faults in a machine. For example, if faults f_1 and f_2 have equal fault detection sets, then they can be regarded as the same fault for the purpose of fault detection, thus reducing the number of faults needed to be considered. Similarly if $f_1 \leq f_2$, then detection of f_2 suffices to detect the presence of f_1 and any other faults dominated by f_1 . Study of these relations is also important for the understanding of how machine structure affects the detectability of faults that may occur. In this section, we will investigate how these relations can be characterized in terms of the behavior of a good machine and faulty machines. Moreover, if F is a set of faults in a machine and $\mathcal{F}$ is the collection of equivalence classes of the fault equivalence relation, i.e. $\mathcal{F} = \{[\mu] \mid \mu \in F\}$, we will study how the greatest lower bound (glb) and the least upperbound (lub) of elements in the partially ordered set $(\mathcal{F}, \leq)$ can be determined, if they exist, in terms of the good and faulty machine behaviors.

To simplify the notation to be used in the following development, we will use the same symbol to represent a regular set and its regular expression. This somewhat abuse in terminology is justified in that

we are only interested in the distinction of regular expressions up to equivalence (representing the same set of sequences).

A fundamental question which we would like to ask is whether the basic q -detection sets (for some state q of the machine under consideration) preserve the partial ordering of set inclusion in the q -detection sets, i. e. if $\hat{D}(\mu, q) \subseteq \hat{D}(\gamma, q)$, is $D(\mu, q) \subseteq D(\gamma, q)$?

Surprisingly, the answer is negative. For example, suppose $\hat{D}(\mu, q) = abaI^*$ and $\hat{D}(\gamma, q) = abI^*$ where $D(\mu, q) = aba$ and $D(\gamma, q) = ab$ for $I = \{a, b\}$, then $\hat{D}(\mu, q) \subseteq \hat{D}(\gamma, q)$ but $D(\mu, q) \not\subseteq D(\gamma, q)$. However, the following theorem shows that the converse is true.

Theorem 5.1 If μ, γ are two faults of machine M and q is a state of M , then

$$D(\mu, q) \subseteq D(\gamma, q) \implies \hat{D}(\mu, q) \subseteq \hat{D}(\gamma, q)$$

Proof: Suppose $D(\mu, q) \subseteq D(\gamma, q)$ and let $x \in \hat{D}(\mu, q)$. Then by Theorem 4.1, $\exists y \in I^+$ and $z \in I^* \ni y \in D(\mu, q)$. Then by hypothesis, $y \in D(\gamma, q)$ and again by Theorem 4.1

$$y \in D(\gamma, q) \text{ and } z \in I^* \implies yz \in \hat{D}(\gamma, q)$$

$$\therefore \hat{D}(\mu, q) \subseteq \hat{D}(\gamma, q)$$

Thus $D(\mu, q) \subseteq D(\gamma, q)$ is sufficient but not necessary for the relation $\hat{D}(\mu, q) \subseteq \hat{D}(\gamma, q)$ to hold. Nevertheless, the study on the relations of basic detection sets of faults constitutes a short cut to

determine the relations of faults directly in terms of a good machine and faulty machine behaviors as first demonstrated by the following lemma and theorem.

Lemma 5.1 Let μ, γ be faults of machine $M = (I, Q, Z, \delta, \omega)$ and $q \in Q$, then the following statements are equivalent

- 1) $D(\mu, q) \subseteq D(\gamma, q)$
- 2) $T_{q, z} \cdot \bar{T}_{q, z}^{\mu} \subseteq \bar{T}_{q, z}^{\gamma} \quad \forall z \in Z$
- 3) $\bar{T}_{q, z} \cdot T_{q, z}^{\mu} \subseteq T_{q, z}^{\gamma} \quad \forall z \in Z$

Proof: 1) $\Leftrightarrow$ 2)

Let $D(\mu, q) \subseteq D(\gamma, q)$. From Theorem 4.3

$$D(\mu, q) = \sum_{z \in Z} T_{q, z} \cdot \bar{T}_{q, z}^{\mu} \quad (5.1)$$

and

$$D(\gamma, q) = \sum_{z \in Z} T_{q, z} \cdot \bar{T}_{q, z}^{\gamma} \quad (5.2)$$

Thus

$$\sum_{z \in Z} T_{q, z} \cdot \bar{T}_{q, z}^{\mu} \subseteq \sum_{z \in Z} T_{q, z} \cdot \bar{T}_{q, z}^{\gamma} \quad (5.3)$$

Now, since $T_{q, z} \cdot T_{q, z'} = \phi$ for $z \neq z'$, it follows that

$$T_{q, z} \cdot \bar{T}_{q, z}^{\mu} \subseteq T_{q, z} \cdot \bar{T}_{q, z}^{\gamma} \quad \forall z \in Z \quad (5.4)$$

But $T_{q, z} \cdot \bar{T}_{q, z}^{\gamma} \subseteq \bar{T}_{q, z}^{\gamma}$, Equation (5.4) becomes

$$T_{q,z} \cdot \bar{T}_{q,z}^{\mu} \subseteq \bar{T}_{q,z}^{\gamma} \quad \forall z \in Z \quad (5.5)$$

Conversely if Equation (5.5) holds, then intersecting both sides of Equation (5.5) with $T_{q,z}$ we have Equation (5.4), i.e.

$$T_{q,z} \cdot \bar{T}_{q,z}^{\mu} \subseteq T_{q,z} \cdot \bar{T}_{q,z}^{\gamma} \quad \forall z$$

Thus

$$\sum_{z \in Z} T_{q,z} \cdot \bar{T}_{q,z}^{\mu} \subseteq \sum_{z \in Z} T_{q,z} \cdot \bar{T}_{q,z}^{\gamma}$$

and by Theorem 4.3 we have

$$D(\mu, q) \subseteq D(\gamma, q)$$

$$1) \iff 3)$$

To show this equivalence relation it suffices to show that

$$D(\mu, q) = \sum_{z \in Z} \bar{T}_{q,z} \cdot T_{q,z}^{\mu} \quad (5.6)$$

Equation (5.6) can be proved almost exactly as the proof of Theorem 4.3. However we will show it in a different way to demonstrate that it can be obtained from direct manipulation of regular expressions.

From Theorem 4.3 and the fact that Boolean operations on regular expressions are distributive and associative, we have

$$\begin{aligned}
D(\mu, q) &= \sum_{z \in Z} T_{q, z} \cdot \bar{T}_{q, z}^{\mu} \\
&= \sum_{z \in Z} T_{q, z} \cdot \left(\sum_{z' \neq z} T_{q, z'}^{\mu} \right) \\
&= \sum_{z \in Z} \sum_{z' \neq z} T_{q, z} \cdot T_{q, z'}^{\mu} \\
&= \sum_{z' \in Z} \left(\sum_{z \neq z'} T_{q, z} \right) \cdot T_{q, z'}^{\mu} \\
&= \sum_{z' \in Z} \bar{T}_{q, z'} \cdot T_{q, z'}^{\mu} \tag{5.7}
\end{aligned}$$

It should be noted that the last term of Equation (5.7) is identical to the right hand side of Equation (5.6). Thus using Equation (5.7) and the method used in the part of proving 1) $\Leftrightarrow$ 2), it can be shown that 1) $\Leftrightarrow$ 3).

A sufficient condition for fault dominance can now be stated precisely as follows:

Theorem 5.2 If μ, γ are faults of machine M and q is a state of M , then

$$\text{or } \left. \begin{aligned} T_{q, z} \cdot \bar{T}_{q, z}^{\mu} &\subseteq \bar{T}_{q, z}^{\gamma} & \forall z \\ \bar{T}_{q, z} \cdot T_{q, z}^{\mu} &\subseteq T_{q, z}^{\gamma} & \forall z \end{aligned} \right\} \Rightarrow \gamma \leq \mu$$

Proof: By Lemma 5.1, 1) and 2) and Theorem 5.1

$$\begin{aligned}
T_{q,z} \cdot \bar{T}_{q,z}^{\mu} &\subseteq \bar{T}_{q,z}^{\gamma} \quad \forall z \iff D(\mu, q) \subseteq D(\gamma, q) \\
&\implies \hat{D}(\mu, q) \subseteq \hat{D}(\gamma, q) \\
&\iff \gamma \leq \mu
\end{aligned}$$

Similarly, by 1) and 3) of Lemma 5.1

$$\bar{T}_{q,z} \cdot T_{q,z}^{\mu} \subseteq T_{q,z}^{\gamma} \implies \gamma \leq \mu$$

Theorem 5.2 gives a sufficient condition for determining the fault dominance relations between any two faults in terms of the componentwise regular expression of the good machine and faulty machine behaviors. Extending this investigation further to the structure of the partially ordered set $(\mathcal{F}, \leq)$, let us consider first the case where three faults are involved. Our objective is to determine whether a third fault is dominated by the first two faults.

Lemma 5.2 If μ, γ, ξ are faults of machine $M = (I, Q, Z, \delta, \omega)$ and $q \in Q$, then the following statements are equivalent

- 1) $D(\xi, q) \subseteq D(\mu, q) \cdot D(\gamma, q)$
- 2) $T_{q,z} \cdot \bar{T}_{q,z}^{\xi} \subseteq \bar{T}_{q,z}^{\mu} \cdot \bar{T}_{q,z}^{\gamma} \quad \forall z \in Z$
- 3) $\bar{T}_{q,z} \cdot T_{q,z}^{\xi} \subseteq T_{q,z}^{\mu} \cdot T_{q,z}^{\gamma} \quad \forall z \in Z$

Proof: 1) $\iff$ 2)

From Theorem 4.3

$$D(\xi, q) = \sum_{z \in Z} T_{q, z} \cdot \bar{T}_{q, z}^{\xi}$$

and

$$\begin{aligned} D(\mu, q) \cdot D(\gamma, q) &= \left(\sum_{z \in Z} T_{q, z} \cdot \bar{T}_{q, z}^{\mu} \right) \cdot \left(\sum_{z' \in Z} T_{q, z'} \cdot \bar{T}_{q, z'}^{\gamma} \right) \\ &= \sum_{z \in Z} \sum_{z' \in Z} T_{q, z} \cdot \bar{T}_{q, z}^{\mu} \cdot T_{q, z'} \cdot \bar{T}_{q, z'}^{\gamma} \end{aligned} \quad (5.8)$$

Now since $T_{q, z} \cdot T_{q, z'} = \phi$ for $z \neq z'$, it follows that Equation (5.8) becomes

$$D(\mu, q) \cdot D(\gamma, q) = \sum_{z \in Z} T_{q, z} \cdot \bar{T}_{q, z}^{\mu} \cdot \bar{T}_{q, z}^{\gamma} \quad (5.9)$$

Therefore

$$\begin{aligned} D(\xi, q) &\subseteq D(\mu, q) \cdot D(\gamma, q) \iff \\ \sum_{z \in Z} T_{q, z} \cdot \bar{T}_{q, z}^{\xi} &\subseteq \sum_{z \in Z} T_{q, z} \cdot \bar{T}_{q, z}^{\mu} \cdot \bar{T}_{q, z}^{\gamma} \end{aligned} \quad (5.10)$$

Again by the exclusiveness of each $T_{q, z}$, Equation (5.10) implies that

$$\begin{aligned} D(\xi, q) &\subseteq D(\mu, q) \cdot D(\gamma, q) \iff \\ T_{q, z} \cdot \bar{T}_{q, z}^{\xi} &\subseteq T_{q, z} \cdot \bar{T}_{q, z}^{\mu} \cdot \bar{T}_{q, z}^{\gamma} \subseteq \bar{T}_{q, z}^{\mu} \cdot \bar{T}_{q, z}^{\gamma} \quad \forall z \end{aligned} \quad (5.11)$$

The proof of $1) \iff 3)$ is similar to the preceding proof except for the regular expression of $D(\mu, q)$, we use Equation (5.6), i.e.

$$D(\mu, q) = \sum_{z \in Z} \bar{T}_{q, z} \cdot T_{q, z}^{\mu}$$

Theorem 5.3 If μ, γ, ξ are faults of machine $M = (I, Q, Z, \delta, \omega)$

and $q \in Q$, then

$$\text{or } \left. \begin{array}{l} T_{q,z} \cdot \bar{T}_{q,z}^{\xi} \subseteq \bar{T}_{q,z}^{\mu} \cdot \bar{T}_{q,z}^{\gamma} \quad \forall z \in Z \\ T_{q,z} \cdot T_{q,z}^{\xi} \subseteq T_{q,z}^{\mu} \cdot T_{q,z}^{\gamma} \quad \forall z \in Z \end{array} \right\} \Rightarrow \begin{array}{l} \mu \leq \xi \\ \text{and} \\ \gamma \leq \xi \end{array}$$

Proof: By Lemma 5.2, the hypothesis is equivalent to the condition that

$$D(\xi, q) \subseteq D(\mu, q) \cdot D(\gamma, q)$$

But by Theorem 5.1

$$\begin{aligned} D(\xi, q) &\subseteq D(\mu, q) \cdot D(\gamma, q) \\ \Rightarrow D(\xi, q) I^* &\subseteq (D(\mu, q) \cdot D(\gamma, q)) I^* \\ &\subseteq D(\mu, q) I^* \cdot D(\gamma, q) I^* \\ &= \hat{D}(\mu, q) \cdot \hat{D}(\gamma, q) \end{aligned} \tag{5.12}$$

i. e.

$$\hat{D}(\xi, q) \subseteq \hat{D}(\mu, q) \cdot \hat{D}(\gamma, q) \tag{5.13}$$

From Equation (4.40), Equation (5.13) is equivalent to

$$\mu \leq \xi \text{ and } \gamma \leq \xi$$

If we denote glb and lub as $\wedge$ and $\vee$, respectively, and recall the following relationships

$$\begin{aligned}
\text{glb}(\mu, \gamma) = \mu \wedge \gamma &\iff \text{lub}(\hat{D}(\mu, q), \hat{D}(\gamma, q)) \\
&= \hat{D}(\mu, q) \vee \hat{D}(\gamma, q)
\end{aligned} \tag{5.14}$$

and

$$\begin{aligned}
\text{lub}(\mu, \gamma) = \mu \vee \gamma &\iff \text{glb}(\hat{D}(\mu, q), \hat{D}(\gamma, q)) \\
&= \hat{D}(\mu, q) \wedge \hat{D}(\gamma, q)
\end{aligned} \tag{5.15}$$

then the purpose of Theorem 5.3 is an attempt to derive a sufficient condition for the lub of μ and γ . For example if $\mu \leq \xi$ and $\gamma \leq \xi$, then it is obvious that

$$\mu \vee \gamma \leq \xi \tag{5.16}$$

In case the lub of μ and γ does not exist, the most we can say after the componentwise regular expression tests have been successful is that $\mu \leq \xi$ and $\gamma \leq \xi$. Note that the converse of Theorem 5.3 is not true. This is due to the fact that although each $T_{q,z}$ is exclusive, each $T_{q,z}^{I*}$ need not be exclusive, i. e. $T_{q,z} \cdot T_{q,z'} = \phi$ for $z \neq z'$ yet it may be the case that

$$T_{q,z}^{I*} \cdot T_{q,z'}^{I*} \neq \phi \quad \text{for } z \neq z'$$

In line with the development of Lemma 5.2 and Theorem 5.3, it is not difficult to understand the following development of their dual results.

