Quarterly Progress Report 5
Covering the Period 10 February to 9 May 1970
The University of Michigan Project 62802
Jet Propulsion Laboratory Contract 952492

THEORY AND DESIGN OF
RELIABLE SPACECRAFT DATA SYSTEMS

Project Director
J. F. Meyer

Prepared for:
Jet Propulsion Laboratory
4800 Oak Grove Drive
Pasadena, California
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. Objectives</td>
<td>1</td>
</tr>
<tr>
<td>II. Personnel</td>
<td>3</td>
</tr>
<tr>
<td>III. Summary of Technical Status</td>
<td>4</td>
</tr>
<tr>
<td>IV. Technical Progress Report</td>
<td>11</td>
</tr>
<tr>
<td>Permanent Memory Faults</td>
<td>12</td>
</tr>
<tr>
<td>Fault Location in Combinational Networks</td>
<td>36</td>
</tr>
<tr>
<td>Fault Diagnosis</td>
<td>51</td>
</tr>
<tr>
<td>References</td>
<td>68</td>
</tr>
</tbody>
</table>
I. OBJECTIVES

The long range objective of this project, as described in the Statement of Work (Article I, JPL Contract No. 952492) is to conduct a study of theory and techniques applicable to the design, analysis and fault diagnosis of reliable spacecraft data systems. In accomplishing this effort, the investigation will be concerned with the following problems:

(A) Design and analysis of redundant combinational and sequential networks. This shall include the development of mathematical models for the study of temporary and permanent faults in switching networks, the results having application to the design of ultrareliable subsystems of the type prevalent in existing science data systems such as counters, sequence generators for timing and encoding, analog-to-digital converters and scratchpad memories. Explore in detail errors which result from permanent malfunctions of memory in sequential switching systems.

(B) Fault diagnosis of redundant systems at both the component and subsystem level. This shall include investigating the problem of specifying test and checkout procedures for systems in which the reliability has been enhanced using redundancy techniques which mask internal faults. Specific areas to be investigated shall include:
(i) Development of efficient diagnostic algorithms for sequential switching networks which contain redundancy.

(ii) Development of theory and techniques for determining test-point allocation in order to reduce the time (relative to input/output testing) needed to isolate and locate faults.

(iii) Investigate questions relating to how a data system should be organized to best facilitate both pre-flight and in-flight fault diagnosis.
II. PERSONNEL

The principal investigator on the project is Professor John F. Meyer, Department of Electrical Engineering and Department of Computer and Communication Sciences, the University of Michigan. Three Research Assistants; Mr. F. Gail Gray, Mr. John R. Kinkel, and Mr. Koumin (Ken) Yeh have been working half-time on the project during the past quarter.
III. SUMMARY OF TECHNICAL STATUS

During the past quarter, investigations have continued with regard to the following three problems:

1) Permanent memory faults,
2) Faults in combinational networks, and
3) Fault diagnosis.

The technical status of each of these investigations is summarized briefly in the paragraphs that follow. Also included is a discussion of planned efforts for the next quarter. A detailed technical report on each of these studies is contained in the body of this report (Section IV).

Permanents Memory Faults

In the previous Quarterly Progress Report the effect of the set of faults $S_n(k;q)$ on the index set of coordinates $H(q,q')$ was investigated. From information about the distribution of faults and fault states the initial conditions for initial state fault masking were obtained.

In this report methods are developed for analyzing a state-assigned machine $M$ in terms of the faulty machines $M^\mu$, where $\mu$ is a stuck-at fault of degree $k$ or less. These methods are based on the relation

$U_\mu = \{ (\bar{\delta}(q_0,x), \bar{\delta}^\mu(\mu(q_0),x)) | x \in \Gamma^* \}$ introduced in QPR4. In that report $U_\mu \subseteq \equiv_1$ was shown to be a necessary and sufficient condition for $q_0$-masking the fault $\mu$ ($\equiv_1$ denotes the output equivalence relation in a Mealy machine). This result is immediately extended to obtain a relation $U_k$ such that $U_k \subseteq \equiv_1$ is necessary and sufficient for $q_0$-masking all $\mu \in S_n[k]$. 


The relations \( U_\mu \) and \( U_k \) are then used to define state sets \([q]_\mu\)
and \([q]\) respectively. For \( q \) a state reachable from \( q_0 \) in \( M \), \([q]_\mu\)
is the set of states \( q' \) such that \( q U_\mu q' \). \([q]\) is similarly defined in
terms of \( U_k \). The sets \([q]_\mu\) are a link between \( M_R \) – the reduced machine
representing the behavior to be realized – and a machine \( M \) of dimension
\( n \) that realizes the desired behavior and \( q_0 \)-masks all \( \mu \in S_n[k] \).

Equivalence relations \( \sim_\mu \) and \( \sim \) are defined on the sets of right relatives
\([q]_\mu\) and \([q]\) respectively. It is shown that if \( M \) is a machine such that
\( \mu \) is \( q_0 \)-masked for all \( \mu \in S_n[k] \), then for all states \( q_1, q_2 \) reachable
from \( q_0 \) the existence of a fault \( \mu \in S_n[k] \) such that \([q_1]_\mu \sim [q_2]_\mu\)
implies \([q_1] \sim [q_2]\).

The report concludes with two methods for relating the machines
\( M^\mu \), in terms of the sets \([q]_\mu\), to the machine \( M \). It is shown that
the transition function for a state-assigned machine \( M \) can be derived
from information about the commonality of states in the sets \([q]_\mu\).

The problem of classifying states to obtain the sets \([q]_\mu\) requires
further investigation; classification procedures in conjunction with the
observations of this report can lead directly to the synthesis of machines
for \( q_0 \)-masking. Another problem we want to investigate is the question
of optimal realizations. For some behavior \( \beta \), we say that an \( n \)-dimen-
sional state-assigned machine \( M = (I, Q, O, \delta, \omega) \) is a \( t \)-tolerant realization
of \( \beta \) if there exists \( q_0 \in Q \) such that \( \beta_{q_0} = \beta \) and \( \mu \) is \( q_0 \)-masked for all
\( \mu \in S_n[t] \). An \( n \)-dimensional \( t \)-tolerant realization is optimal if there
is no \( t \)-tolerant realization of \( \beta \) having lower dimension than \( n \). The
optimal dimension for a given behavior is a measure of the tolerance of the behavior to faults and is an open question. It may be possible to find some answers to this question prior to the discovery of general synthesis procedures.

Faults in Combinational Networks

The purpose of this investigation is to formalize the concepts of fault-masking, detection, location, and diagnosis as applied to combinational networks in a way that will allow efficient analysis and economical synthesis of redundant fault-tolerant switching networks. It is expected that fundamental relationships between these concepts and basic limitations on their applicability will emerge from this study.