Lemma 5.3 If μ, γ, ξ are faults of machine $M = (I, Q, Z, \delta, \omega)$

and $q \in Q$, then the following are equivalent

- 1) $D(\mu, q) + D(\gamma, q) \subseteq D(\xi, q)$
- 2) $T_{q, z} \cdot (\bar{T}_{q, z}^{\mu} + \bar{T}_{q, z}^{\gamma}) \subseteq \bar{T}_{q, z}^{\xi} \quad \forall z \in Z$
- 3) $\bar{T}_{q, z} \cdot (T_{q, z}^{\mu} + T_{q, z}^{\gamma}) \subseteq T_{q, z}^{\xi} \quad \forall z \in Z$

Proof: 1) $\Leftrightarrow$ 2)

Using Theorem 4.3 again, we have

$$\begin{aligned} D(\mu, q) + D(\gamma, q) &= \sum_{z \in Z} T_{q, z} \cdot \bar{T}_{q, z}^{\mu} + \sum_{z \in Z} T_{q, z} \cdot \bar{T}_{q, z}^{\gamma} \\ &= \sum_{z \in Z} T_{q, z} \cdot (\bar{T}_{q, z}^{\mu} + \bar{T}_{q, z}^{\gamma}) \end{aligned} \quad (5.17)$$

Therefore

$$\sum_{z \in Z} T_{q, z} \cdot (\bar{T}_{q, z}^{\mu} + \bar{T}_{q, z}^{\gamma}) \subseteq \sum_{z \in Z} T_{q, z} \cdot \bar{T}_{q, z}^{\xi}$$

Again by the exclusiveness of $T_{q, z}$ it follows that

$$D(\mu, q) + D(\gamma, q) \subseteq D(\xi, q)$$

$\Leftrightarrow$

$$\begin{aligned} T_{q, z} \cdot (\bar{T}_{q, z}^{\mu} + \bar{T}_{q, z}^{\gamma}) &\subseteq T_{q, z} \cdot \bar{T}_{q, z}^{\xi} \subseteq \bar{T}_{q, z}^{\xi} \\ \forall z \in Z \end{aligned} \quad (5.18)$$

1) $\Leftrightarrow$ 3) can be similarly proved by using Equation (5.6).

Theorem 5.4 If μ, γ, ξ are faults of machine $M = (I, Q, Z, \delta, \omega)$

and $q \in Q$, then

$$\text{or } \left. \begin{array}{l} T_{q,z} \cdot (\bar{T}_{q,z}^{\mu} + \bar{T}_{q,z}^{\gamma}) \subseteq \bar{T}_{q,z}^{\xi} \quad \forall z \in Z \\ \bar{T}_{q,z} \cdot (T_{q,z}^{\mu} + T_{q,z}^{\gamma}) \subseteq T_{q,z}^{\xi} \quad \forall z \in Z \end{array} \right\} \Rightarrow \begin{array}{l} \xi \leq \mu \\ \text{and} \\ \xi \leq \gamma \end{array}$$

Proof: From Lemma 5.3, the hypothesis implies that

$$D(\mu, q) + D(\gamma, q) \subseteq D(\xi, q)$$

$\Rightarrow$

$$D(\mu, q) I^* + D(\gamma, q) I^* \subseteq D(\xi, q) I^*$$

$$\Leftrightarrow \hat{D}(\mu, q) + \hat{D}(\gamma, q) \subseteq \hat{D}(\xi, q) \quad (5.19)$$

Interpreting Equation (5.19), it is obvious that $\xi \leq \mu$ and $\xi \leq \gamma$.

Again, the converse of Theorem 5.4 is false i. e. it may be the case that $\xi \leq \mu$ and $\xi \leq \gamma$ but $\exists z \in Z$ such that

$$T_{q,z} \cdot (\bar{T}_{q,z}^{\mu} + \bar{T}_{q,z}^{\gamma}) \not\subseteq \bar{T}_{q,z}^{\xi}.$$

Let us illustrate these developments with an example.

Example 5.1

Consider the machine M with state table and $T_{q,z}$ shown below

M =

	a
1	2/0
2	3/1
3	4/0
4	1/0

(5.20)

$$T_{1,0} = (a^4) * (a + a^3 + a^4) \quad (5.21)$$

$$T_{1,1} = (a^4) * a^2 \quad (5.22)$$

The memory faults μ_1 and μ_2 , specified by the following table

μ_i q	$\mu_1(q)$	$\mu_2(q)$
1	2	2
2	3	3
3	3	1
4	3	3

(5.23)

are equivalent, i.e. $\mu_1 \equiv \mu_2$ since

$$T_{1,0}^{\mu_1} = a^2 I^* \quad (5.24)$$

$$T_{1,1}^{\mu_1} = a \quad (5.25)$$

$$T_{1,0}^{\mu_2} = a^2 + a^3 I^* \quad (5.26)$$

$$T_{1,1}^{\mu_2} = a \quad (5.27)$$

$$T_{1,1}^{\mu_1} = a = T_{1,1}^{\mu_2} \quad (5.28)$$

and

$$T_{1,0}^{\mu_2} = a^2 + a^3 I^* = a^2 I^* = T_{1,0}^{\mu_1} \quad (5.29)$$

Thus

$$\hat{D}(\mu_1, 1) = \hat{D}(\mu_2, 1) \quad (5.30)$$

and

$$\mu_1 \equiv \mu_2 \quad (5.31)$$

Now by Theorem 4.3

$$\begin{aligned} D(\mu_1, 1) &= D(\mu_2, 1) \\ &= T_{1,0} \cdot T_{1,1}^{\mu_1} + T_{1,1} \cdot T_{1,0}^{\mu_1} \\ &= (a^4) * (a + a^3 + a^4) \cdot a + (a^4) * a^2 \cdot a^2 I^* \\ &= a + a^2(a^4) * \end{aligned} \quad (5.32)$$

Thus

$$\hat{D}(\mu_1, 1) = \hat{D}(\mu_2, 1) = (a + a^2(a^4) *) I^* = aI^* \quad (5.33)$$

To illustrate the fault dominance relation condition specified in Theorem 5.2, let us consider the memory faults μ_3 and μ_4 specified by the following table

$\begin{matrix} \mu_i \\ q \end{matrix}$	$\mu_3(q)$	$\mu_4(q)$
1	2	1
2	2	2
3	1	3
4	1	3

(5.34)

$$T_{1,0}^{\mu_3} = (a^2) * a^2 \quad (5.35)$$

$$T_{1,1}^{\mu_3} = (a^2) * a \quad (5.36)$$

$$T_{1,0}^{\mu_4} = a + a^3 I^* \quad (5.37)$$

$$T_{1,1}^{\mu_4} = a^2 \quad (5.38)$$

Now

$$\begin{aligned} T_{1,0} \cdot \bar{T}_{1,0}^{\mu_4} &= (a^4) * (a + a^3 + a^4) \cdot a^2 \\ &= \phi \subseteq T_{1,1}^{\mu_3} = \bar{T}_{1,0}^{\mu_3} \end{aligned} \quad (5.39)$$

and

$$\begin{aligned} T_{1,1} \cdot \bar{T}_{1,1}^{\mu_4} &= (a^4) * a^2 \cdot (a + a^3 I^*) \\ &= a^6 (a^4) * \subseteq (a^2) * a^2 \\ &= \bar{T}_{1,1}^{\mu_3} \end{aligned} \quad (5.40)$$

Thus a condition of Theorem 5.2 is satisfied and it follows that

$$\hat{D}(\mu_4, 1) \subseteq \hat{D}(\mu_3, 1) \quad (5.41)$$

and

$$\mu_3 \leq \mu_4 \quad (5.42)$$

To illustrate Theorem 5.3, consider another two memory faults μ_5 and μ_6 specified below

$q \backslash \mu_i$	$\mu_5(q)$	$\mu_6(q)$
1	1	1
2	3	1
3	4	1
4	2	1

(5.43)

$$T_{1,0}^{\mu_5} = (a^4) * (a + a^2 + a^4) \quad (5.44)$$

$$T_{1,1}^{\mu_5} = (a^4) * a^3 \quad (5.45)$$

$$T_{1,0}^{\mu_6} = I^* \quad (5.46)$$

$$T_{1,1}^{\mu_6} = \phi \quad (5.47)$$

$$T_{1,0} \cdot T_{1,1}^{\mu_6} = \phi \quad (5.48)$$

$$T_{1,1} \cdot T_{1,0}^{\mu_6} = (a^4) * a^2 \cdot I^* = (a^4) * a^2 \quad (5.49)$$

$$T_{1,1}^{\mu_5} \cdot T_{1,1}^{\mu_1} = (a^4) * a^3 \cdot a = \phi \quad (5.50)$$

$$\begin{aligned} T_{1,0}^{\mu_5} \cdot T_{1,0}^{\mu_1} &= (a^4) * (a + a^2 + a^4) \cdot a^2 I^* \\ &= (a^4) * a^2 \end{aligned} \quad (5.51)$$

Thus

$$T_{1,0} \cdot \bar{T}_{1,0}^{\mu_6} \subseteq \bar{T}_{1,0}^{\mu_5} \cdot \bar{T}_{1,0}^{\mu_1} \quad (5.52)$$

and

$$T_{1,1} \cdot \bar{T}_{1,1}^{\mu_6} \subseteq \bar{T}_{1,1}^{\mu_5} \cdot \bar{T}_{1,1}^{\mu_1} \quad (5.53)$$

Thus the condition of Theorem 5.3 is satisfied and it follows that

$$\hat{D}(\mu_6, 1) \subseteq \hat{D}(\mu_1, 1) \cdot \hat{D}(\mu_5, 1) \quad (5.54)$$

and

$$\mu_1 \leq \mu_6 \quad \text{and} \quad \mu_5 \leq \mu_6$$

To illustrate Theorem 5.4, let us consider the memory faults μ_1, μ_3 and μ_5 as shown in Tables (5.23), (5.34) and (5.43) respectively. From Equations (5.21), (5.45), (5.25) and (5.36) we have

$$\begin{aligned} & T_{1,0} \cdot (\bar{T}_{1,0}^{\mu_5} + \bar{T}_{1,0}^{\mu_1}) \\ &= (a^4) * (a + a^3 + a^4) \cdot [(a^4) * a^3 + a] \\ &= a + (a^4) * a^3 \\ &\subseteq (a^2) * a = \bar{T}_{1,0}^{\mu_3} \end{aligned} \quad (5.55)$$

Similarly from Equations (5.22), (5.44), (5.24) and (5.35), we obtain

$$\begin{aligned} & T_{1,1} \cdot (\bar{T}_{1,1}^{\mu_5} + \bar{T}_{1,1}^{\mu_1}) \\ &= (a^4) * a^2 \cdot [(a^4) * (a + a^2 + a^4) + a^3 I^*] \\ &= (a^4) * a^2 \\ &\subseteq (a^2) * a^2 = \bar{T}_{1,1}^{\mu_3} \end{aligned} \quad (5.56)$$

Thus Theorem 5.4 is satisfied and we have

$$\hat{D}(\mu_5, 1) + \hat{D}(\mu_1, 1) \subseteq \hat{D}(\mu_3, 1) \quad (5.57)$$

and

$$\mu_3 \leq \mu_5 \quad \text{and} \quad \mu_3 \leq \mu_1$$

As noted earlier, the motivation for developing Theorems 5.3 and 5.4 is an attempt to provide a way of determining lub and glb of two faults if they exist. It is obvious that

$$\xi = \mu \vee \gamma \implies \hat{D}(\xi, q) \subseteq \hat{D}(\mu, q) \cdot \hat{D}(\gamma, q) \quad (5.58)$$

and

$$\xi' = \mu \wedge \gamma \implies \hat{D}(\mu, q) + \hat{D}(\gamma, \xi) \subseteq \hat{D}(\xi', q) \quad (5.59)$$

Thus Theorems 5.3 and 5.4 provide a method of determining whether a necessary condition for the existence of the lub and glb of any two faults has been satisfied. Due to the fact that concatenation of regular expressions is not distributive over the Boolean intersection, we have not been able to derive a sufficient condition for the existence of lub of any two faults in terms of componentwise regular expressions. However, it is possible to derive a sufficient condition for the case of glb as shown in the following theorem.

Theorem 5.5 If μ, γ , and ξ are faults of machine $M = (I, Q, Z, \delta, \omega)$, and $q \in Q$, then

$$T_{q,z} \cdot (\bar{T}_{q,z}^{\mu} + \bar{T}_{q,z}^{\gamma}) = T_{q,z} \cdot \bar{T}_{q,z}^{\xi} \quad \forall z \in Z$$

$$\Rightarrow \xi = \mu \wedge \gamma$$

Proof: From Theorem 4.3, it is immediate that

$$D(\xi, q) = D(\mu, q) + D(\gamma, q) \quad (5.60)$$

Now since concatenation of regular expressions is distributive over the Boolean operation of set union, it follows that

$$\begin{aligned} D(\xi, q) I^* &= [D(\mu, q) + D(\gamma, q)] I^* \\ &= D(\mu, q) I^* + D(\gamma, q) I^* \end{aligned} \quad (5.61)$$

Thus

$$\hat{D}(\xi, q) = \hat{D}(\mu, q) + \hat{D}(\xi', q) \quad (5.62)$$

Now if $\hat{D}(\xi', q)$ is an upperbound of $\hat{D}(\mu, q) + \hat{D}(\gamma, q)$, then

$$\hat{D}(\mu, q) + \hat{D}(\gamma, q) \subseteq \hat{D}(\xi', q) \quad (5.63)$$

i. e.

$$\hat{D}(\xi, q) \subseteq D(\xi', q) \quad (5.64)$$

Thus

$$\begin{aligned} \hat{D}(\xi, q) &= \text{lub}(\hat{D}(\mu, q), \hat{D}(\gamma, q)) \\ &= \hat{D}(\mu, q) \vee \hat{D}(\gamma, q) \end{aligned} \quad (5.65)$$

By Equation (5.14)

$$\xi = \mu \wedge \gamma \quad (5.66)$$

Let us illustrate Theorem 5.5 with the following example.