In the first annual report, a model was introduced to describe these concepts. Faults were classified as masked, detectable, or locatable according to implications that arose as a result of observing the system behavior \( \alpha(f) \). A fault \( f \) is masked if \( \alpha(f) \) is the fault-free behavior of the system and detectable otherwise. A fault \( f \) is locatable if the set of faulty nodes can be deduced when the system behavior \( \alpha(f) \) is observed. Finding that the notion of a fault being locatable is very restrictive, a more general concept of location was introduced, namely a fault \( f \) is \([B, A]\)-locatable if the system behavior \( \alpha(f) \) implies that all nodes in the set \( B \) are faulty and that all faulty nodes are contained in the set \( A \).
The basic approach being used to analyze networks with single faults is first to investigate the properties of a two-node series system and then to generalize these results for larger systems. In particular, we have developed a three-node series parallel network (called the general system form) which is universally applicable to the analysis of any system.

As described in QPR4, the concepts of a single masked fault and a single detectable fault are easily characterized in set-theoretic notation. Using these characterizations, one can enumerate the number of single masked faults and the number of single detectable faults in an arbitrary combinational network wholly in terms of properties of the fault-free system structure. A procedure was developed to generate a list of all such masked faults. The enumeration of locatable faults will be studied in the next quarter.

Necessary and sufficient conditions for masking and for detecting all single faults at a node in an arbitrary system were also described in QPR4. These conditions indicate that the input stages of a system are more restrictive to fault detection than are the output stages; whereas output stages are more restrictive for fault masking. The network requirements for all single faults to be locatable in a two-node system were found to be very restrictive. The generalization to larger systems has not yet been solved, and some effort in this direction is planned for the next quarter.
Due to the apparent severe restrictions imposed by locatable faults, the study of \([B,A]\)-locatable faults was emphasized during the past quarter. In QPR4, it was proven that if a fault is \([B,A]\)-locatable and if \([B',A'] \subseteq [B,A]\), then the fault is also \([B',A']\)-locatable. Since the smallest interval, \([B,A]\), for which a fault is \([B,A]\)-locatable represents the most information about the fault that can be obtained from observation of system behavior, this interval is known as the locatability of the fault. We now can state that locatability is an invariant of \(\alpha\) where \(\alpha\) is the system net mapping. (See QPR4, page 142, for definition of net mapping.) An interesting consequence of this result, is that if any masked fault is \([B,A]\)-locatable, then all masked faults must be \([B,A]\)-locatable. Stated another way, if a masked fault is \([B,A]\)-locatable, then all faults whose set of faulty nodes is not a subset of \(A\) must be detectable. We now see that in order to improve the locatability of masked faults, we must reduce the potential size of the set of masked faults, and, conversely to make possible the masking of more faults, we must reduce their locatability.

In general, a fault can be \(K_f\)-locatable but not locatable. However, a single detectable fault is locatable if and only if it is \(K_f\)-locatable. In QPR4, necessary and sufficient conditions for a single fault at node 2 in a general system form to be \([2]\)-locatable (and hence locatable) were stated. We can now state the requirements for a masked fault to be \([2]\)-locatable, namely (1) \(2^1b_1\) is onto \(W \times U\) and (2) \(|[b_1[x],b_3,b_2]| = 1\),
for all $x \in X$. From the above statement concerning masked faults, these are also the requirements for all masked faults to be $\{2\}$-locatable. (No proper masked fault is locatable.)

One of the most important applications of the present theory is to the design of fault-tolerant switching systems. In QPR4, optimum two-node parameters were derived that maximize the percentage of node 1 faults masked over all two node realizations of a given net function. During the next quarter, this result will be generalized to find parameters that maximize the percentage of all faults masked in a two-node system. In particular, the special case of stuck-at faults will be studied.

**Fault Diagnosis**

Some properties of linear machines relating to machine diagnosis have been investigated during the past quarter. First, it has been shown that the $i$-equivalence relation on a linear machine partitions its state set into cosets when the state space is considered as an additive abelian group. Based on this observation, it is shown then that if $\pi_i$ is the $i$-equivalence partition of the state set of a linear machine $M$ over a Galois field of $p^m$ elements, then $|\pi_{i+1}| = p^{k_i}|\pi_i|$ with $0 \leq k_i < \ell m$, where $\ell$ is the dimension of the output space. If $n$ is the dimension of the state space and $\ell$ divides $n$, then $M$ is optimally diagnosable if and only if $|\pi_{i+1}| = q^{\ell}|\pi_i|$ for all $0 \leq i < \frac{n}{\ell}$, where $q = p^m$. The optimal diagnosable characterization is then generalized to some non-linear sequential machines.
In the network diagnosis area, the concept of path sensitizing has been extended to subgraphs where every path is a sensitized path. The notion of "node detection" under some network input $x$ has been found to be a partial ordering of the node set of the sensitized subgraph. This ordering has been applied to obtain properties for the notion of fault detection by a node. Using these results and the concept of multiple faults detection, it is then shown that the set of stuck-at faults in a sensitized path detected by a node under some network input is also multiply detected by the same node under the same input.

If the network graph is a tree, then in a rooted sensitized subgraph, any combination of "singly" detected stuck-at faults is also multiply detected by the "root" node under the sensitizing input.

Plans for the next quarter include the study of sequential machine decomposition into maximal linear submachines or shift register realizable submachines so that diagnosing experiments can be easily implemented. They also include the application of "node detection" and "fault detection" concepts to analysis of redundant networks for test points selection.
IV. TECHNICAL PROGRESS REPORT

The following is a technical progress report on the research activity of the past quarter. Investigations during this period were concerned with the three problem areas summarized in Section III: 1) permanent memory faults, 2) fault location in combinational networks and 3) fault diagnosis.

As in QPR4, the report includes proofs of all theorems as well as a cohesive discussion of concepts, results, motivation, and interpretation. Examples are also included to illustrate key points.
1. PERMANENT MEMORY FAULTS

Much of the terminology of this report—e.g. \( q_0 \)-masking, stuck-at faults, state-assigned machines, and autonomous machines—was introduced formally in QPR4. To facilitate reading this report we review briefly the essential terminology and results of that report.

If \( \mu \) is a fault of a machine \( M \) with states \( Q \) and \( R \subseteq Q \), then \( \mu \) is \( R \)-masked if

\[
\beta_{\mu}^R(r) = \beta_r, \quad \text{for all } r \in R
\]

where \( \beta_{\mu}^R \) is the behavior of \( M^\mu \) for initial state \( q \). In particular, if \( M \) has a distinguished reset state \( q_0 \) and the only behavior of interest is the input-output function that results when the system is initially in the reset state, we let \( R = \{q_0\} \).

We consider \( q_0 \)-masking in the context of state-assigned machines and stuck-at faults. \( M \) is state-assigned if the states of \( Q \) are binary \( n \)-tuples; the integer \( n \) is called the dimension of \( M \). We say \( \mu \) is a stuck-at fault, if for all \((b_1, b_2, \ldots, b_n) \in Q \)

\[
\mu(b_1, b_2, \ldots, b_n) = (\mu_1(b_1), \mu_2(b_2), \ldots, \mu_n(b_n))
\]

where \( \mu_i = \sigma_0 \) if \( i \)-th coordinate is stuck-at 0 (sa 0) and if \( \mu_i = \sigma_1 \) if \( i \)-th coordinate is stuck-at 1 (sa 1). The degree \( d(\mu) \) of \( \mu \) is the number of coordinates which are sa 0 or sa 1. For \( S_n \), the set of stuck-at faults of an \( n \)-dimensional state-assigned machine, we define the subsets:

\[
S_n(k) = \{ \mu \in S_n \mid d(\mu) = k \}
\]
\[ S_n(k; q) = \{ \mu \in S_n(k) \mid \mu(q) = \hat{q} \} \]

\[ S_n[k] = \bigcup_{t=0}^{k} S_n(t). \]

The problem, then, is to design a state-assigned machine which realizes some specified behavior \( B \) and for some set of stuck-at faults \( F \), \( \mu \) is \( q_0 \)-masked for all \( \mu \in F \). We want to ensure that \( B \) is a machine realizable behavior so we may assume that \( B \) is specified by a reduced machine \( M' \) such that \( B_{M'} = B \).

A class of machines which possess a well-defined structure for analysis are the autonomous machines or one-input sequence generators. The state diagram of an autonomous machine with initial state consists of a loop with a tail segment that connects the initial state and loop. We consider machines with tails of any length, but with an output sequence which is periodic from the initial state. We say an output sequence has period \( p \) if there is a sequence from \( \{0, 1\} \) of length \( p \) with no proper subperiods.

In QPR4 relationships between \( H(q, q') \) and \( S_n(k; q) \) were found and applied to the problem of \( q_0 \)-masking. \( H(q, q') \) denotes the set of coordinate indices for which the coordinates of \( q \) and \( q' \) are different, that is

\[ H(q, q') = 1(q) \oplus 1(q') \]

where \( \oplus \) is symmetric difference. From

\[ H(q, \mu(q')) = H(q, q') \cap X(\mu) \]
we found that the number of fault states $\mu(q')$ z-distant from q is $\binom{y}{z}$ where $h(q, q') = z$ and $\mu \in S_n(k; q)$. The number of faults from $S_n(k; q)$ with $s$—one of the $\binom{y}{z}$ fault states—in the range is $\binom{n-y}{n-(k+z)}$. From these results the initial conditions for $q_0$-masking were obtained:
each of the $\binom{n}{y}$ initial fault states $y$-distant from $q_0$ is in the range of $\binom{n-y}{k-y}$ faults from $S_n(k)$.

In this report we want to analyze the machines $M^\mu$, $\mu \in S_n[k]$, to determine the structure of transition functions which $q_0$-mask faults in $S_n[k]$. An understanding of this structure will permit the derivation of transition functions for $M$ given the behavior to be realized. Our analysis begins by repeating the definition of a relation (formerly denoted $\mu_{q_0}$) defined in QPR4.

**Definition 1.1**

For $\mu$ a fault of $M$,
\[
U_\mu = \{(\delta(q_0, x), \delta^\mu(\mu(q_0), x)) | x \in I^*\}.
\]

The importance of this relation arises from the result (Theorem 4/1.7) that $\mu$ is $q_0$-masked iff $U_{\mu} \subseteq \equiv_1 (M \text{ a Mealy machine}),$ that is iff
\[
\delta(q_0, x) \equiv_1 \delta^\mu(\mu(q_0), x), \text{ for all } x \in I^*.
\]

For all $q \in Q_0$, the set of states reachable from $q_0$,
\[
Q_0 = \{ q | \delta(q_0, x) = q, x \in I^* \}
\]

let $[q]_\mu$ denote the set of right relatives of $q$ in $U_{\mu}$, that is
\[
[q]_\mu = \{ q' | q \in U_{\mu} q' \}.
\]
This set contains all states reachable from $\mu(q_0)$ in $M^\mu$ under an input sequence that takes $M$ from $q_0$ to $q$.

**Lemma 1.1**

For $q \in Q_0$, $\mu$ is $q_0$-masked iff

$q' \in [q]_\mu \implies \beta^\mu_{q'} = \beta_{q^*}$

**Proof** Necessity:

Suppose $q' \in [q]_\mu$, then there exists $x \in I^*$ such that

$q = \delta(q_0, x)$

$q' = \delta^\mu(q_0), x)$.  

But $\mu$ is $q_0$-masked which says

$\beta^\mu_{\mu(q_0)} = \beta_{q_0}$

and implies

$\beta^\mu_{\delta^\mu(q_0), y} = \beta_{\delta(q_0), y}$, $\forall y \in I^*$.  

In particular, when $y=x$ we have

$\beta^\mu_{q'} = \beta_{q^*}$

**Sufficiency:**

Let $q = q_0$, then

$\mu(q_0) \in [q_0]_\mu \implies \beta^\mu_{\mu(q_0)} = \beta_{q_0}$

and $\mu$ is $q_0$-masked by definition. This concludes the proof.
Clearly, all the states in $[q]_\mu$ are equivalent in $M^\mu$ if $\mu$ is $q_0$-masked.

To clarify the preceding discussion consider the following example.

Example 1.1

For the periodic output sequence 0101... let $M$ be a state-assigned Mealy machine of dimension 3 which realizes this behavior from $q_0 = 000$.

<table>
<thead>
<tr>
<th>Q \ I</th>
<th>$\delta(q, a)/\omega(q, a)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>101/0</td>
</tr>
<tr>
<td>001</td>
<td>010/1</td>
</tr>
<tr>
<td>010</td>
<td>111/0</td>
</tr>
<tr>
<td>011</td>
<td>000/1</td>
</tr>
<tr>
<td>$M$:</td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>010/1</td>
</tr>
<tr>
<td>101</td>
<td>000/1</td>
</tr>
<tr>
<td>110</td>
<td>111/0</td>
</tr>
<tr>
<td>111</td>
<td>101/1</td>
</tr>
</tbody>
</table>

Let $\mu$ be the fault denoted in cubical notation by $\mu = 0xx$ ($\mu \in S_3(1)$), that is

<table>
<thead>
<tr>
<th>q</th>
<th>$\mu(q)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>000</td>
</tr>
<tr>
<td>001</td>
<td>001</td>
</tr>
<tr>
<td>010</td>
<td>010</td>
</tr>
<tr>
<td>011</td>
<td>011</td>
</tr>
<tr>
<td>100</td>
<td>000</td>
</tr>
<tr>
<td>101</td>
<td>001</td>
</tr>
<tr>
<td>110</td>
<td>010</td>
</tr>
<tr>
<td>111</td>
<td>011</td>
</tr>
</tbody>
</table>
The machine $M$ under the fault $\mu$ has the transition table