Example 5.2

Consider the machine M and faults μ_3 and μ_5 of Example 5.1 and μ_7 of M specified by the following table

$q \backslash \mu_1$	$\mu_7(q)$
1	2
2	3
3	1
4	4

(5.67)

$$T_{1,0}^{\mu_7} = (a^4) * (a^2 + a^3 + a^4) \quad (5.68)$$

$$T_{1,1}^{\mu_7} = (a^4) * a \quad (5.69)$$

Now

$$\begin{aligned} & T_{1,0} \cdot (\bar{T}_{1,0}^{\mu_5} + \bar{T}_{1,0}^{\mu_7}) \\ &= (a^4) * (a + a^3 + a^4) \cdot [(a^4) * a^3 + (a^4) * a] \\ &= (a^4) * (a + a^3) \end{aligned} \quad (5.70)$$

$$\begin{aligned} & T_{1,1} \cdot (\bar{T}_{1,1}^{\mu_5} + \bar{T}_{1,1}^{\mu_7}) \\ &= (a^4) * a^2 \cdot [(a^4) * (a + a^2 + a^4) + (a^4) * (a^2 + a^3 + a^4)] \\ &= (a^4) * a^2 \end{aligned} \quad (5.71)$$

Since $\bar{T}_{1,0}^{\mu_3} = T_{1,1}^{\mu_3} = (a^2) * a$

and

$$\bar{T}_{1,1}^{\mu_3} = T_{1,0}^{\mu_3} = (a^2) * a^2$$

we have

$$\begin{aligned} T_{1,0} \cdot \bar{T}_{1,0}^{\mu_3} &= (a^4) * (a + a^3 + a^4) \cdot (a^2) * a \\ &= (a^4) * (a + a^3) \end{aligned} \quad (5.72)$$

and

$$\begin{aligned} T_{1,1} \cdot \bar{T}_{1,1}^{\mu_3} &= (a^4) * a^2 \cdot (a^2) * a^2 \\ &= (a^4) * a^2 \end{aligned} \quad (5.73)$$

Thus the condition of Theorem 5.5 is satisfied and

$$\mu_3 = \mu_5 \wedge \mu_7 \quad (5.74)$$

By direct construction

$$\hat{D}(\mu_3, 1) = aI^* \quad (5.75)$$

$$\hat{D}(\mu_5, 1) = a^2I^* \quad (5.76)$$

$$\hat{D}(\mu_7, 1) = aI^* \quad (5.77)$$

and the above equality is verified. In fact we found that $\mu_3 \equiv \mu_7$ and

$$\mu_5 \leq \mu_3.$$

Section 5.3 Conditions of Fault Detection and a Class of Easily Detectable Faults

Let us now turn our attention to the application of results obtained in Chapter 4 and Section 5.2 to the problem of identifying behavior classes which are conducive to testing. One such class of machines is the strongly connected machines which will be studied here with regard to fault detection with emphasis on failures caused by the memory elements. The property of machine diagnosability relative to computation of optimum test set will also be discussed in the context of memory fault detection concept developed in Section 4.2. We begin by examining some conditions and characterizations for fault detection.

Suppose q is a state of machine M , we would like to know what are the conditions for a given memory fault to be q -detectable in terms of the structure of good machine and the result of the fault. The following theorem give a sufficient condition.

Theorem 5.6 If μ is a (memory) fault of machine $M = (I, Q, Z, \delta, \omega)$ and $q \in Q$, then μ is q -detectable if μ is r -detectable for some $r \in Q$, $r \neq q$ and $\exists x \in I^+$ such that

$$1) \quad \bar{\delta}(q, x) = r \text{ and}$$

$$2) \quad \mu \bar{\delta}(q, x) = \bar{\delta}^{\mu}(\mu(q), x)$$

Proof: Since μ is r -detectable, by definition, $\exists y \in I^+ \ni$

$$\beta_r(y) \neq \beta_{\mu(r)}^\mu(y) \quad (5.78)$$

Now from 1)

$$\beta_q(xy) = \beta_{\bar{\delta}(q,x)}(y) = \beta_r(y) \quad (5.79)$$

and from 2)

$$\begin{aligned} \beta_{\mu(q)}^\mu(xy) &= \beta_{\bar{\delta}^\mu(\mu(q),x)}^\mu(y) \\ &= \bar{\beta}_{\mu\bar{\delta}(q,x)}(y) \\ &= \beta_{\mu(r)}^\mu(y) \end{aligned} \quad (5.80)$$

From Equations (5.79) and (5.80), it follows that

$$\begin{aligned} \beta_r(y) \neq \beta_{\mu(r)}^\mu(y) &\Rightarrow \beta_q(xy) \neq \beta_{\mu(q)}^\mu(xy) \\ &\Rightarrow \beta_q \neq \beta_{\mu(q)}^\mu \end{aligned} \quad (5.81)$$

$\therefore \mu$ is q -detectable

Theorem 5.6 relates the detection of a memory fault from a given state to the detection of the same fault from another state.

Although this result may not be directly useful in connection with test generation, it nevertheless establishes some structural relationship of machine in terms of fault detection. To explore further the nature of this relationship, we have the following characterization of a q -detectable fault.

Theorem 5.7 A memory fault μ of machine $M = (I, Q, Z, \delta, \omega)$ is q -detectable, where $q \in Q$, if and only if $\exists x \in I^*$ such that

$$\bar{\delta}(q, x) \not\equiv_1 \bar{\delta}^\mu(\mu(q), x)$$

where $\equiv_1$ represents 1-equivalence.

Proof: Sufficiency. If $\exists x \in I^* \ni \bar{\delta}(q, x) \not\equiv_1 \bar{\delta}^\mu(\mu(q), x)$, then let $y = xa \ni$

$$\omega(\bar{\delta}(q, x), a) \neq \omega^\mu(\bar{\delta}^\mu(\mu(q), x), a)$$

$$\text{i.e.} \quad \beta_q(xa) \neq \beta_{\mu(q)}^\mu(xa)$$

$\therefore \mu$ is q -detectable.

Necessity. Suppose μ is q -detectable, then $\exists x \in I^+ \ni \beta_q(x) \neq \beta_{\mu(q)}^\mu(x)$. Let $x = ya$ for $y \in I^*$ and $a \in I$, then

$$\omega(\bar{\delta}(q, y), a) \neq \omega^\mu(\bar{\delta}^\mu(\mu(q), y), a)$$

By definition

$$\bar{\delta}(q, y) \not\equiv_1 \bar{\delta}^\mu(\mu(q), y)$$

completing the proof.

From Theorems 5.6 and 5.7, it is easy to see that if μ is to be q -detectable, some successor state of q in M should be distinguishable from some successor state of $\mu(q)$ in M^μ . The least upper-bound of a shortest (μ, q) -detection sequence has been derived in Lemma 4.1.

That result was then used to derive an upper-bound for the cost of an optimum (F, q) -test set where F is a set of faults in machine M in terms of the number of states in M and number of faults in F . In some special class of faults, the dependence of this bound to the number of faults under consideration can be eliminated, as to be shown below.

Definition 5.1 A memory fault μ of machine $M = (I, Q, Z, \delta, \omega)$ is definitely q -detectable for some $q \in Q$, if there is an integer k such that $\forall x \in I^k$

$$\hat{\beta}_q(x) \neq \hat{\beta}_{\mu(q)}^\mu(x)$$

Lemma 5.4 If μ is a definitely q -detectable memory fault of $M = (I, Q, Z, \delta, \omega)$, then $\forall x \in I^k \ni$

$$k \geq |Q| + |Q^\mu|$$

x is a (μ, q) -detection sequence.

Proof: The proof is similar to Theorem 2.2. Suppose to the contrary, i.e. $\exists x \in I^+ \ni$

$$\lg(x) \geq |Q| + |Q^\mu|$$

and

$$\hat{\beta}_q(x) = \hat{\beta}_{\mu(q)}^\mu(x).$$

First we observe that since μ is a memory fault, $|Q^\mu| \leq |Q|$. Then consider the set of successor state pair $(\bar{\delta}(q, y), \bar{\delta}^\mu(\mu(q), y))$ where y is a prefix of x . Since there are at most $|Q^\mu| + |Q| \leq |Q|^2$ distinct such state pairs, it must be the case that some such state pairs repeat

under x , i.e. $\exists y, w \in I^*$ and $z \in I^+ \ni x = yzw$ and $(\bar{\delta}(q, y), \bar{\delta}^\mu(\mu(q), y)) = (\bar{\delta}(q, yz), \bar{\delta}^\mu(\mu(q), yz))$. This is illustrated in Figure 5.1

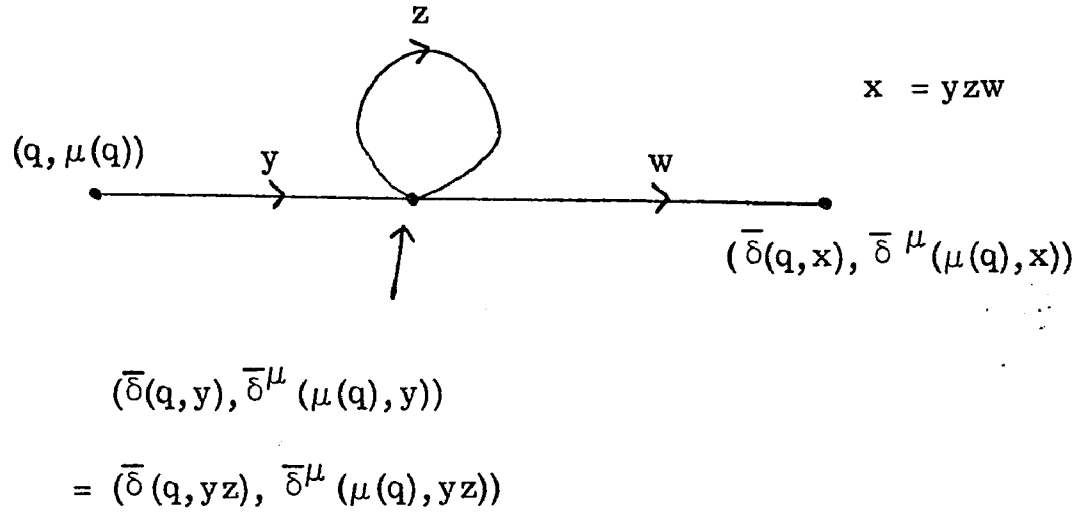


Figure 5.1 Repeated Successor State Pair of $(q, \mu(q))$ under x .

Now since $\hat{\beta}_q(x) = \hat{\beta}_{\mu(q)}^\mu(x)$ and the fact that $(\bar{\delta}(q, y), \bar{\delta}^\mu(\mu(q), y)) = (\bar{\delta}(q, yz), \bar{\delta}^\mu(\mu(q), yz))$, the sequence y followed by arbitrary iteration of z , yz^+ cannot be a (μ, q) -detection sequence. Thus by Definition 5.1 μ is not definitely q -detectable, contrary to our assumption, and thus completing the proof.

Theorem 5.8 If F is a set of definitely q -detectable memory faults of $M = (I, Q, Z, \delta, \omega)$ where $q \in Q$ and X is a minimum cost (F, q) -test set, then

$$\varphi(X) \leq |Q|^2 + 1$$

Proof: From Lemma 5.4, $\forall x \in I^{|Q|^2}$, x is a (μ, q) -detection sequence for any $\mu \in F$. By Definition 4.6, $\{x\}$ is a (F, q) -test set. By Definition 4.7 and the fact that X is of minimum cost, it follows that

$$\varphi(X) \leq \varphi(\{x\}) = |Q|^2 + 1 \quad (5.82)$$

From Lemma 5.4, if μ is definitely q -detectable then it is possible that $\hat{D}(\mu, q)$ contains a regular expression of the form $I^k I^*$ where $k \leq |Q| |Q|^\mu$. Thus the regular representation of the q -detection set of a fault provides a convenient method of identifying a definitely q -detectable fault. From Theorem 5.8, if F is a set of definitely q -detectable faults, then

$$\bigcap_{\mu \in F} \hat{D}(\mu, q) \supseteq I^k I^* \quad (5.83)$$

where $k \leq |Q|^2$. An example of a class of machines where all q -detectable faults are definitely q -detectable is the class of autonomous machines. In this case, if X is a minimum cost (F, q) -test set of an autonomous machine where F is the set of all q -detectable faults which does not increase the number of states, then

$$\varphi(X) \leq 2 |Q| \quad (5.84)$$

Let us illustrate the results and observation with an example.

Example 5.3

Let us consider the machine M whose state table is shown below

	0	1
1	2/0	1/0
2	2/1	3/0
3	3/0	1/1

(5.85)

$$T_{1,0} = (1 + 00*10*1) * (I + 00*1 + 00*10*0) \quad (5.86)$$

$$T_{1,1} = (1 + 00*10*1)*00*(0 + 10*1) \quad (5.87)$$

The memory faults μ_1 and μ_2 specified by the following table.

$q \backslash \mu_i$	$\mu_1(q)$	$\mu_2(q)$
1	3	2
2	2	2
3	3	3

(5.88)

are definitely 1-detectable since

$$T_{1,0}^{\mu_1} = I*0 \quad (5.89)$$

$$T_{1,1}^{\mu_1} = I*1 \quad (5.90)$$

$$T_{1,0}^{\mu_2} = (0 + 10*1)*(1 + 10*0) \quad (5.91)$$

$$T_{1,1}^{\mu_2} = (0 + 10*1)*(0 + 10*1) \quad (5.92)$$

and from Equations (5.86) - (5.92),

$$\begin{aligned}
\hat{D}(\mu_1, 1) &= (T_{1,0} \cdot T_{1,1}^{\mu_1} + T_{1,1} \cdot T_{1,0}^{\mu_1}) I^* \\
&= (1 + 00*10*1) * (1 + 00*1) I^* \\
&+ (1 + 00*10*1) * 00*0 I^* \\
&= (1 + 00*10*1) * (1 + 00*0 + 00*1) I^* \\
&= (1 + 00*0 + 00*1) I^* \\
&= (1 + 00*I) I^* \\
&= 1 \Pi^* + 1 + 0 I I^* + 0^2 0^* I I^* \\
&= 1 + I^2 I^*
\end{aligned} \tag{5.93}$$

$$\begin{aligned}
\hat{D}(\mu_2, 1) &= (T_{1,0} \cdot T_{1,1}^{\mu_2} + T_{1,1} \cdot T_{1,0}^{\mu_2}) I^* \\
&= (00*10*1) * (0 + 11) I^* \\
&+ 101 I^* + 100 I^* \\
&= (0 + 11 + 101 + 100) I^* \\
&= (0 + 11) + I^3 I^*
\end{aligned} \tag{5.9}$$

If $F = \{\mu_1, \mu_2\}$, then it can be shown that $\forall x \in I^3$, $\{x\}$ is a minimum cost test set and

$$\varphi(\{x\}) = 4 \leq 3^2 + 1 = 9 + 1 = 10$$

Thus Theorem 5.8 is verified. Similarly for any $x \in I^2$, x is a $(\mu_1, 1)$ -detection sequence. Comparing to the bound of Lemma 5.4, $2 \leq 3 \times 1 = 3$ and the Lemma is thus verified.

Let us now examine the question of when all proper memory faults of a machine can be detected, proper in the sense that the fault is not an identity mapping of the state set. The following theorem gives a necessary condition for every proper memory fault to be q_0 -detectable where q_0 is assumed to be a reset state of the machine.

Theorem 5.9 If M is a machine with initial state q_0 and every proper memory fault is q_0 -detectable, then M must be reduced.

Proof: Suppose M is not reduced, then $\exists q, r \in Q \ni q \equiv r$.

Consider the proper memory fault $\mu \ni \mu(q) = r$ and $\forall q' \in Q \ni q' \neq q$, but $\mu(q') = q'$. Since $q \equiv r$, it follows that $\mu(q) \equiv q$. Now consider the

set of all sequences $x \in I^* \ni \bar{\delta}(q_0, x) = q$, we claim $\bar{\delta}^\mu(\mu(q_0), x) \equiv r$.

First consider the set of all minimal length sequences x which takes

q_0 to q , i.e. no proper prefix of x, x' , is a transition sequence from

q_0 to q . Then clearly $\bar{\delta}(q_0, x') = \bar{\delta}^\mu(\mu(q_0), x')$ since $\forall q' \neq q$, $\mu(q') = q'$.

Consider then the set of such x' and $a \in I \ni x = x'a$

$$\delta(\bar{\delta}(q_0, x'), a) = q$$

$$\mu \delta(\bar{\delta}(q_0, x'), a) = \delta^\mu(\bar{\delta}(q_0, x'), a) = \mu(q)$$

$$\begin{aligned} \text{i.e.} \quad \bar{\delta}^\mu(\mu(q_0), x) &= \delta^\mu(\bar{\delta}^\mu(\mu(q_0), x'), a) \\ &= \delta^\mu(\bar{\delta}(q_0, x'), a) = \mu(q) = r. \end{aligned}$$

For all $y \in I^*$

$$\bar{\delta}^\mu(\mu(q), y) = \bar{\delta}(r, y) \equiv \bar{\delta}(q, y)$$

$$\therefore \forall x \in I^* \exists \bar{\delta}(q_0, x) = q$$

$$\bar{\delta}^\mu(\mu(q_0), x) \equiv r \equiv \bar{\delta}(q_0, x) = q$$

and for all other $x \in I^* \ni x$ does not take M thru q, it is obvious

$$\bar{\delta}^\mu(\mu(q_0), x) = \bar{\delta}(q_0, x)$$

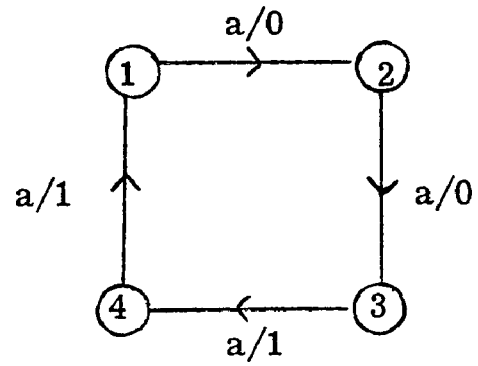
Thus $\beta_{q_0} = \beta_{\mu(q_0)}^\mu$ and μ cannot be q_0 -detectable.

Theorem 5.9 does not produce any surprise to our intuition because a machine with equivalent states possesses memory redundancy which naturally masks memory faults occurred among the equivalent states. It might be expected that the converse of Theorem 5.9 would also hold but interestingly this is not so. The following example illustrates a reduced machine M and a proper memory fault μ such that μ is not q -detectable for some initial state q of M.

Example 5.4

Consider the machine M and a proper memory fault μ shown in Figure 5.2 where μ permutes the state of M . It is obvious that M is reduced and μ is a proper memory fault of M , yet state 1 of $M \equiv \mu(1) = \text{state 2 of } M^\mu$. Therefore, μ is not 1-detectable.

	a
1	2/0
2	3/0
3	4/1
4	1/1



Machine M

q \ μ	$\mu(q)$
1	2
2	3
3	1
4	4

Fault μ

	a
2	1/0
1	3/0
3	4/1
4	2/1

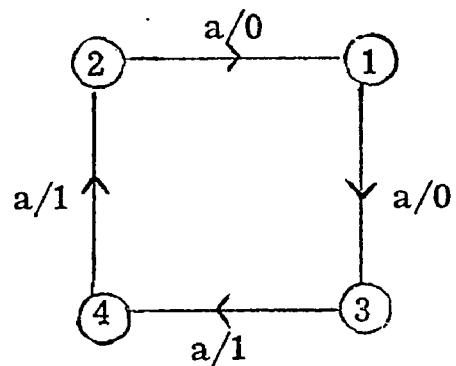
Results of μ, M^μ

Figure 5.2 Examples of a Proper Memory Fault in a Machine Which is Not q -Detectable.

Section 5.4 Strongly Connected and Diagnosable Machines

If M is a reduced and strongly connected machine, it is known that a fault of M is checkable (in the sense of [26]) if and only if the behavior of the faulty machine differs from M . Accordingly, a memory fault μ of M is checkable if $M^\mu \neq M$. To explore the relationship between the concept of checking and that of state-detection, let us first consider the following lemma.

Lemma 5.5 If M is a reduced and strongly connected machine, then every checkable fault of M is q -detectable for any state q of M .

Proof Let μ be a checkable fault of M and suppose there is a state q of M such that μ is not q -detectable, i. e.

$$\beta_q = \beta_{\mu(q)}^\mu .$$

Since M is strongly connected, we have [19]

$$M \leq M^\mu$$

Then $\forall r \in Q$, there is an $r' \in Q^\mu$ such that $r \equiv r'$. But since M is reduced, $|Q| \leq |Q^\mu|$. Now since μ is a memory fault, we have $|Q^\mu| \leq |Q|$. Thus it must be the case that $|Q^\mu| = |Q|$ and it follows that $M^\mu \equiv M$, contrary to our hypothesis that μ is checkable. Therefore, the supposition is false and μ must be q -detectable for any state q of M , completing the proof.

Note that the converse of the above lemma is not true, i. e. there

are q -detectable faults which are not checkable. Extending Lemma 5.5 to the case of faults set, we have,

Theorem 5.10 If M is a reduced and strongly connected machine, q is a state of M and F is a set of checkable faults, then

$$\bigcap_{\mu \in F} \hat{D}(\mu, q) \neq \phi$$

Proof: Choose $\mu_1 \in F$ and $x_1 \in I^+ \ni x_1$ is a (μ_1, q) -detection sequence. This is possible because μ_1 is q -detectable. Choose $\mu_2 \in F$, then since M is reduced and strongly connected, by Lemma 5.5, $\bar{\delta}(q, x_1) \neq \bar{\delta}^{\mu_2}(q, x_1)$. Thus $\exists x_2 \in I^+ \ni$

$$\beta_q(x_1 x_2) \neq \beta_{\mu_2(q)}^{\mu_2}(x_1 x_2) \quad (5.94)$$

Repeating this process, for the i th fault $\mu_i \in F$, $\exists x_i \in I^+ \ni$

$$\beta_q(x_1 x_2 \dots x_i) \neq \beta_{\mu_i(q)}^{\mu_i}(x_1 x_2 \dots x_i) \quad (5.95)$$

Finally, if $|F| = m$ then

$$\hat{\beta}_q(x_1 x_2 \dots x_m) \neq \hat{\beta}_{\mu_i(q)}^{\mu_i}(x_1 x_2 \dots x_m) \quad (5.96)$$

for $1 \leq i \leq m$.

Thus $x = x_1 x_2 \dots x_m$ is an (F, q) -test set and

$$x \in \bigcap_{\mu \in F} \hat{D}(\mu, q)$$

Corollary 5.10.1 If M is a reduced and strongly connected machine, q is a state of M , F is a set of checkable faults and X is an optimum (F, q) -test set, then

$$\varphi(X) \leq 1 + (2|Q| - 1)|F|$$

Proof: From Lemma 4.1, for each μ_i and x_i selected in the proof of Theorem 5.10 $\lg(x_i) \leq |Q| + |Q^{\mu_i}| - 1$. Thus if $x = x_1 x_2 \dots x_{|F|}$, then

$$\begin{aligned} \varphi(\{x\}) &= 1 + \lg(x) \\ &\leq 1 + \sum_{\mu_i \in F} (|Q| + |Q^{\mu_i}| - 1) \\ &= 1 + |F||Q| - |F| + \sum_{\mu_i \in F} |Q^{\mu_i}| \\ &\leq 1 + (2|Q| - 1)|F| \end{aligned} \tag{5.97}$$

Since X is an optimum test set and from Equation (5.97), it follows that

$$\varphi(X) \leq \varphi(\{x\}) \leq 1 + (2|Q| - 1)|F| \tag{5.98}$$

In case M is also diagnosable, the requirement that $M^\mu \neq M$ $\forall \mu \in F$ is not needed, that is,

Corollary 5.10.2 If M is a strongly connected and diagnosable machine, $q \in Q$ and F is a set of q -detectable faults, then

$$\bigcap_{\mu \in F} \hat{D}(\mu, q) \neq \phi$$

Proof: Let x be a DS of M , then if a fault μ is q -detectable such that $M^\mu \equiv M$, then $\exists r \in Q, r \neq q$ and $r \equiv \mu(q) \ni$

$$\hat{\beta}_q(x) \neq \hat{\beta}_r(x) = \hat{\beta}_{\mu(q)}^\mu(x)$$

We can then append to x the sequence constructed in the proof of Theorem 5.10 and denote it y . It is clear that xy is an (F, q) -test set and

$$xy \in \bigcap_{\mu \in F} D(\mu, q)$$

Moreover if X is an optimum (F, q) -test set, then

$$\phi(X) \leq \lg(x) + 1 + (2|Q| - 1)|F|.$$

Theorem 5.10 says that if a machine is reduced and strongly connected, then there is a simple experiment [40] which will detect any given set of nonequivalent faults in the machine. The properties that a machine be reduced and strongly connected and the faults occurred be nonequivalent are not required in the case of state-detection since in the latter approach we allow for multiple experiment. The fundamental question of whether the property of strong connectedness is useful or not relative to our fault detection concept remains unsettled. However, in the case where all q -detectable faults occurred are nonequivalent to the fault-free machine, the bound derived in Corollary 5.10.1 for the cost of an optimum test set is smaller than the general bound derived in Theorem 4.7 and strong connectedness appears to be a desirable property. If further the property of diagnosability is added, then all proper memory faults which are q -detectable can be detected by a

simple experiment as shown in Corollary 5.10.2. To further explore the application of these detection concepts, let us next consider a simple experiment on strongly connected and diagnosable machines with cost of test set independent of the number of faults in a given faults set. If x is a distinguishing sequence (DS) of machine M , then we say that a state q in M is identified (by x) if M is initially in state q when x is applied and $\hat{\beta}_q(x)$ observed. Let us first present the following lemma.

Lemma 5.6 If $M = (I, Q, Z, \delta, \omega)$ is a strongly connected diagnosable machine and if $k < n$ states have been identified, where $n = |Q|$, then $\exists x \in I^\ell$, $\ell \leq k$, so that the final state of M is not in any of the states already identified if x is applied and M is initially in one of the states identified.

Proof: Let S be the set of states that have been identified. We prove the lemma by induction.

Basis If $S = \{q_0\}$ for $q_0 \in Q$ then it must be the case that $\exists a \in I \ni \delta(q_0, a) \neq q_0$. Otherwise M cannot be strongly connected.

Induction Step Suppose the lemma holds for $|S| = k$, i.e. let $S = \{q_0, q_1, \dots, q_{k-1}\}$, then $\exists x \in I^\ell$, $\ell \leq k$, $\ni \bar{\delta}(q_i, x) = q_k \notin S \forall q_i \in S$. Consider $S' = S \cup \{q_k\}$ and suppose $\forall x \in I^\ell$, $\ell \leq k+1 < n$ and $\forall q_i \in S'$

$$\bar{\delta}(q_i, x) \in S'.$$

Then $\forall y_{k+1} \in I^{k+1}$, $\bar{\delta}(q_k, y_{k+1}) \in S'$.

If $\bar{\delta}(q_k, y_{k+1}) \in S$, then $\forall q \in S$, $\bar{\delta}(q, y_k) \in S$ contrary to the hypothesis.

If $\bar{\delta}(q_k, y_{k+1}) = q_k$, then since $\forall a \in I, \delta(q_k, a) \in S'$, M cannot be strongly connected, completing the proof.

Interpreting Lemma 5.6, if M is a strongly connected machine and S is a proper subset of the state set, then the longest transition sequence from any state in S to any state in $Q - S$ needs not exceed the number of elements in the set S . Using this lemma, if M is a strongly connected diagnosable machine and F is the set of proper faults in M such that $\forall \mu \in F, |Q^\mu| < |Q|$, then it is possible to derive an (F, q) -test set, where $q \in Q$, such that the cost of the test set is independent of the number of faults in F . An Algorithm which accomplishes this result is presented below:

Algorithm 5.1

1. Assume q_0 is the starting state, $S \leftarrow \{q_0\}$. Choose a DS x of the shortest length.
2. Apply x to M . If the terminal state q is in S , then apply a transition sequence (TS) y so that the terminal state q' is not in S . Note that $\lg(y) \leq |S|$. $S \leftarrow S \cup \{q'\}$.
3. If the terminal state q is not in S , then $S \leftarrow S \cup \{q\}$.
4. Use q or q' as the next starting state and repeat steps 2) - 3) until x has been applied to each state in M .

A flow chart for Algorithm 5.1 is shown in Figure 5.3. In essence this is just a formalization of the second part of the checking experiment first proposed by Hennie [26]. The following theorem shows that a

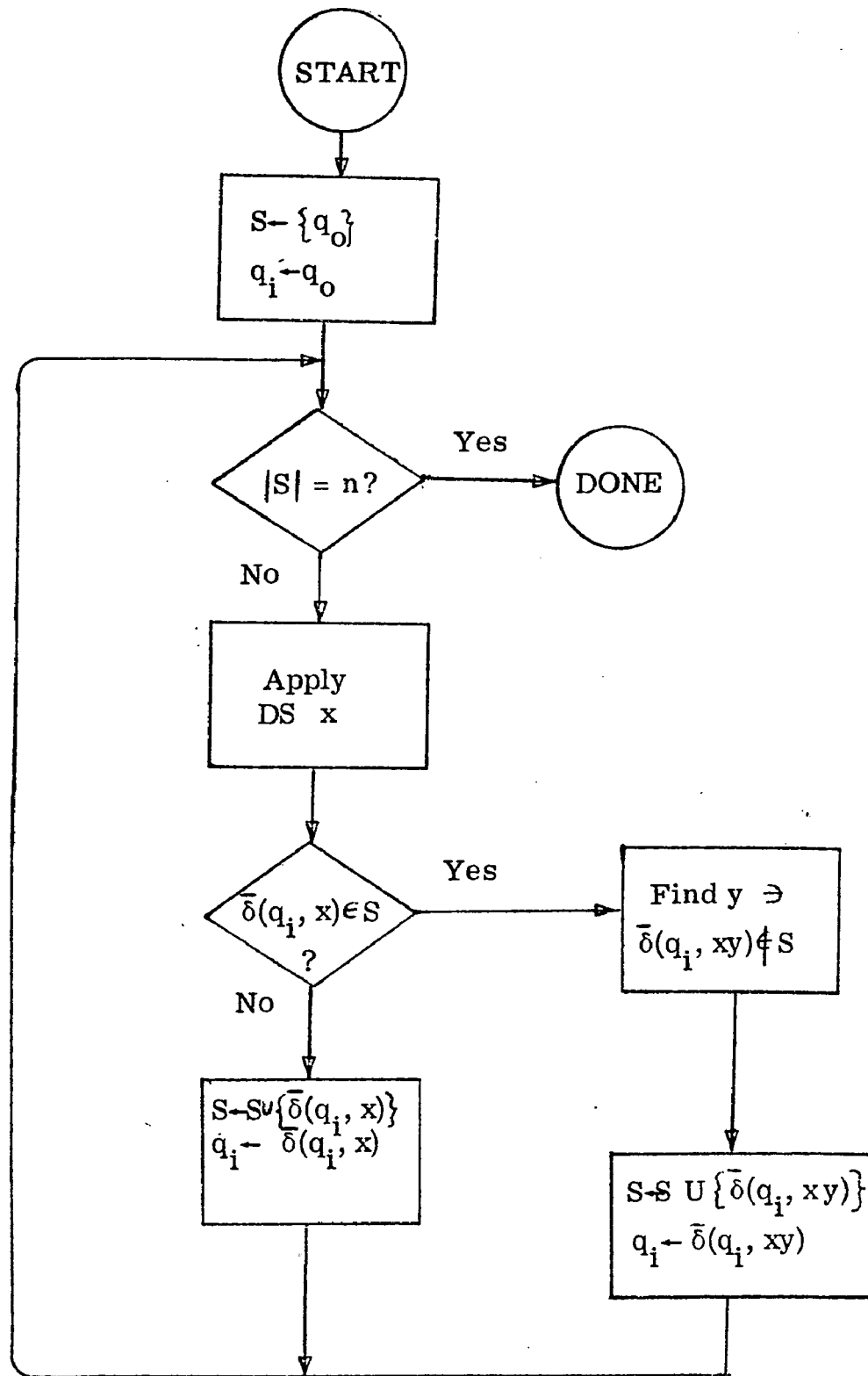


Figure 5.3 Flow Chart of Algorithm 5.1

sequence obtained by Algorithm 5.1 is indeed an (F, q) -test set for some starting state q of M , and from there an upper-bound on the cost of an optimum (F, q) -test set is derived.