<table>
<thead>
<tr>
<th>$Q \backslash I$</th>
<th>$\delta^\mu(\mu(q), a)/\omega(\mu(q), a)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>001/0</td>
</tr>
<tr>
<td>001</td>
<td>010/1</td>
</tr>
<tr>
<td>010</td>
<td>011/0</td>
</tr>
<tr>
<td>011</td>
<td>000/1</td>
</tr>
<tr>
<td>100</td>
<td>001/0</td>
</tr>
<tr>
<td>101</td>
<td>010/1</td>
</tr>
<tr>
<td>110</td>
<td>011/0</td>
</tr>
<tr>
<td>111</td>
<td>000/1</td>
</tr>
</tbody>
</table>

Using decimal equivalents of the binary 3-tuples to denote states and beginning with $q_0 = 0$, the sequence of states is $0, 5, 0, 5, \ldots$ in $M$ and $0, 1, 2, 3, 0, 1, 2, 3, \ldots$ in $M^\mu$, so

$$U_\mu = \{(0, 0), (5, 1), (0, 2), (5, 3)\}.$$

The output equivalence relation is

$$=_1 = \{0, 2, 6; 1, 3, 4, 5, 7\}$$

and since $U_\mu \subseteq =_1$, $\mu$ is $q_0$-masked. The sets of right relatives are

$$[0]_\mu = \{0, 2\}; \quad [5]_\mu = \{1, 3\}$$

and the state equivalences $0 \equiv_1 2$ and $1 \equiv_1 3$ are easily verified.

Suppose now that $M$ is a state-assigned machine of dimension $n$ and let $U_k$ denote the union of the relations $U_\mu, \mu \in S_n[k]$, i.e.

$$U_k = \bigcup_{\mu \in S_n[k]} U_\mu.$$  \hspace{1cm} (1.2)

Then by Theorem 4/1.7 it is immediate that
Theorem 1.1

If \( M \) is a Mealy machine

\[ \mu \text{ is } q_0 \text{-masked, } \forall \mu \in S_n[k] \text{ iff } U_k \subseteq \equiv_1. \]

In general \( U_k \) is neither symmetric nor transitive. However, if we let \( E_k \) denote the symmetric, transitive closure of \( U_k \), i.e.

\[ E_k = \{(q, q') \mid \text{there exist } q_1 = q, q_2, \ldots, q_m = q' \text{ such that } q_iU_kq_{i+1} \text{ or } q_{i+1}U_kq_i, i=1, 2, \ldots, m-1\} \]

we obtain

Corollary 1.1.1

If \( M \) is a Mealy machine

\[ \mu \text{ is } q_0 \text{-masked, } \forall \mu \in S_n[k] \text{ iff } E_k \subseteq \equiv_1. \]

Proof

Necessity:

\( E_k \) is the smallest equivalence relation containing \( U_k \). Since \( \equiv_1 \) is also an equivalence relation containing \( U_k \), it must contain \( E_k \).

Sufficiency: Obvious.

According to the corollary there is some flexibility in the choice of behavior for \( M \) as long as the partition defined by \( E_k \) refines the output partition.

In conjunction with the relation \( U_k \) we introduce \( [q] \), where

\[ [q] = \bigcup_{\mu \in S_n[k]} [q]_{\mu} = \{q'| qU_k q'\}. \] (1.3)
Note that $q \in [q]$ since $\iota$—the identity function on $Q$—is in $S_n[k]$.

Each state of $[q]$ is a state of one or more faulty machines, $M^\mu$, $\mu \in S_n[k]$.

The following example should help to clarify the definitions of $U_k$, $E_k$, and $[q]$ and Theorem 1.1.

**Example 1.2**

For the periodic output sequence 0101 ... let $M$ be a 3 dimensional state-assigned Mealy machine which realizes this sequence beginning with $q_0 = 0$. Let the set of faults be $S_3(1)$ consisting of

- $\mu_1 = xx1$
- $\mu_2 = xx0$
- $\mu_3 = x1x$
- $\mu_4 = x0x$
- $\mu_5 = 1xx$
- $\mu_6 = 0xx$.

The transition function for $M$ and the faulty machines $M^\mu$ is given by the following table; the entry in row $q$ is $\delta(q,a)/\omega(q,a)$ for $M$ and $\delta^\mu(\mu(q),a)/\omega(\mu(q),a)$ for $M^\mu$.

<table>
<thead>
<tr>
<th>$Q \setminus I$</th>
<th>$\delta$</th>
<th>$\delta_1$</th>
<th>$\delta_2$</th>
<th>$\delta_3$</th>
<th>$\delta_4$</th>
<th>$\delta_5$</th>
<th>$\delta_6$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>7/0</td>
<td>3/0</td>
<td>6/0</td>
<td>7/0</td>
<td>5/0</td>
<td>6/0</td>
<td>3/0</td>
</tr>
<tr>
<td>1</td>
<td>3/0</td>
<td>3/0</td>
<td>6/0</td>
<td>3/0</td>
<td>1/0</td>
<td>4/1</td>
<td>3/0</td>
</tr>
<tr>
<td>2</td>
<td>7/0</td>
<td>1/0</td>
<td>6/0</td>
<td>7/0</td>
<td>5/0</td>
<td>4/1</td>
<td>3/0</td>
</tr>
<tr>
<td>3</td>
<td>1/0</td>
<td>1/0</td>
<td>6/0</td>
<td>3/0</td>
<td>1/0</td>
<td>4/1</td>
<td>1/0</td>
</tr>
<tr>
<td>4</td>
<td>6/0</td>
<td>5/1</td>
<td>6/0</td>
<td>2/1</td>
<td>4/0</td>
<td>6/0</td>
<td>3/0</td>
</tr>
<tr>
<td>5</td>
<td>4/1</td>
<td>5/1</td>
<td>6/0</td>
<td>2/1</td>
<td>4/1</td>
<td>4/1</td>
<td>3/0</td>
</tr>
<tr>
<td>6</td>
<td>0/1</td>
<td>1/1</td>
<td>0/1</td>
<td>2/1</td>
<td>4/0</td>
<td>4/1</td>
<td>3/0</td>
</tr>
<tr>
<td>7</td>
<td>0/1</td>
<td>1/1</td>
<td>0/1</td>
<td>2/1</td>
<td>4/1</td>
<td>4/1</td>
<td>1/0</td>
</tr>
</tbody>
</table>
The state and output sequences for each machine $M^\mu$ beginning in state $\mu(q_0)$ are:

<table>
<thead>
<tr>
<th>States</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>$M_1^\mu$</td>
<td>1, 3, 1, 3, 1, ...</td>
</tr>
<tr>
<td>$M_2^\mu$</td>
<td>0, 6, 0, 6, 0, ...</td>
</tr>
<tr>
<td>$M_3^\mu$</td>
<td>2, 7, 2, 7, 2, ...</td>
</tr>
<tr>
<td>$M_4^\mu$</td>
<td>0, 5, 4, 4, 4, ...</td>
</tr>
<tr>
<td>$M_5^\mu$</td>
<td>4, 6, 4, 6, 4, ...</td>
</tr>
<tr>
<td>$M_6^\mu$</td>
<td>0, 3, 1, 3, 1, ...</td>
</tr>
</tbody>
</table>

Clearly the faults $\mu_1$, $\mu_4$ and $\mu_6$ are not $q_0$-masked. From the state sequences we obtain:

$$U_1 = \{(0, 0), (0, 1), (0, 2), (0, 4), (7, 3), (7, 4), (7, 5), (7, 6), (7, 7)\}.$$  

The output equivalence relation is

$$\equiv_1 = \{0, 1, 2, 3, 4; 5, 6, 7\}$$

and Theorem 1.1 is verified because $U_1 \not\subseteq \equiv_1$ and not all faults in $S_3[1]$ are $q_0$-masked. The sets of right relatives are

$$\begin{align*}
[0]_{\mu_1} &= \{1\}, & [0]_{\mu_2} &= \{0\}, & [0]_{\mu_3} &= \{2\} \\
[0]_{\mu_4} &= \{0, 4\}, & [0]_{\mu_5} &= \{4\}, & [0]_{\mu_6} &= \{0, 1\} \\
[7]_{\mu_1} &= \{3\}, & [7]_{\mu_2} &= \{6\}, & [7]_{\mu_3} &= \{7\} \\
[7]_{\mu_4} &= \{4, 5\}, & [7]_{\mu_5} &= \{6\}, & [7]_{\mu_6} &= \{3\}
\end{align*}$$

From these we see that, for example, $\mu_1$ is not $q_0$-masked because the condition of Lemma 1.1
Now let $M'$ be a Mealy machine with the same transition function as $M$ and any output assignment such that all $\mu \in S_3[1]$ are $q_0$-masked. (At least two assignments exist: $\omega(q, a) = 0$ and $\omega(q, a) = 1$ for all states in $Q$.) Then

$$E_1 = \{1, 2, 3, 4, 5, 6, 7\}$$

and $E_1 \subseteq \tau$ (Corollary 1.1.1) imply that $M'$ cannot realize any non-trivial behavior. In other words, there is no output assignment such that machine $M'$ with that output assignment and the transition function of $M$ can realize a nontrivial behavior and $q_0$-mask all $\mu \in S_3[1]$.

To correct the deficiencies of this machine consider another Example 1.3

Let $M$ be the same machine as the previous example with two exceptions:

1) $\delta(5, a) = 2$.
2) $\omega(3, a) = 1$

These changes yield

$$U_1 = \{ (0, 0), (0, 1), (0, 2), (0, 4), (7, 3), (7, 5), (7, 6), (7, 7) \}$$

and

$$\tau_1 = \{ 0, 1, 2, 4; \quad 3, 5, 6, 7 \}.$$
and all faults in \(S_3[1]\) are \(q_0\)-masked, a result which is in agreement with Theorem 1.1.

A machine \(M'\) with the output assignment
\[
\omega(0, a) = \omega(1, a) = \omega(2, a) = \omega(4, a) = 1 \\
\omega(3, a) = \omega(5, a) = \omega(6, a) = \omega(7, a) = 0
\]
and the transition function of \(M\) realizes the periodic sequence 1010... such that \(\mu\) is \(q_0\)-masked for all \(\mu \in S_3[1]\). From 
\[
E_1 = \{0, 1, 2, 4; 3, 5, 6, 7\}
\]
and Corollary 1.1.1 we see that this sequence is the only other non-trivial behavior realizable with the transition function of \(M\) such that all \(\mu \in S_3[1]\) are \(q_0\)-masked.

The fact that \(E_k\) must be a subset of \(= 1\) implies that many state assignments for \(M\) will not lead to \(q_0\)-masking all faults in \(S_{n}[k]\) because a suitable output assignment cannot be found. Some information to narrow the choice for state assignment can be obtained by considering state equivalence and the set of machines \(M^{\mu}, \mu \in S_{n}[k]\). We begin by defining an equivalence relation on \([q]_\mu | q \in Q_0\} and another on \([q] | q \in Q_0\}.

**Definition 1.2**

For \(q_1, q_2 \in Q_0, \mu \in S_{n}[k]\)
\[
[q_1]_\mu \sim [q_2]_\mu \text{ if } \forall q'_1 \in [q_1]_\mu, q'_2 \in [q_2]_\mu, q'_1 = M^{\mu} q'_2
\]
\[
(\sim_{M^{\mu}} \text{ is state equivalence in } M^{\mu}).
\]
Definition 1.3

For $q_1, q_2 \in Q_0$

$$[q_1] \sim [q_2] \iff \text{for all } \mu \in S_n[k], [q_1]_\mu \sim [q_2]_\mu.$$  

Theorem 1.2

If $M$ is a state assigned Mealy machine with $\mu$ $q_0$-masked,

for all $\mu \in S_n[k]$, then for all $q_1, q_2 \in Q_0$

$$\exists \mu \in S_n[k] \text{ such that } [q_1]_\mu \sim [q_2]_\mu \implies [q_1] \sim [q_2].$$

Proof.

If $[q_1]_\mu \sim [q_2]_\mu$ and $q'_1 \in [q_1]_\mu$, $q'_2 \in [q_2]_\mu$, then, by definition,

$$q'_1 \stackrel{M^\mu}{=} q'_2$$

and so

$$\beta^\mu_{q'_1} = \beta^\mu_{q'_2}.$$  

By Lemma 1.1, since $\mu$ is $q_0$-masked

$$\beta^\mu_{q'_1} = \beta_{q_1} \quad \text{and} \quad \beta^\mu_{q'_2} = \beta_{q_2},$$

so that

$$\beta_{q_1} = \beta_{q_2}.$$  

Now let $\gamma \in S_n[k]$ with $q''_1 \in [q_1]_\gamma$, $q''_2 \in [q_2]_\gamma$; since $\gamma$ is $q_0$-masked,

$$\beta^\gamma_{q''_1} = \beta_{q_1} = \beta_{q_2} = \beta^\gamma_{q''_2}$$

so that

$$q''_1 \stackrel{M^\gamma}{=} q''_2.$$
But $q_1''$ and $q_2''$ are any states in $[q_1]_\gamma$ and $[q_2]_\gamma$ respectively, so that

$$[q_1]_\gamma \sim [q_2]_\gamma$$

and since $\gamma$ is any fault in $S_n[k]$, the result holds for all faults in $S_n[k]$, i.e.

$$[q_1] \sim [q_2]$$

which concludes the proof.

**Corollary 1.2.1**

If $\mu$ is $q_0$-masked, for all $\mu \in S_n[k]$, then

$$q_1 \equiv M q_2 \iff [q_1] \sim [q_2].$$

Therefore $q_0$-masking all $\mu \in S_n[k]$ implies that if any machine $M^\mu$ has states in $[q_1]_\mu$ and $[q_2]_\mu$ (as defined above) which are equivalent, all machines have states in $[q_1]$ and $[q_2]$ which are equivalent.