Theorem 5.11 If $M = (I, Q, Z, \delta, \omega)$ is a strongly connected diagnosable machine, L is the order of diagnosability and F is the set of all proper faults in M such that $\forall \mu \in F \quad |Q^\mu| < |Q|$, then Algorithm 5.1 determines an (F, q) -test set for some $q \in Q$. Moreover, if X is an optimum (F, q) -test set, then

$$\varphi(X) \leq nL + \frac{n(n-1)}{2} + 1$$

where $n = |Q|$.

Proof: Since M is strongly connected, every state of M can be reached at least once starting from any state. The algorithm applies the DS x exactly n times, we shall expect n different responses at n states of M . Suppose μ in F occurs, since $|Q^\mu| < n$ it follows that $|\{\beta_{\mu(q)}^\mu(x) \mid q \in Q\}| < n$ and the outputs of M^μ cannot be the same as M under the sequence generated by the algorithm.

To obtain the bound, we note that n times of x have been applied to M , thus the test sequence must not be shorter than nL . From the lemma, we know that after identifying $k < n$ states, the longest transition sequence required to take M to a new state is k and since possibly we may have to apply these transition sequences $n-1$ times we obtain the maximum total length of these transition sequences as:

$$\sum_{i=1}^{n-1} i = \frac{n(n-1)}{2} \quad (5.99)$$

Therefore, if $y \in I^+$ is the test sequence generated by the algorithm

$$\ell g(y) \leq nL + \frac{n(n-1)}{2}. \quad (5.100)$$

Since X is of minimum cost, it follows that

$$\varphi(X) \leq 1 + \ell g(y) = nL + \frac{n(n-1)}{2} + 1 \quad (5.101)$$

Section 5.5 Definite Machines

Continuing our exploration of the application of the fault detection concepts and regular representation of fault detection sets as developed in the last chapter, let us now consider another special class of machines where the output behavior of the machine depends only on the past k -input symbols for some integer k . More precisely

Definition 5.2 A machine $M = (I, Q, Z, \delta, \omega)$ is said to be definite if there is an integer k such that $\forall x \in I^+, \ell g(x) \geq k$, then

$$\beta_q(x) = \beta_r(x) \quad \forall q, r \in Q.$$

It is widely known that a definite machine can be realized by a network containing no feedback loops. Because of this property, it may be expected that this class of machines is "easier" for determining test set. We will attempt to formally support this conjecture in the development that follows. We begin by deriving a regular expression characterization of definite machine [12].

Theorem 5.12 A machine $M = (I, Q, Z, \delta, \omega)$ with initial state q is definite if and only if for every $z \in Z$, $T_{q,z}$ can be represented by the following expression

$$T_{q,z} = A_z + I * B_z$$

where A_z and B_z represent finite sets of sequences.

Proof Sufficiency

Since A_z and B_z are finite, $T_{q,z}$ can be represented in a form such that $A_z \cdot I^* B_z = \phi$. Since M is a Mealy machine

$$\sum_{z \in Z} T_{q,z} = I^+ = A + I^* B \quad (5.102)$$

where

$$A = \sum_{z \in Z} A_z \text{ and } I^* B = \sum_{z \in Z} I^* B_z \quad (5.103)$$

Let

$$m = \max \{ \ell g(x) \mid x \in A \} \quad (5.104)$$

and

$$k = m + 1.$$

Then $\forall z \in Z$, if $x \in T_{q,z}$ and $\ell g(x) \geq k$, $x \in I^* B_z$.

That is, if $x = y'w$ for some $y' \in I^*$ and $w \in B_z$ then $\forall y \in I^*$

$$\beta_q(w) = \beta_q(yw) = z \quad (5.105)$$

i. e.

$$\beta_r(w) = \beta_s(w) = z \quad \text{for } r, s \in \mathcal{R}(\delta(q, I))$$

Since this is true for all $z \in Z$, it follows that $\forall x \in I^+ \ni \ell g(x) \geq k$

$$\beta_r(x) = \beta_s(x) \quad \forall r, s \in \mathcal{R}(\delta(q, I)) \quad (5.106)$$

Since M is an initial state machine, the proof is complete.

Necessity

Suppose M is definite, then $\forall x \in I^+ \ni \ell g(x) \geq k$

$$\beta_r(x) = \beta_s(x) \quad \forall r, s \in Q$$

If $x \in T_{q,z}$ and $\ell g(x) = k$, then because of definiteness

$$\beta_q(x) = \beta_r(x) = z \quad \forall r \in Q \quad (5.107)$$

i.e. $\forall y \in I^*$

$$\beta_q(x) = \beta_q(yx) = z \quad (5.108)$$

i.e. $I^*x \subseteq T_{q,z}$. Since there are finite number of sequences of length k in $T_{q,z}$, it follows that $\exists$ finite set $B_z \ni I^*B_z \subseteq T_{q,z}$. If $x \in T_{q,z} \ni \lg(x) \geq k$, then $x \in I^*B_z$. Otherwise, there are finite number of sequences of length less than k .

Let $A_z = \{x \in T_{q,z} \mid \lg(x) < k\}$, then it follows that

$$T_{q,z} = A_z + I^*B_z \quad (5.109)$$

Since, we choose arbitrary $z \in Z$ to derive this result, Equation (5.109) holds for all $z \in Z$, completing the proof.

Thus, it is evident that regular expression provides a useful characterization of definite machines. An event R over $I^*(R \subseteq I^*)$ is said to be definite if it can be represented in a form as that of Equation (5.109), i.e. if

$$R = E + I^*F \quad (5.110)$$

where E and F are finite expressions. Thus by Theorem 5.12 a machine is definite if and only if each of its output event $T_{q,z}$ is a definite event. A definite event of the form $R = E$ is called initial while event of the form $R = I^*F$ is called non-initial. Initial events are transient behavior while non-initial events can be considered as steady state conditions of the machine. An example of a definite machine is machine M of Figure 4.1, and regular expressions of the

output behaviors $T_{q,z}$'s of M are demonstrated by Equations (4.8) and (4.9). Another point perhaps worth mentioning is the definition of definite machine. Some author [30] define definite machine in terms of structure property, i.e. a machine M with initial state q is definite if and only if $S_{q,r}$'s are definite events for every $r \in Q$. It can be shown that such definition is a special case of our more general behavior type definition given in Definition 5.2 and Theorem 5.12. For example, if $S_{q,r}$ is definite for every $r \in Q$, then it can be easily verified that $T_{q,z}$ is a definite event for every $z \in Z$, but the converse is not true. It is well known that in the case of reduced machine, these two definitions are equivalent. From the stand point of studying machine structure per se, it might be expected that no additional knowledge would be gained by considering non-reduced machines. However, in the case of studying fault detection problem, many faulty machines are non-reduced, and adoption of the structure type definition will inevitably reduce the number and types of failures that can be considered.

Returning now to the problem of fault detection in definite machines, consider first the following special type of faults.

Definition 5.3 Let M be a machine and μ be a fault of M . μ is said to be definite if M^μ is a definite machine.

In other words, a fault μ is definite if the result of μ (i.e. the faulty machine under μ) is a definite machine. In a definite machine,

if a fault is non-definite, then a process of determining whether the given machine is definite would be generally sufficient to detect that fault. As might be expected from intuition that such types of faults are "easier" to detect. Thus in the development that follows, we will focus on the type of faults that are definite in definite machines. It will be shown next that the regular expression representation of fault detection set is very convenient for such application.

Theorem 5.13 Let $M = (I, Q, Z, \delta, \omega)$ be a definite machine, $q \in Q$ and μ be a fault of M . If μ is definite then $D(\mu, q)$ is a definite event.

Proof: If μ is not q -detectable, then by definition, $D(\mu, q) = \phi$ implies $D(\mu, q)$ is definite. If μ is q -detectable, then $D(\mu, q) \neq \phi$ and from Theorem 5.12, $\forall z \in Z$

$$T_{q, z} = A_z + I * B_z \quad (5.111)$$

and

$$T_{q, z}^\mu = A_z^\mu + I * B_z^\mu \quad (5.112)$$

where A_z, B_z, A_z^μ and B_z^μ are finite expressions. From Theorem 4.3

$$\begin{aligned} D(\mu, q) &= \sum_{z \in Z} T_{q, z} \cdot \overline{T_{q, z}^\mu} \\ &= \sum_{z \in Z} (A_z + I * B_z) \cdot \overline{(A_z^\mu + I * B_z^\mu)} \\ &= \sum_{z \in Z} (A_z + I * B_z) \cdot \sum_{z' \neq z} (A_{z'}^\mu + I * B_{z'}^\mu) \end{aligned}$$

$$\begin{aligned}
&= \sum_{z \in Z} (A_z + I^*B_z) \cdot (A_z^\mu + I^*B_z^\mu) \\
&= \sum_{z \in Z} (A_z \cdot A_z^\mu + A_z \cdot I^*B_z^\mu + I^*B_z \cdot A_z^\mu \\
&\quad + I^*B_z \cdot I^*B_z^\mu) \\
&= A_q^\mu + I^*B_q^\mu \tag{5.113}
\end{aligned}$$

where

$$A_z^\mu = \sum_{\substack{z' \neq z \\ z' \in Z}} A_{z'}^\mu \tag{5.114}$$

$$I^*B_z^\mu = \sum_{\substack{z' \neq z \\ z' \in Z}} I^*B_{z'}^\mu = I^* \sum_{\substack{z' \neq z \\ z' \in Z}} B_{z'}^\mu \tag{5.115}$$

$$A_q^\mu = \sum_{z \in Z} (A_z \cdot A_z^\mu + A_z \cdot I^*B_z^\mu + I^*B_z \cdot A_z^\mu) \tag{5.116}$$

$$I^*B_q^\mu = \sum_{z \in Z} I^*B_z \cdot I^*B_z^\mu \tag{5.117}$$

Thus by Definition 5.3, $D(\mu, q)$ as represented by Equation (5.113) is a definite event and the theorem is proven.

Thus if both the good machine M and the faulty machine M^μ are definite machines, then the basic q -detection set of μ is a definite event. We will further require that the faulty machine be non-equivalent to the fault free machine. Although we have interpreted previously that the non-initial definite event part of $T_{q,z}$ in a definite machine as a steady

state output behavior, it is not completely clear how a necessary condition for the existence of such behavior can be characterized in terms of machine structure. However, we are able to obtain a sufficient condition in which every $T_{q,z}$ contains a non-initial definite event.

Lemma 5.7 If M is a strongly connected definite machine and $q \in Q$, then $\forall z \in Z$ $T_{q,z} = A_z + I*B_z$ and $B_z \neq \phi$

Proof: With no loss of generality, let us assume that M is reduced. Since M is definite and reduced, it follows that each $S_{q,r}$ is also a definite event, i.e. $\forall r \in Q$

$$S_{q,r} = A_r + I*B_r \quad (5.118)$$

where A_r and B_r are finite expressions. We first claim that $\forall r \in Q$, $B_r \neq \phi$. We first note that since M is a Mealy machine

$$\sum_{r \in Q} S_{q,r} = I^* \quad (5.119)$$

Therefore, it is obvious that $\exists s \in Q \ni$

$$S_{q,s} = A_s + I*B_s \text{ and } B_s \neq \phi$$

Now since M is strongly connected, for any $r \in Q \exists x \in I^+ \ni S_{q,s} x \subseteq S_{q,r}$, i.e. $I*B_s x \subseteq S_{q,r}$, this means that $I*B_r \neq \phi$ for any $r \in Q$.

From Equation (4.1)

$$\begin{aligned} T_{q,z} &= \sum_{\substack{\text{all } r \in Q \text{ } a \in I \\ \ni \omega(r,a)=z}} S_{q,r} a \\ &= \sum_{\substack{\text{all } r \in Q \text{ } a \in I \\ \ni \omega(r,a)=z}} (A_r + I*B_r) a \\ &= A_z + I*B_z \end{aligned} \quad (5.120)$$

Since $I*B_r \neq \phi$ for $r \in Q$, it follows that $B_z \neq \phi \quad \forall z \in Z$.

Using the above lemma, we will be able to show in the following that the basic q -detection set of any definite fault in a strongly connected definite machine contains a non-initial definite event.

Theorem 5.14 If $M = (I, Q, Z, \delta, \omega)$ is a reduced and strongly connected definite machine, $q \in Q$ and μ is a q -detectable definite fault, then the basic q -detection set of μ contains a non-initial definite event.

Proof: From Lemma 5.7, since M is strongly connected and definite, $\forall z \in Z$

$$T_{q,z} = A_z + I*B_z \text{ and } B_z \neq \phi \quad (5.121)$$

where A_z and B_z are finite expressions. Since M is reduced and definite, $T_{q,z}$ has a canonical form [12], and we will assume that all events are in canonical form and consequently $A_z \cdot I*B_z \neq \phi$. Since μ is q -detectable and definite, $D(\mu, q) \neq \phi$ and from Theorem 5.13,

$$\begin{aligned} D(\mu, q) = & \sum_{z \in Z} (A_z \cdot A_z^\mu + A_z \cdot I*B_z^\mu + I*B_z \cdot A_z^\mu) \\ & + \sum_{z \in Z} I*B_z \cdot I*B_z^\mu \end{aligned} \quad (5.122)$$

What we want to show is that the last term of Equation (5.122) is non-empty. By the duality of Theorem 4.3 which is shown in Equation (5.6), we can obtain a second expression for $D(\mu, q)$,

$$\begin{aligned} D(\mu, q) = & \sum_{z \in Z} (A_z^\mu \cdot A_z + A_z^\mu \cdot I*B_z + I*B_z^\mu \cdot A_z) \\ & + \sum_{z \in Z} I*B_z^\mu \cdot I*B_z \end{aligned} \quad (5.123)$$

where

$$A'_z = \sum_{\substack{z' \neq z \\ z' \in Z}} A_{z'} \quad (5.124)$$

and

$$I^*B'_z = I^* \sum_{\substack{z' \neq z \\ z' \in Z}} B_{z'} \quad (5.125)$$

Suppose we assume that the last terms of Equations (5.122) and (5.123) are empty, i. e.

$$I^*B_z \cdot I^*B_z^\mu = \phi \quad \forall z \quad (5.126)$$

and

$$I^*B_z^\mu \cdot I^*B'_z = \phi \quad \forall z \quad (5.127)$$

and further if we let

$$A^\mu = \sum_{z \in Z} A_z^\mu \quad (5.128)$$

and

$$A = \sum_{z \in Z} A_z \quad (5.129)$$

Then Equations (5.126) and (5.127) imply that

$$I^*B_z \subseteq A^\mu + I^*B_z^\mu \quad \forall z \quad (5.130)$$

and

$$I^*B_z^\mu \subseteq A + I^*B_z \quad \forall z \quad (5.131)$$

But it can be immediately verified that Equations (5.130) and (5.131) again imply, $\forall z \in Z$

$$A + A^\mu + I^*B_z^\mu = A^\mu + A + I^*B_z \quad (5.132)$$

Therefore

$$I*B_Z^\mu = C_Z^\mu + I*D_Z \quad (5.133)$$

and

$$I*B_Z = C_Z + I*D_Z \quad (5.134)$$

where C_Z^μ , C_Z and D_Z are finite expressions. Thus $\forall z \in Z$

$$T_{q,z} = A_z + C_z + I*D_z \quad (5.135)$$

and

$$T_{q,z}^\mu = A_z^\mu + C_z^\mu + I*D_z \quad (5.136)$$

But since M is strongly connected, by Lemma 5.5, this is impossible unless

$$A_z + C_z = A_z^\mu + C_z^\mu \quad \forall z \in Z \quad (5.137)$$

But Equations (5.136) and (5.137) imply that $D(\mu, q) = \phi$, contrary to our assumption that μ is q -detectable. Thus the assumption is wrong and the theorem is proven.