Some notation which was introduced in QPR4 and is useful in the following discussion is reviewed here. For $\mu \in S_n$, the index sets of the free coordinates, stuck-at 0 coordinates, stuck-at 1 coordinates, and stuck-at coordinates are denoted by $X(\mu)$, $0(\mu)$, $1(\mu)$, and $C(\mu)$ respectively. That is, if $\mu = (\mu_1, \mu_2, \ldots, \mu_n)$ then

$$X(\mu) = \{ i \mid \mu_i = \alpha_x \},$$

$$0(\mu) = \{ i \mid \mu_i = \alpha_0 \},$$

$$1(\mu) = \{ i \mid \mu_i = \alpha_1 \},$$

$$C(\mu) = 0(\mu) \cup 1(\mu).$$
Similarly for \( q = (b_1, b_2, \ldots, b_n) \in \{0, 1\}^n \), let
\[
0(q) = \{ i | b_i = 0 \}
\]
\[
1(q) = \{ i | b_i = 1 \}.
\]

Now we consider three observations which are the basis for two methods of relating the machines \( M^\mu \) and the state assignment for \( M \).

The first observation shows how information about the images of a state \( r \) under a set of faults \( F \) is used to determine the coordinates of \( r \). For a subset \( F \) of \( S_n \) and \( r = (r_1, r_2, \ldots, r_n) \)
\[
r_j = \begin{cases} 
0, & \text{if there exists } \mu \in F \text{ such that } j \in X(\mu) \cap 0(\mu(r)) \\
1, & \text{if there exists } \mu \in F \text{ such that } j \in X(\mu) \cap 1(\mu(r)) \\
\text{indeterminate, if for all } \gamma \in F, j \in C(\gamma) 
\end{cases} \tag{1.4}
\]

In the special case that there is a unique image under the set of faults, the next two observations show how the coordinates of \( r \) can be obtained from information about the faults.

**Theorem 1.3**

Let \( F \) be a subset of \( S_n \).

\[ \exists q \text{ such that } q \in \bigcap_{\mu \in F} R(\mu) \implies \text{for all } \mu, \gamma \in F, 0(\mu) \cap 1(\gamma) = \emptyset \]

**Proof.**

Suppose \( q \in \bigcap_{\mu \in F} R(\mu) \) and \( \mu, \gamma \in F \). By Lemma 4/1.3
\[
0(q) = 0(\mu(q)) = 0(\mu) \cup 0(q X(\mu)) \\
1(q) = 1(\gamma(q)) = 1(\gamma) \cup 1(q X(\gamma))
\]
so that

$$0(\mu) \subseteq 0(q) \text{ and } 1(\gamma) \subseteq 1(q).$$

But $0(q) \cap 1(q) = \emptyset$ and therefore

$$0(\mu) \cap 1(\gamma) = \emptyset$$

which proves the theorem.

Clearly, $F$ must be a proper subset of $S_n$ if $\bigcap_{\mu \in F} \bar{A}(\mu) \neq \emptyset$.

**Theorem 1.4**

If $F$ is a subset of $S_n$, $\mu \in F$ and $\mu(r) = s \in \bigcap_{\gamma \in F} \bar{A}(\gamma)$ then

$$r_j = \begin{cases} 
0, & \text{if } j \in X(\mu) \text{ and there exists } \gamma \in F \text{ such that } j \in 0(\gamma) \\
1, & \text{if } j \in X(\mu) \text{ and there exists } \gamma \in F \text{ such that } j \in 1(\gamma) \\
s_j, & \text{if for all } \gamma \in F, j \in X(\gamma) \\
\text{indeterminate, if } j \in C(\mu)
\end{cases}$$

**Proof.**

Let $j$ represent a coordinate of $r$, then since $\mu(r) = s$

$$j \in X(\mu) \implies r_j = s_j.$$ 

By Theorem 1.3

$$\forall \gamma \in F, 0(\gamma) \subseteq 0(s) \text{ and } 1(\gamma) \subseteq 1(s).$$

so that

$$\exists \gamma \in F \text{ such that } j \in 0(\gamma) \implies j \in 0(s).$$
Together these remarks imply
\[ j \in X(\mu) \text{ and there exists } \gamma \in F \text{ such that } j \in 0(\gamma) \implies r_j = 0 \]
and similarly
\[ j \in X(\mu) \text{ and there exists } \gamma \in F \text{ such that } j \in 1(\gamma) \implies r_j = 1. \]
Finally
\[ j \in C(\mu) \implies r_j = 0 \text{ or } 1 \]
since \( \mu_j(0) = \mu_j(1) \). This concludes the proof.

Now we consider the application of these observations to the problem of relating the machines \( M^{\mu}, \mu \in S_n[k] \), in terms of the state sets \([q], q \in Q_0\), to the state assignment for \( M \). In both cases we are dealing with known sets of states \([q]\) and \([s]\) where \( s = \delta(q, a), a \in I \). The object is to relate subsets of \([q]\) and \([s]\)

1) to each other by determining the correspondence between states and machines \( M^{\mu} \), and then

2) to the machine \( M \) by determining the state(s) \( r \) which arise from fault free transitions
\[ \delta(q', a) = r, \quad q' \in [q] \]
To introduce some notation, let
\[ \delta^\mu([q][\mu], z) = \{s' \mid \text{there exists } q' \in [q][\mu] \text{ such that } \delta^\mu(q', z) = s'\} \quad (1.5) \]
for \( z \in I^* \). Then we note that
\[ \forall \mu \in S_n[k], \forall z \in I^*, \delta^\mu([q][\mu], z) \subseteq [\delta(q, z)]_\mu \quad (1.6) \]
since \( s' \in \delta^\mu([q][\mu], z) \) implies
there exists $q' \in [q]$ such that $\tilde{\delta}^\mu(q', z) = s'$

and

$$q \cup \mu q' \implies \delta(q, z) \cup \mu \tilde{\delta}^\mu(q', z) \implies s' \in [\delta(q, z)]_\mu .$$

In the first case we deal with the divergence to states $s_1, s_2, \ldots, s_m$ as shown in the diagram

![Diagram](image)

Let $q \in Q_0$ and $q_1 \bigcap \gamma \in [q]$ such that $\delta(q_1, a) = r$, $a \in I$ and

$$\mu_i(r) = s_i, \mu_i \in F, i=1, 2, \ldots, m.$$ Then information about the states $s_i$ and (1.4) can be used to specify $r$.

**Example 1.4**

Let $F = \{\mu_1, \mu_2, \mu_3\}$ where

$$\mu_1 = \text{x0xxx},$$
$$\mu_2 = \text{xx0xx},$$
$$\mu_3 = \text{xxxx0}$$

and $M$ be a state assigned machine such that

$$q_1 = 0 \in \bigcap_{\gamma \in F} [q]_\gamma ,$$
\[ s_1 = \delta_{\mu_1}(q_1, a) = 23 \]
\[ s_2 = \delta_{\mu_2}(q_1, a) = 27 \]
\[ s_3 = \delta_{\mu_3}(q_1, a) = 30 \]

Then for \( r = (r_1, r_2, r_3, r_4, r_5) \)

\[ \mu_{11} = \sigma_x, s_{11} = 1 \implies r_1 = 1 \]
\[ \mu_{22} = \sigma_x, s_{22} = 1 \implies r_2 = 1 \]
\[ \mu_{13} = \sigma_x, s_{13} = 1 \implies r_3 = 1 \]
\[ \mu_{14} = \sigma_x, s_{14} = 1 \implies r_4 = 1 \]
\[ \mu_{15} = \sigma_x, s_{15} = 1 \implies r_5 = 1 \]

so that

\[ \delta(0, a) = 31. \]

In the second case we are concerned with the convergence of states \( q_1, q_2, \ldots, q_m \) to \( s_1 \) according to the diagram

More precisely, let \( q \in Q_0 \) and for \( \mu \in F, q' \in [q]_\mu \) such that

\[ \delta(q', a) = r \text{ and } \mu(r) = s_1 \in \bigcap_{\gamma \in F} \delta'([q]\gamma, a). \]

Then information about the faults in \( F \) can be applied to the specification of states \( r \).
according to Theorem 1.4.

**Example 1.5**

Let \( \mathcal{F} = \{ \mu_1, \mu_2, \mu_3 \} \) where

\[
\begin{align*}
\mu_1 &= x1xx \vspace{2mm} \\
\mu_2 &= xxx0x \vspace{2mm} \\
\mu_3 &= xxx1
\end{align*}
\]

and \( M \) be a state-assigned machine such that

\[
\begin{align*}
q_1 &= 9 \in [q]_{\mu_1} \\
q_2 &= 13 \in [q]_{\mu_1} \\
q_3 &= 29 \in [q]_{\mu_2} \\
q_4 &= 5 \in [q]_{\mu_3} \\
s_1 &= 25 \in \bigcap_{\gamma \in \mathcal{F}} \delta(\gamma([q], a), a \in L)
\end{align*}
\]

Then for \( r_1 = (r_{11}, r_{12}, r_{13}, r_{14}, r_{15}) \)

\[
\begin{align*}
\mu_{11} &= \mu_{21} = \mu_{31} = \sigma_x, s_{11} = 1 \implies r_{11} = 1 \\
\mu_{12} &= \sigma_1 \implies r_{12} = x \\
\mu_{13} &= \mu_{23} = \mu_{33} = \sigma_x, s_{13} = 0 \implies r_{13} = 0 \\
\mu_{14} &= \sigma_x, \mu_{24} = \sigma_0 \implies r_{14} = 0 \\
\mu_{15} &= \sigma_x, \mu_{35} = \sigma_1 \implies r_{15} = 1
\end{align*}
\]

so that \( \delta(9, a) = 17 \) or 25. Similarly

\[
\begin{align*}
\delta(13, a) &= 17 \text{ or } 25 \\
\delta(29, a) &= 25 \text{ or } 27 \\
\delta(5, a) &= 24 \text{ or } 25
\end{align*}
\]
To summarize our findings we see that the search for machines which $q_0$-mask faults can be divided as follows:

1) identify state sets $[q]_\mu$ suitable for $q_0$-masking given the behavior to be realized and the faults to be masked

2) verify the state sets (state assignment for the machines $M^\mu$) by deriving the transition function for $M$ as a state assigned machine.

Most of our results apply to the problem of verification; to demonstrate the application of the definitions and theorems to this problem, we consider an example.

**Example 1.6**

The object of this example is to find

1) sequences of period 7 which can be generated by 5-dimensional machines such that all $\mu \in S_5[1]$ are $q_0$-masked, and

2) the machines which generate these sequences.

We assume a classification of states and proceed to apply the results of this report to achieve the objective. Let the faults in $S_5[1]$ be denoted by

\[
\begin{align*}
\mu_1 &= \text{xxxx1} \\
\mu_2 &= \text{xxxx0} \\
\mu_3 &= \text{xxx1x} \\
\mu_4 &= \text{xxx0x} \\
\mu_5 &= \text{xx1xx} \\
\mu_6 &= \text{xx0xx} \\
\mu_7 &= \text{x1xxx} \\
\mu_8 &= \text{x0xxx} \\
\mu_9 &= \text{1xxxx} \\
\mu_{10} &= \text{0xxxx}
\end{align*}
\]
Then the states, denoted by the decimal equivalent of the binary 5-tuple, are classified according to the following table:

<table>
<thead>
<tr>
<th>Q</th>
<th>$\mu_1$</th>
<th>$\mu_2$</th>
<th>$\mu_3$</th>
<th>$\mu_4$</th>
<th>$\mu_5$</th>
<th>$\mu_6$</th>
<th>$\mu_7$</th>
<th>$\mu_8$</th>
<th>$\mu_9$</th>
<th>$\mu_{10}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>16</td>
<td>0</td>
</tr>
<tr>
<td>31</td>
<td>11</td>
<td>30</td>
<td>30</td>
<td>29</td>
<td>29</td>
<td>27</td>
<td>15</td>
<td>23</td>
<td>27</td>
<td>15</td>
</tr>
<tr>
<td>21</td>
<td>21</td>
<td>14</td>
<td>14</td>
<td>13</td>
<td>13</td>
<td>19</td>
<td>9</td>
<td>21</td>
<td>19</td>
<td>1</td>
</tr>
<tr>
<td>17</td>
<td>17</td>
<td>6</td>
<td>6</td>
<td>12</td>
<td>12</td>
<td>18</td>
<td>28</td>
<td>17</td>
<td>18</td>
<td>10</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>20</td>
<td>22</td>
<td>20</td>
<td>22</td>
<td>25</td>
<td>25</td>
<td>3</td>
<td>25</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>26</td>
<td>3</td>
<td>25</td>
<td>5</td>
<td>26</td>
<td>26</td>
<td>5</td>
<td>26</td>
<td>5</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>24</td>
<td>7</td>
<td>24</td>
<td>7</td>
<td>24</td>
<td>24</td>
<td>7</td>
<td>24</td>
<td>7</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>16</td>
<td>0</td>
</tr>
</tbody>
</table>

This classification was obtained by trial and error to conform with the necessary conditions for $q_0$-masking of Theorems 1.1 through 1.4. The states in the first row correspond to the initial states for $q_0$-masking in a 5-dimensional machine. The states in the seventh row are the minimum number necessary to cover all the faults in $S_{511}$. The rows in between are then filled, working backward from the sixth row, with states such that a state appears in as many columns and as few rows as possible. The states in the column designated by $Q^\mu$ are in the range of the fault $\mu$ and the periodicity of states in each column is 7.
The rows of the classification table are potential sets of right relatives \([q]\) for states \(q\) reachable from \(q_0\):

\[
\{0, 1, 2, 4, 8, 16\} \\
\{11, 15, 23, 27, 29, 30, 31\} \\
\{1, 9, 13, 14, 19, 21\} \\
\{6, 10, 12, 17, 18, 28\} \\
\{3, 20, 22, 25\} \\
\{3, 5, 25, 26\} \\
\{7, 24\}
\]