Perhaps we should look ahead at this point to the utilities of the above theorem. If given a set of faults F in machine M such that all basic q -detection sets of faults in F have non-initial definite sub-events, for some state q of M , then the q -detection set of each of these faults has a subevent representable in the form of $I*BI^*$ for some finite expression B . As shall be shown later that these q -detection sets have a non-empty common intersection which is also representable in the form of $I*B'I^*$ for some regular expression B' . Such form of representation would be useful for computing bound of test set and for obtaining

test set to include faults outside F . Before we state and prove these results, we need the following definition and lemma.

Definition 5.4 Let A and B be two regular expressions over I^* .

The contraction of A and B , denoted C , represents the set of all sequences obtained according to the following rules.

- 1) If $A \cdot B \neq \phi$, then $A \cdot B \subseteq C$
- 2) $\forall x \in A - A \cdot B$ and $y \in B - A \cdot B$ or $x \in B - A \cdot B$ and $y \in A - A \cdot B$, if x is a proper subsequence of y , then $y \in C$ and x and y should be removed from further consideration in the generation of C .
- 3) For the set of remaining sequences in A and B , for each $x \in A$ and $y \in B$, if $x = uv$ for $u, v \in I^+$ and $y = vw$ for $v, w \in I^+$ then $uvw \in C$. Similarly if $x = wz$ then $vwz \in C$.
- 4) When $x \in A$ has compared to each $y \in B$ according to step 3), x is deleted from A .
- 5) The process terminated when A is exhausted.

Lemma 5.8 Let A and B be two regular sets, then

$$I^*AI^* \cdot I^*BI^* = I^*AI^*BI^* + I^*BI^*AI^* + I^*CI^*$$

where C is the contraction of A and B .

Proof: Let $x \in I^*AI^* \cdot I^*BI^*$. Then $\exists u, w, u', w' \in I^*, v \in A$ and $v' \in B \Rightarrow x = uvw = u'v'w'$. We consider the following cases

- 1) If $u'v'$ is a prefix of u , then let $u = u'v'v''$ where $v'' \in I^*$, $x = u'v'v''vw$ and $x \in I^*BI^*AI^*$.
- 2) If uv is a prefix of u' , then using arguments presented in 1), we have $x \in I^*AI^*BI^*$.
- 3) If $v = v'$, then $v \in A \cdot B$ and by rule 1) of Definition 5.4, $v \in C$ and $x \in I^*CI^*$.
- 4) If v is a proper subsequence of v' or vice versa, then v or $v' \in C$ by rule 2) of Definition 5.4, thus $x \in I^*CI^*$.
- 5) If u' is a proper prefix of u and $v' = u''v'' \ni u = u'u''$ and v'' is a proper prefix of v , then $u''v \in C$ and $x = u'u''vw$, thus $x \in I^*CI^*$ by rule 3) of Definition 5.4.
- 6) If u is a proper prefix of u' and $v = u''v'' \ni u' = uu''$ and v'' is a proper prefix of v' then using arguments of 5) we have $x \in I^*CI^*$.

$$\therefore I^*AI^* \cdot I^*BI^* \subseteq I^*AI^*BI^* + I^*BI^*AI^* + I^*BI^*.$$

Conversely, let $x \in$ the right hand side. First let $x \in I^*AI^*BI^*$, i. e. $\exists u, w, z \in I^*, v \in A$ and $y \in B \ni z = uvwyz$. Since $v \in A$, $x \in I^*AI^*$. Similarly $y \in B$ implies $x \in I^*BI^*$. Thus $x \in I^*AI^* \cdot I^*BI^*$. For the case where $x \in I^*BI^*AI^*$ similar reasoning can be used and again $x \in I^*AI^* \cdot I^*BI^*$. Now if $x \in I^*CI^*$, let $x = uvw$, where $u, w \in I^*$, then we consider the following cases:

- 1) If $v \in A \cdot B$, then $x \in I^*(A \cdot B)I^* \subseteq I^*AI^* \cdot I^*BI^*$ by the property of Boolean intersection of regular expressions.

- 2) If $v = v'v''v'''$ where $v', v'', v''' \in I^+$, $v'v'' \in A$ and $v''v''' \in B$, then $u(v'v'')v'''w \in I^*AI^*$ and $uv'(v''v''')w \in I^*BI^*$.
Thus $x \in I^*AI^* \cdot I^*BI^*$.

- 3) If as in 2) $v'v'' \in B$ and $v''v''' \in A$, using the same arguments as in 2), we have $x \in I^*AI^* \cdot I^*BI^*$.

- 4) If $v \in A$ and $v'' \in B$ as in 2), then $x \in I^*AI^*$,
 $x = uv'(v'')v'''w \in I^*BI^*$ and $x \in I^*AI^* \cdot I^*BI^*$.

Similarly if $v \in B$ and $v'' \in A$, $x \in I^*AI^* \cdot I^*BI^*$.

Since we have exhausted all possible situations in $x \in I^*CI^*$ and with the preceding arguments we conclude

$$I^*AI^*BI^* + I^*BI^*AI^* + I^*CI^* \subseteq I^*AI^* \cdot I^*BI^*$$

Thus

$$I^*AI^* \cdot I^*BI^* = I^*AI^*BI^* + I^*BI^*AI^* + I^*CI^*$$

Theorem 5.15 If $M = (I, Q, Z, \delta, \omega)$ is a reduced and strongly connected definite machine, $q \in Q$ and F is a set of q -detectable definite faults, then there exists a non-empty regular set $B \ni$

$$I^*BI^* \subseteq \bigcap_{\mu \in F} \hat{D}(\mu, q)$$

Proof: From Theorem 5.14, $\forall \mu, \gamma \in F$

$$\hat{D}(\mu, q) = D(\mu, q)I^* = A_q^\mu I^* + I^*B_q^\mu I^* \quad (5.133)$$

$$\hat{D}(\gamma, q) = D(\gamma, q)I^* = A_q^\gamma I^* + I^*B_q^\gamma I^* \quad (5.139)$$

Where A_q^μ , B_q^μ , A_q^γ and B_q^γ are finite expressions, and $B_q^\mu \neq \phi$ and $B_q^\gamma \neq \phi$.

$$\begin{aligned}\hat{D}(\mu, q) \cdot \hat{D}(\gamma, q) &= A_q^{\mu \cdot \gamma} I^* + I^* B_q^\mu I^* \cdot I^* B_q^\gamma I^* \\ &= A_q^{\mu \cdot \gamma} I^* + I^* B_q^{\mu \cdot \gamma} I^*\end{aligned}\quad (5.140)$$

where

$$A_q^{\mu \cdot \gamma} I^* = A_q^\mu I^* \cdot I^* B_q^\gamma I^* + A_q^\mu I^* \cdot A_q^\gamma I^* + A_q^\gamma I^* \cdot I^* B_q^\mu I^* \quad (5.141)$$

and

$$I^* B_q^{\mu \cdot \gamma} I^* = I^* B_q^\mu I^* \cdot I^* B_q^\gamma I^* \quad (5.142)$$

Now from Lemma 5.8, it follows that

$$B_q^{\mu \cdot \gamma} \neq \phi \quad (5.143)$$

By induction with repeated application of Lemma 5.8, we have

$$I^* B I^* \subseteq \bigcap_{\mu \in F} \hat{D}(\mu, q)$$

and $B \neq \phi$. B is obtained from Definition 5.4 and Lemma 5.8.

Let us illustrate the above development with the following example.

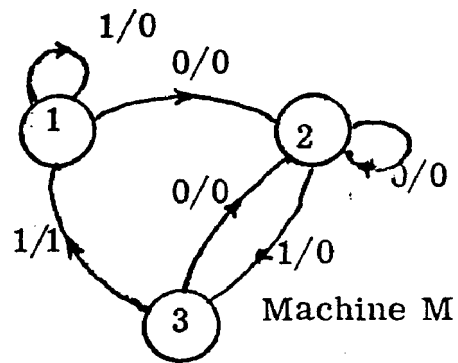
Example 5.5

Consider the machine M and faults μ and μ' of Example 4.1 which are repeated here as shown in Figure 5.4

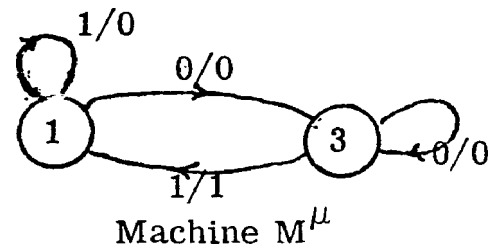
$$\hat{D}(\mu, 1) = I^* 01 I^* \quad (5.144)$$

$$\hat{D}(\mu', 1) = 1 I^* + I^* 111 I^* \quad (5.145)$$

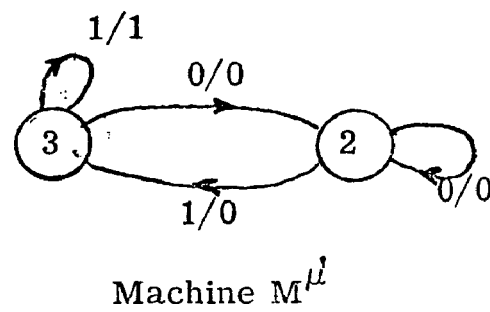
If $F = \{\mu, \mu'\}$, then an $(F, 1)$ -test set can be determined as follows



q	$\mu(q)$
1	1
2	3
3	3

Fault μ 

q	$\mu'(q)$
1	3
2	2
3	3

Fault μ' Figure 5.4 Definite Machine M and Fault set $F = \{\mu, \mu'\}$

$$\begin{aligned}
\hat{D}(\mu, 1) \cdot \hat{D}(\mu', 1) &= I^*01I^* \cdot (1I^* + I^*111I^*) \\
&= 1I^*01I^* + I^*0111I^* + I^*01I^*111I^* \\
&\quad + I^*111I^*01I^* \\
&= 1I^*01I^* + I^*(0111 + 01I^*111 + 111I^*01)I^* \\
&\hspace{15em} (5.146)
\end{aligned}$$

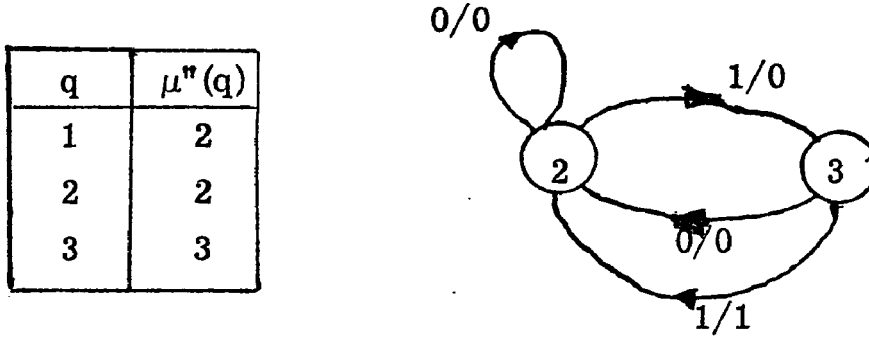
It can be verified that Equation (5.146) is equal to Equation (4.36).

The last term of Equation (5.146) illustrates the form of expression we may obtain for the test set of a set of q -detectable definite faults as prescribed by Theorem 5.15.

Interpreting Theorem 5.15, if F is a set of q -detectable definite faults of a strongly connected definite machine M , for some $q \in Q$, then $\exists$ an (F, q) -test set of the form I^*BI^* for some regular event B . A test set of this form indicates that the test set can be independent of any starting state and from the construction of B by Definition 5.4 and Lemma 5.8, the ordering of faults in the generation of the test set is unimportant. Furthermore, the test set so generated has the property that it has non-empty intersection with any other q -detection sets of faults outside F . Thus potentially many other faults are also detected by this test set. To illustrate these observations, let us consider the following example.

Example 5.6

Consider now a third memory fault μ'' of M of the last example shown in Figure 5.5

Figure 5.5 A Non-definite Fault μ'' of M

$$S_{1,2}^{\mu''} = (1^2)* + I*0(1^2)* \quad (5.147)$$

$$S_{1,2}^{\mu''} = (1^2)*1 + I*0(1^2)*1 \quad (5.148)$$

$$\begin{aligned} T_{1,0}^{\mu''} &= S_{1,2}^{\mu''}I + S_{1,3}^{\mu''}0 \\ &= I*0 + S_{1,2}^{\mu''}1 \\ &= (1^2)*1 + I*[0 + 0(1^2)*1] \end{aligned} \quad (5.149)$$

$$T_{1,1}^{\mu''} = (1^2)*1^2 + I*0(1^2)*1^2 \quad (5.150)$$

Thus from Equations (5.149) and (5.150), μ'' is not definite. Next, let us proceed to compute the 1-detection set of μ'' by first computing the basic 1-detection set of μ'' .

$$\begin{aligned} D(\mu'', 1) &= T_{1,0} \cdot T_{1,1}^{\mu''} + T_{1,1} \cdot T_{1,0}^{\mu''} \\ &= [(1 + 1^2) + I*(0 + 01 + 1^3)] \cdot [(1^2)*1^2 + I*0(1^2)*1^2] \\ &\quad + [I*011] \cdot [(1^2)*1 + I*(0 + 0(1^2)*1)] \\ &= (1^2)*1^2 + I*0(1^2)*1^4 \end{aligned} \quad (5.151)$$

Thus

$$\begin{aligned}
 \hat{D}(\mu'', 1) &= D(\mu'', 1)I^* \\
 &= (1^2)*1^2I^* + I*0(1^2)*1^4I^* \\
 &= 1^2I^* + I*01^4I^*
 \end{aligned} \tag{5.152}$$

Now let us compute a test set for $F' = \{\mu, \mu', \mu''\}$

$$\begin{aligned}
 &\hat{D}(\mu, 1) \cdot \hat{D}(\mu', 1) \cdot \hat{D}(\mu'', 1) \\
 &= [1I*01I^* + I*(01^3 + 01I*1^3 + 1^3I*01)I^*] \cdot [1^2I^* + I*01^4I^*] \\
 &= 1^2I*01I^* + \cancel{1^2I*01^3I^*} + \cancel{1^2I*01I*1^3I^*} + \cancel{1^2I*1^3I*01I^*} \\
 &\quad + 1I*01^4I^* + I*01^4I^* + \cancel{I*01^4I*1^3I^*} + \cancel{I*01^4I*01I^*} + \cancel{I*1^3I*01^4I^*} \\
 &= \cancel{1I*01^4I^*} + 1^2I*01I^* + I*01^4I^* \\
 &= 1^2I*01I^* + I*01^4I^*
 \end{aligned} \tag{5.153}$$

This illustrates the observation that a test set obtained by common intersection of detection sets in a class of q -detectable definite faults has non-empty intersection with the detection set of any other faults including those which are not definite.

It is interesting to note that Equation (5.152) represents a detection set which is identical in form to one obtainable from a definite fault. Moreover, μ'' of Example 5.6 illustrates a class of "easily detectable" faults more general than that of Theorem 5.15. It can be interpreted as saying that in the class of faults F , in order to obtain a test set of the form $I*BI^*$ for some regular event R , all we need is that $\forall \mu \in F$, $D(\mu, q)$ contains a set of sequences of the form $I*R$ where R is a regular event. Thus Theorem 5.15 can be generalized as follows.

Theorem 5.16 Let $M = (I, Q, Z, \delta, \omega)$ be a reduced and strongly connected definite machine, $q \in Q$ and F is a set of q -detectable faults

$\ni \forall \mu \in F$ and $z \in Z$

$$T_{q, z}^{\mu} = R_z^{\mu} + I * S_z^{\mu}$$

where R_z^{μ}, S_z^{μ} are regular sets and $S_z^{\mu} \neq \phi$. Then $\exists$ a non-empty regular set $T \ni$

$$I * T I^* \subseteq \bigcap_{\mu \in F} \hat{D}(\mu, q)$$

Proof: The proof is similar to Theorem 5.15 and we will not elaborate it here.

Let us recall from Definition 5.2 that a machine is definite if there exists an integer k such that for any sequence of length at least k , the future behavior of the machine can be determined. If the machine under consideration is reduced, then this is equivalent to saying that the terminal states of those sequences can be uniquely determined. Such type of sequences is called synchronizing sequence. Rephrasing our observation on the reduced definite machine, we say that a reduced machine is definite (k -definite) if and only if every sequence of length k is a synchronizing sequence. Since in a reduced definite machine almost all sequences are synchronizing sequences (i.e. only a finite number of sequences are not synchronizing sequences), it is reasonable to assume that a large class of faults will somehow preserve the synchronizing property of the machine. Furthermore, the common

intersection of $\hat{D}(\mu, q)$ for $\mu \in F$, a class of such faults, has a non-empty intersection with the q -detection set of any other fault outside of F , it is believed that most faults will be detected by this test set. Thus Theorem 5.16 can be regarded as a theoretical support to the conjecture that definite machines are better for testing and diagnosis.

The last two theorems and the discussion that followed suggest a generalization of definite machine to a class of machines where q -detection sets satisfying Theorem 5.16 are likely to occur. What we want here is a machine where each of its output behavior can be represented as

$$T_{q, z} = A_z + I^*B_z$$

for some regular events A_z and $B_z \neq \phi$. The following theorem provides a sufficient condition for a machine when such property can be obtained.

Theorem 5.17 If $M = (I, Q, Z, \delta, \omega)$ is a reduced, strongly connected and synchronizable machine, then $\forall q \in Q \ni \forall z \in Z$

$$T_{q, z} = A_z + I^*B_z \text{ and } B_z \neq \phi$$

where A_z and B_z are regular expressions.

Proof: Let x be a synchronizing sequence of M and suppose $\forall r \in Q$

$$\bar{\delta}(r, x) = s \quad \text{for some } s \in Q.$$

Choosing any $q \in Q$, since

$$\sum_{r \in Q} S_{q, r} = I^* \quad (5.154)$$

it follows that $I^*x \subseteq S_{q,s}$. Let

$$S_{q,s} = A_s + I^*B_s \quad (5.155)$$

Since M is strongly connected, $S_{s,r} \neq \phi \quad \forall r \in Q$. Now

$$S_{q,r} = S_{q,s} S_{s,r} \quad (5.156)$$

we have

$$I^*B_s S_{s,r} \subseteq S_{q,r} \quad \forall r \in Q$$

Thus $\forall r \in Q$

$$S_{q,r} = A_r + I^*B_r \text{ and } B_r \neq \phi$$

where A_r and B_r are regular expressions. By Equation (4.1), $\forall z \in Z$

$$\begin{aligned} T_{q,z} &= \sum_{\substack{r \in Q, a \in I \\ \ni \omega(r,a)=z}} S_{q,r} a \\ &= A_z + I^*B_z \end{aligned} \quad (5.157)$$

where A_z, B_z are regular expressions and $B_z \neq \phi$, thus completing the proof.

From the previous discussion and the result obtained above, it appears that synchronizability and strongly connectedness contribute significantly to the role of fault detection in sequential machines. Intuitively, synchronizability of a machine reduces the necessity of frequently applying reset input while strongly connectedness amplifies the synchronizability by producing a large number of synchronizing sequences. Thus if a machine fails, the faulty machine will more likely preserve some synchronizability and a large number of faults will satisfy condition of Theorem 5.16.

In summary, Sections 5.3 and 5.4 are mainly devoted to the application of the fault detection concepts and regular representation of fault detection sets as developed in chapter 4 and Section 5.2. These results are indicative of potential application to the study of easily testable sequential machines by means of algebraic representation of their test sets.

Chapter VI

SUMMARY AND CONCLUSIONS

The discussion of the previous chapters is concerned with questions relating to the problem of fault detection and diagnosis of sequential systems. Questions that have been considered or answered include the following:

- i) Investigate properties of sequential machines that relate to "inherent" diagnosability in the sense that the behavior can be easily verified and classify these machines according to some measure of "easiness".
- ii) Determine methods of realizing (simulating) machines (or behaviors) that are not diagnosable by diagnosable machines using augmentation to the specified input-output behavior. By diagnosable, in this context, we mean the machine possesses a distinguishing sequence.
- iii) Given a known set of faults in a machine, determine conditions under which the given machine can be tested against the occurrence of any fault in this set and, if testable, determine optimum test sets.
- iv) Investigate properties of machine structure and behavior that are conducive to efficient fault detection when knowledge of the faulty machine structures is included.

The approach taken in the above investigations has been system theoretic in the sense that a formal model of sequential machine (finite automaton) was used to represent the system and formal methods were used in studying this model. The advantage of this approach in studying system diagnosability is that structure changes (due to faults) can be precisely related to their effects on system behavior, thus permitting the discovery of properties conducive to easy diagnosis independent of any particular physical realization. These investigations will now be summarized.

Chapter 2 began with a review of some basic definitions and concepts of sequential machine theory that relate to the problem of fault detection and diagnosis. When considering procedures for diagnosing faults in sequential systems, such procedures can often be simplified if it is possible to infer the initial state or final state of the system, given the output response to some distinguished input sequences [26]. Thus the properties of interest chosen to answer the first question posed above were the possession of distinguishing sequence and homing sequence and machines having these properties are called diagnosable and homable, respectively. Relative to these classes of machines, two measures of "desirability" of these properties are possible; one is the abundance of such sequences and the other is the length of the shortest such sequences.

The classes of definitely diagnosable (homable) machines [32] where almost all input sequences are distinguishing (homing) sequences were reviewed and studied in Section 2.1. Results obtained in this section include characterizations of a definitely diagnosable machine in terms of being convergence free and definitely homable (Corollary 2.3.2) as well as of being convergence free and having every single-input submachine reduced (Theorem 2.4). These structure characterizations are useful in that they permit generalization of these machines to less restrictive classes of machine without affecting the order of diagnosability (homability), i.e. the length of the shortest distinguishing (homing) sequence remains unchanged. Applications of these results were discussed in Chapter 3 where the purpose was to obtain a diagnosable realization with short distinguishing sequences.

Sequence generators and linear machines when considered as refinements of the definitely diagnosable machines were then discussed (Section 2.2). The order of diagnosability in a reduced sequence generator can be determined by the least integer k such that $\pi_k = \pi_{k+1}$ where π_k is the k -equivalence partition on the state set. Thus optimally diagnosable (i.e. having a distinguishing sequence of the shortest possible length as determined by the number of states and the number of output symbols in a given machine) sequence generators can be characterized in terms of such partitions. The class of reduced linear machines was found to have some common diagnostic properties with that of the reduced sequence generators. First, if a linear machine

has a distinguishing sequence of length k , then every input sequence of length k is a distinguishing sequence. Thus, the order of diagnosability can be determined by the least integer k such that $\pi_k = \pi_{k+1}$. Equivalently, the order of diagnosability can be determined from the least integer k such that the rank of an associated matrix is equal to the dimension of the state space. Consequently a reduced 2^n -state linear machine is definitely diagnosable of order no greater than n . From the known result that i -equivalence relation of a linear machine partitions its state set into cosets when the state space is considered as an Abelian group, it was then shown (Theorem 2.8) that if π_i is the i -equivalence partition of the state space of a linear machine over a Galois field of p^m elements, then $|\pi_{i+1}| = p^{k_i} |\pi_i|$, where $0 \leq k_i \leq \ell m$ and ℓ is the dimension of the output space. Moreover, if n is the dimension of the state space and ℓ divides n , then the linear machine is optimally diagnosable if and only if $|\pi_{i+1}| = q^\ell |\pi_i|$ for all $0 \leq i \leq \frac{n}{\ell}$, where $q = p^m$. Finally, the optimal diagnosable characterization was then generalized to some non-linear sequential machines.

From these discussions, it is evident that the bound on the order of diagnosability is usually dependent on the abundance of the desired sequences. Using this measure as our basis of machine classification, a partially ordered set of these classes of machines using set containment as partial ordering was obtained (Figure 2.3). Such classification is useful in that it permits tradeoffs between hardware complexity and efficiency of diagnostic test during the design stage of a machine.

To answer question ii), three types of machine realizations were considered in Chapter 3 employing control-input augmentation, test-output augmentation and state-output augmentation, respectively.

In the problem of control-input augmentation, it has been shown that diagnosable realizations can always be obtained where the realizing machine has at most one more input symbol than the realized machine. Thus minimum complexity when measured by the number of augmented input symbols is trivially obtainable. Moreover, in all cases one can obtain realizations which are optimal in the sense that they have the shortest possible distinguishing sequence (as determined by the number of states and output symbols).

The problem of test-output augmentation was then considered where the tradeoff between time (length of distinguishing sequence) and space (output alphabet size) was investigated. It has been shown that realizations having distinguishing sequence of length 1 can always be obtained and the best bound on the number of output symbols for such realizations was derived (Theorem 3.4). To obtain a minimum complexity realization, a special class of distinguishing sequences was considered where the restriction is not directly related to the length of the sequences. Such a problem was formulated as that of determining the minimum coloring of a graph and a heuristic procedure was proposed (Procedure 3.1).

To motivate the study of state-output augmentation, it was first shown that it is not possible to obtain a diagnosable realization of any nondiagnosable reduced machine by increasing the number of states alone (Theorem 3.7). The study of output augmentation was generalized to devising methods of obtaining diagnosable realizations which reduce the number of augmented output symbols by increasing the number of states. It has been shown that in many cases it is possible to augment at most one output symbol to obtain a diagnosable realization by sufficiently increasing the number of states (Theorems 3.9, 3.10, 3.14). Means of tradeoffs between the number of states and the number of output symbols were also investigated.

Reviewing major contributions of Chapter 3, the input augmentation method provided a means of achieving an optimal diagnosable realization by increasing the minimum number of external connections. This is important in the case of Large Scale Integrated Circuit (LSIC) design when the number of external pins is a premium limitation. From a network point of view, however, such realizations may require greater network complexity than desired or than required by some other realization techniques. It is believed that any future research in this area would require a redefinition of the measure of machine complexity which also includes some properties of physical networks. In the case of output augmentation, our measure of machine and test complexity in term of the number of output symbols and length of distinguishing sequence, respectively, seem justified because of the well known fact

that points of observation need only very small amounts of logic.

Although we were not able to solve the problem of obtaining a minimum output diagnosable realization, our derivation of best bound for the 1-diagnosable realization and the graphic technique of Procedure 3.1 should provide a foundation for obtaining a reasonably good solution to the output augmentation realization problem. Finally, the state-output augmentation technique provided a tradeoff between the number of test outputs and the complexity of machine in terms of the number of states for obtaining diagnosable realizations. Again, this result is significant in the design of LSIC when the premium limitation is the number of pins and when addition of a moderate number of flip-flops and slight lengthening in test time are acceptable.

The methods discussed above are by no means inclusive. They merely serve to illustrate some basic approaches that may be taken. Using the general concept of diagnosable realization introduced, other feasible techniques can also be investigated. For example, a single input pin feeding an n -stage shift register in a circuit can sometimes be regarded as effectively providing n test pins - an input-state augmentation problem. Similarly, input-output augmentation is usually required when a long chain of counters in a given circuit is to be broken up to reduce the test time. Future research in the design of diagnosable realizations should be beneficial to the derivation of design criteria for easily testable large scale integrated circuits.

Our discussion so far has been limited to the verification of machine behavior without explicitly stating the effects of faults on the fault-free system. Such approach is far too general in most applications, since in practice only much more limited types of faults can occur in a physically realized system. To alleviate this deficiency, the effects of changes in machine structure (due to faults) have been investigated in Chapters 4 and 5 and are now summarized below.

In order to answer question iii), the class of faults considered was restricted to faults which represent permanent changes in the memory structure of the system. This restriction was made primarily to simplify the discussion and the results obtained can be generalized to include any fault which i) does not increase the number of states, and ii) does not affect the reset mechanism. The problem considered then was the representation and minimization of test sets for a sequential system.

The problem of representing detection sequences was considered first and it has been shown that if D is the set of all sequences that distinguish faulty behavior (for a given fault) from fault-free behavior (in a given initial state), then D is a regular set (Theorem 4.2). Moreover, a regular expression that denotes D can be obtained from expression associated with the fault-free and faulty behaviors in much of the same way that test sets are determined for combinational networks using Boolean differences [47].

The problem of obtaining a minimum cost test set (with cost measured in terms of testing time) was then considered where the primary difficulty lies in the fact that detection sets, although regular, are nevertheless infinite. However, we showed that the cost of an optimum (minimum cost) test set is bounded from above by a quantity which depends only on the size of the fault-free machine and the number of faults to be detected (Theorem 4.7). From this it follows that the length of the longest sequence in any minimum cost test set is also bounded by a known quantity. Thus only a finite subset of each fault detection set needs be considered in deriving an optimum test-set. Employing some rather natural notions of fault equivalence and fault dominance, the problem of finding an optimum test set of a sequential machine, given a complete description of the fault set, can then be formulated as a covering problem. This parallels the solution suggested by [28] and others for obtaining optimum test sets.

Although the implementation of these procedures may be impractical for large networks, these results are nevertheless valuable in that they delimit the complexity of the problem. Such solutions may also indicate simpler, more practical methods of solving the problem at some sacrifice in optimality or completeness of the test set.

Chapter 5 was devoted to answering question iv) stated earlier by application of the fault detection concepts and the representation of fault detection sets introduced in Chapter 4. One important subject related to the determination of efficient test sets is the relations of

faults. Fault equivalence relation reduces the number of distinct faults that need to be considered. Similarly fault dominance relation alleviates the necessity of exhaustively computing fault detection set for each fault. To help determine properties of sequential machine desirable for efficient testing, classes of faults which are easily detectable were defined. Machine classes which tend to produce these types of failures were then investigated. These are subjects considered in Chapter 5 and they are briefly summarized below.

The problem of determining fault equivalence and fault dominance relations among faults was first considered. The comparison of these faults was made in terms of componentwise behavior representations of the faulty machines and the fault-free machine. Sufficient conditions for the existence of these relations have been derived but due to the fact that concatenation of regular expression is not distributive over the Boolean operation of set intersection, we were unable to obtain the corresponding necessary conditions. Moreover, if F is a set of faults and $\mathcal{F}$ is the collection of equivalence classes of faults, we were able to establish a sufficient condition for the existence of the greatest lower bound of any two elements in the partially ordered set $(\mathcal{F}, \leq)$. These results are useful in that they may provide shortcuts for computing a test set for any given fault set.

The general problem of investigating properties of easily testable sequential machines using regular expression representation of fault detection sets was then explored. Section 5.3 discussed conditions and

characterizations of memory faults detection in terms of machine structures and nature of faults. Moreover, a class of easily detectable faults has been introduced where the fault detection depends only on the length of the test sequence rather than the choice of sequences. It has been shown that an upper bound on the cost of an optimum test set can be derived which is independent of the size of the fault set.

The class of strongly connected machines was then investigated. In this case we have been able to establish an upperbound on the cost of an optimum test set smaller than that obtainable from the general class of machines (Corollary 5.10.1). If the machine is also diagnosable and the type of faults occurred reduces the number of states in the machine, then it is possible to obtain a test set whose cost is independent of the size of the fault set.

Finally, the class of definite machines was then considered. Due to the widely known property that definite machines can be realized by networks without feedback loop, it has been conjectured that definite machines are easier for fault detection. It is the purpose of this study to formally verify this conjecture. It has been first established that each output behavior of a definite machine can be represented by regular expression of the form $A + I*B$ where A and B are finite expressions and I^* is the set of all possible input sequences to the machine. Moreover, it has been shown that if a fault is also definite, then the basic detection set of that fault can also be represented as a definite event. Such type of faults generally has the property that the common intersection of all

its fault detection sets is non-empty and a test set so obtained either contains or has a non-empty intersection with any other fault detection set outside this given set of faults. Strongly connectedness has been found to be a sufficient condition for the definite machine to have this property when the fault set is definite. Later we have been able to generalize the class of definite faults to the class of faults which preserves some synchronizability of the fault-free machine and essentially obtain the same type of fault detection sets. Since almost all sequences of a reduced definite machine is a synchronizing sequence, it is reasonable to assume that any malfunction particularly of memory type will preserve some degree of synchronizability. With this assumption and the results obtained, it can be concluded that the class of definite machines is "easier" for fault detection.

Fault equivalence and fault dominance relations in combinational networks have been previously investigated by D. Schertz [49] and F. Gray [21] . Their results are useful in fault location (i.e. to determine which physical component or module fails) but appear to be more restrictive than our concepts when only fault detection is concerned. Although fault equivalence relation in sequential machines has been studied by E. J. McCluskey, et al [9] , their findings are mainly extensions of results obtained in combinational networks and as such differ somewhat from our approach taken here. Nevertheless, all these results are important in that they all contribute to the development of an evolving theory of fault diagnosis that further research in this area

is justified. In particular, extension of our research to the study of the partially order set of fault detection sets for a given class of faults (memory faults, stuck-at faults, etc) would probably reveal more fundamental properties of sequential systems that would lead to the quick determination of the set of prime faults, i.e. the set of faults which dominate all other faults in the given set.

The results discussed so far have been applicable to the general model of sequential systems. As any physical realization will definitely constraint its possible behaviors in some way, the characterization and inclusion of these limitations may simplify the problem complexity and possibly result in more fruitful discoveries. For example, the class of definitely detectable faults is very desirable for fault detection. Aside from the rather trivial case of autonomous machines, the question of what classes of machines will have all or most of their physically characterizable faults definitely detectable is very difficult and unresolved. However, for some class of machines where a certain canonical form of realization can be assumed, it is believed that the question can be answered when proper restriction is placed upon the nature of physical failures such as stuck-at failure in some memory elements. The solution of this problem will be useful to the circuit designer who can initially discard the consideration of these faults when determining test set. When the test set is determined for all other types of faults, arbitrary extension of any test sequence to an appropriate length (such as one determined by Theorem 5.8) will be sufficient to complete the test set.

Relative to the problem of behavior verification, it is also possible to consider a more general type of sequences than the distinguishing sequences considered in this study. One such investigation using general compound distinguishing sequences is currently being carried out by L. Hsieh [36]. Such sequences when considered for behavioral augmentation may result in saving on the number of test inputs or outputs that need to be added. However, a more complicated procedure may be required for determining a test set.

Another important unsolved problem is fault detection in redundant systems where some faults are masked purposely to increase system reliability. To detect these masked faults, it is necessary that some additional test inputs or outputs be provided. Relative to the augmented input-output behavior, all faults are then detectable. In this respect, our work on the diagnosable realization of sequential behavior can be extended to the case of redundant machine where there are equivalent states. For example, in the case of memory fault-tolerant realizations [34], the machine behavior can be first made diagnosable using methods proposed in Chapter 3. The equivalent states can then be made distinguishable by providing additional inputs or outputs in a way that does not destroy the diagnosability provided in the first step. Otherwise, methods of diagnosable realizations are again used and the final augmented machine will be diagnosable. This approach, although possible in theory, may not be practical in most cases. Because of the dual nature of fault masking and fault detection, an integrated approach

simultaneously considering fault tolerance for system operation and fault detection for check out would be more desirable. Various aspects of this problem are still being investigated by other researchers (cf [35] and [36]).

References

- [1] Arbib, M. A. , Theories of Abstract Automata, Prentice-Hall, Inc. , Englewood Cliffs, New Jersey, 1969.
- [2] Arden, D. N. , "Delay Logic and Finite State Machines", Proceeding of the Second Annual Symposium on Switching Circuit Theory and Logical Design, 1961, pp. 133-151.
- [3] Armstrong, D. B. , "On Finding a Nearly Minimal Set of Fault Detection Tests for Combinational Logic Nets", IEEE Transactions on Electronic Computers, vol. EC-15, February 1966, pp. 66-73.
- [4] Bennetts, R. B. and D. W. Lewin, "Fault Diagnosis of Digital Systems -a Review", Computer, vol. 4, July/August 1971, pp. 12-21.
- [5] Berlekamp, E. R. , Algebraic Coding Theory, McGraw-Hill Book Company, New York, 1968.
- [6] Berge, C. , The Theory of Graphs and its Applications, Methuen, London, 1962.
- [7] Booth, T. L. , Sequential Machines and Automata Theory, John Wiley and Sons, Inc. , New York, 1968.
- [8] Bouricius, W. G. , E. P. Hsieh, G. R. Putzulu, J. P. Roth, P. R. Schneider and C. -J. Tan, "Algorithms for Detection of Faults in Logic Circuits", IEEE Transactions on Computers, vol. C-20, November 1971, pp. 1258-1264.
- [9] Boute, R. and E. J. McCluskey, "Fault Equivalence in Sequential Machines", Technical Report No. 15, Stanford Electronic Laboratories , Stanford University, Stanford, California, June 1971.
- [10] Breuer, M. A. , "A Random and An Algorithmic Technique for Fault Detection Test Generation for Sequential Circuits", IEEE Transactions on Computers, vol. C-20, November 1971, pp. 1364-1370.
- [11] Brzozowski, J. A. , "A Survey of Regular Expressions and their Applications", IRE Transactions on Electronic Computers, vol. EC-11, 1962, pp. 324-335.
- [12] Brzozowski, J. A. , "Canonical Regular Expressions and Minimal State Graphs for Definite Events", Proceedings of the Symposium on the Mathematical Theory of Automata, New York, 1962, pp. 529-561.

- [13] Chang, H. Y. , "An Algorithm for Selecting an Optimum Set of Diagnostic Tests ", IEEE Transactions on Electronic Computers, vol. EC-14, October 1965, pp 706-711.
- [14] Chang, H. Y. , E. G. Manning and G. Metze, Fault Diagnosis of Digital Systems, John Wiley and Sons, Inc. , New York, 1970.
- [15] Cohn, M. and S. Even, "Identification and Minimization of Linear Machines", IEEE Transactions on Electronic Computers, vol. EC-14, 1965, pp. 367-376.
- [16] Galey, J. M. , R. E. Norby and J. P. Roth, "Techniques for the Diagnosis of Switching Circuit Failures", IEEE Transactions on Communication and Electronics, 33(74), 1964, pp. 509-514.
- [17] Gelenbe, S. E. , "Regular Expressions and Checking Experiments", Report PIBMRI-1378-67, Polytechnic Institute of Brooklyn, Brooklyn, New York, September, 1967.
- [18] Gill, A. , Introduction to the Theory of Finite-State Machines, McGraw-Hill Book Company, N. Y. , 1962.
- [19] Ginsburg, A. , Algebraic Theory of Automata, Academic Press, New York, 1968.
- [20] Golomb, S. W. , L. D. Baument, M. F. Easterling, J. J. Stiffler, and A. J. Viterbi, Digital Communications, Prentice-Hall, Inc. , Englewood Cliffs, New Jersey, 1969.
- [21] Gray, F. G. , "Fault Tolerance, Detection and Location in Abstract Networks", Ph. D. Dissertation, The University of Michigan, Ann Arbor, Michigan, 1971.
- [22] Gray, F. G. and J. F. Meyer, "Locatability of Faults in Combinational Networks", IEEE Transactions on Computers, vol. C-20, November 1971, pp. 1407-1412.
- [23] Harary, F. , Graph Theory, Addison-Wesley, Reading, Mass. , 1969.
- [24] Hartmanis, J. and R. E. Stearns, Algebraic Structure Theory of Sequential Machines, Prentice-Hall, Inc. , Englewood Cliffs, N. J. , 1966.
- [25] Hennie, F. C. , Finite-State Models for Logical Machines, John Wiley and Sons, Inc. , New York, 1968.
- [26] Hennie, F. C. , "Fault Detection Experiments for Sequential Circuits", Proceedings of the Fifth Annual Switching Theory and Logical Design Symposium, vol. S-164, 1964, pp. 95-110.

- [27] Karp, R. M. , Selected Topics in Automata Theory, Report No. RADC-TR-68-106, System Engineering Laboratory, The University of Michigan, Ann Arbor, Michigan, 1968.
- [28] Kautz, W. H. , "Fault Testing and Diagnosis in Combinational Digital Circuits", IEEE Transactions on Computers, vol. C-17, April 1968, pp. 352-366.
- [29] Kime, C. R. , "An Organization for Checking Experiments on Sequential Circuits", IEEE Transactions on Electronic Computers, vol. EC-15, Feb. 1966, pp. 113-115.
- [30] Kohavi, Z. , Switching and Finite Automata Theory, McGraw-Hill Book Company, New York, 1970.
- [31] Kohavi, I. and Z. Kohavi, "Variable Length Distinguishing Sequences and Their Application to the Design of Fault Detection Experiments", IEEE Transactions on Computers, vol. C-17, August 1968, pp. 792-795.
- [32] Kohavi, Z. and P. Lavalley, "Design of Sequential Machines with Fault Detection Capabilities", IEEE Transactions on Electronic Computers, vol. EC-16, August 1967, pp. 473-484.
- [33] Kubo, H. , "A Procedure for Generating Test Sequences to Detect Sequential Circuits Failures", NEC Research and Development No. 12, October 1968, 69-78.
- [34] Meyer, J. F. , "Fault Tolerant Sequential Machines", IEEE Transactions on Computers, vol. C-20, October 1971, pp. 1167-1177.
- [35] Meyer, J. F. , F. G. Gray and K. Yeh, "Theory and Design of Reliable Spacecraft Data Systems", Final Report, Jet Propulsion Laboratory, California Institute of Technology, Pasadena, California, Sept. 1970.
- [36] Meyer, J. F. , L. Hsieh and K. Yeh, "Theory of Reliable Systems", Semi Annual Status Report, NASA Research Grant NGR23-005-463, System Engineering Laboratory, The University of Michigan Ann Arbor, Michigan, February 1972.
- [37] Meyer, J. F. and K. Yeh, "Diagnosable Machine Realizations of Sequential Behavior", Digest of 1971 International Symposium on Fault-Tolerant Computing, March 1971, pp. 22-25.
- [38] Meyer, J. F. and B. P. Zeigler, "On the Limit of Linearity", Theory of Machines and Computations (Edited by Z. Kohavi and A. Paz), Academic Press, New York, 1971, pp. 229-241.

- [39] Miller, R. E. , Switching Theory, vol. 2, John Wiley and Sons, Inc. , New York, 1966.
- [40] Moore, E. F. , "Gedanken Experiments on Sequential Machines", Automata Studies 34, Princeton University Press, Princeton, New Jersey, 1956, pp. 129-153.
- [41.] Murakami, S. , K. Kinoshita and H. Ozaki, "Sequential Machines Capable of Fault Diagnosis", IEEE Transactions on Computers, vol. C-19, November 1970, pp. 1079-1085.
- [42] Peterson, W. W. , Error Correcting Codes, John Wiley and Sons and MIT Press, New York, 1961.
- [43.] Poage, J. F. , "Derivation of Optimum Tests to Detect Faults in Combinational Circuits", Proceedings of 1963 Symposium on Mathematical Theory of Automata, 1963, pp. 483-528.
- [44] Putzolu, G. R. and J. P. Roth, "A Heuristic Algorithm for the Testing of Asynchronous Circuits", IEEE Transactions on Computers, vol. C-20, June 1971, pp. 639-647.
- [45] Roth, J. P. , "Diagnosis of Automata Failures A Calculus and Mehtod", IBM Journal of Research and Development, July 1966, pp. 278-291.
- [46] Roth, J. P. , W. Bouricius and P. R. Schneider, "Programmed Algorithm to Compute Tests to Detect and Distinguish between Failures in Logic Circuits", IEEE Transactions on Electronic Computers, vol. EC-16, October 1967, pp. 567-580.
- [47] Sellers, F. F. , M. Y. Hsiao and L. W. Bearson, "Analyzing Errors with the Boolean Difference", IEEE Transactions on Computers, vol. C-17, July 1968, pp. 676-683.
- [48] Seshu, S. and D. N. Freeman, "The Diagnosis of Asynchronous Sequential Switching Systems", IRE Transactions on Electronic Computers, vol. EC-11, August 1962, pp. 459-465.
- [49] Shertz, D. R. , "On the Representation of Digital Faults", Coordinated Science Laboratory, University of Illinois Report R-418, May 1969.
- [50] Short, R. A. , "The Attainment of Reliable Digital System Through the Use of Redundancy-a Survey", Computer Group News, March 1968, pp. 2-17.

- [51] Tsiang, S. H. and W. Ulrich, "Automatic Trouble Diagnosis of Complex Logic Circuits", Bell System Technical Journal, vol. 41, July 1962, pp. 1177-1200.