If these sets are to be the right relatives \([q]\), \(q \in Q_0\), of a machine \(M\) that \(q_0\)-masks all faults in \(S_{q_0}[1]\), then by Lemma 1.1 all states in the same set must have the same output; the output assignment must define a partition which is refined by the partition

\[
\{0, 1, 2, 4, 8, 9, 13, 14, 16, 19, 21; 3, 5, 20, 22, 25, 26; 6, 10, 12, 17, 18, 28; 7, 24; 11, 15, 23, 27, 29, 30, 31\}.
\]

For the output assignment:

For all \(q \in \{0, 1, 2, 4, 8, 9, 13, 14, 16, 19, 21\}\), \(\omega(q, a) = b\), \(a \in I\)

For all \(q \in \{11, 15, 23, 27, 29, 30, 31\}\), \(\omega(q, a) = c\)

For all \(q \in \{6, 10, 12, 17, 18, 28\}\), \(\omega(q, a) = d\) \hfill (1.6)

For all \(q \in \{3, 5, 20, 22, 25, 26\}\), \(\omega(q, a) = e\)

For all \(q \in \{7, 24\}\), \(\omega(q, a) = f\)

this partition implies that sequences of the form

\[bcbdeef, \quad b, c, d, e, f, \in \{0, 1\}\]
can be generated if a machine $M$ exists with transition function such that the columns of the classification table represent the successive states of the faulty machines $M^\mu$. The transition table is therefore derived from this table using equation 1.4 and Theorem 1.4. For the transitions $\delta(0, a)$, $\delta(18, a)$, and $\delta(25, a)$ we find

$$
\begin{align*}
\delta \mu_2(0, a) = 30 & \Rightarrow \delta(0, a) = 30 \text{ or } 31 \\
\delta \mu_4(0, a) = 29 & \Rightarrow \delta(0, a) = 29 \text{ or } 31 \\
& \Rightarrow \delta(0, a) = 31 \\
\delta \mu_4(20, a) = \delta \mu_6(18, a) = \delta \mu_9(19, a) = \delta \mu_7(28, a) = s & \Rightarrow \delta(18, a) = 24 \text{ or } 25 (1100x) \\
& \Rightarrow \delta(18, a) = 25 \\
s = 25 & \Rightarrow \delta(18, a) = 25 \\
\end{align*}
$$

and

$$
\begin{align*}
\delta \mu_7(25, a) = 26 & \Rightarrow \delta(25, a) = 18 \text{ or } 26 \\
\delta \mu_9(25, a) = 26 & \Rightarrow \delta(25, a) = 10 \text{ or } 26 \\
& \Rightarrow \delta(25, a) = 26 \\
\end{align*}
$$

In summary, the transition table is:
Note that there is no output assignment such that nontrivial sequences of period less than 7 can be realized with this transition function and all \( \mu \in S_5[1] \) are \( q_0 \)-masked. This is because each column of the classification table has period not less than 7 and 7 is prime.

In conclusion we have found 30 nontrivial sequences of the form

\[
b, c, d, e, f \in \{0, 1\}
\]

which can be generated by a 5 dimensional machine such that all \( \mu \in S_5[1] \) are \( q_0 \)-masked. The machine to generate a particular sequence has the transition function of (1.7) and the output assignment given by (1.6).
2. FAULT LOCATION IN COMBINATIONAL NETWORKS

In QPR 4, the following definitions were introduced and discussed. They are repeated here for ease of reference.

If \( C = (D, S, F, b) \) is a combinational network having an \((n, m, k, \ell)\)-digraph \( D \) (\( n \) inputs, \( m \) outputs, \( k \) nodes, \( \ell \) lines), signal set \( S \), fault set \( F \), and fault-free structure \( b \); if \( f \) is any fault from the set \( F \); and if \( \alpha(f) \) is the system behavior under \( f \), then

**Definition 2.1**

- \( f \) is masked iff \( \alpha(f) = \alpha(b) \)
- \( f \) is detectable iff \( \alpha(f) \neq \alpha(b) \)

In other words, a fault \( f \) is masked when the system behavior under fault \( f \) is the same as the fault-free behavior, and is detectable otherwise.

If \( K \) denotes the set of nodes of \( C \); if \( K_i = \{ i | f_i \neq b_i, 1 \leq i \leq k \} \) denotes the set of "faulty" nodes under fault \( f \); and if \([B, A]\) denotes a closed interval in the partially ordered set of subsets of \( K \), i.e.

- \( B \subseteq K \)
- \( B \subseteq A \)
- \([B, A] = \{X | X \subseteq K, B \subseteq X \subseteq A\} \)

**Definition 2.2**

- \( f \) is \([B, A]-locatable\) if, for all \( g \in F \), \( \alpha(g) = \alpha(f) \Rightarrow K_g \in [B, A] \).

This formally states that, if the system behavior is \( \alpha(f) \) and \( f \) is \([B, A]-locatable\), then we can infer that the set of faulty nodes includes set \( B \) and is included in set \( A \). In other words without any knowledge of the present system structure, we are able to bound the set of faulty...
nodes by observing the system behavior. In the lattice of subsets of
K, B is a lower bound for the set of faulty nodes and A is an upper
bound.

Obviously, if the set of faulty nodes includes the set B it also
includes any subset B' of B, and if the set of faulty nodes is a subset
of A it is also a subset of any superset, A', of A. These simple
observations lead to the following theorem.

Theorem 2.1

In an \((n, m, k, \ell)\)-combinational network \(C = (D, S, F, b)\), if fault \(f\)
is \([B, A]\)-locatable and if \([B', A']\) is a closed interval of the
partially ordered set of subsets of \(K\) that includes interval
\([B, A]\), then \(f\) is \([B', A']\)-locatable.

Proof

See Theorem 4/2.27.

Theorem 2.1 suggests that the minimum interval \([B, A]\) for which
a fault \(f\) is \([B, A]\)-locatable would be a good indicator of the "locata-
ibility" of the fault \(f\) because it represents the most information about
the set of faulty nodes that can be deduced from knowledge of the
system behavior.

Definition 2.3

The \textbf{locatability} \(L(f)\) of a fault \(f\) is the minimum interval \([B, A]\)
for which \(f\) is \([B, A]\)-locatable, i.e., \(f\) is not \([B', A']\)-locatable
for any proper subinterval of \([B, A]\).
That $L(f)$ is well-defined for a given fault $f$ is a direct consequence of the following theorem.

**Theorem 2.2**

In a combinational network $C = (D, S, F, b)$, if $f$ is $[B, A]$-locatable and $[B', A']$-locatable, then $f$ is $[B \cup B', A \cap A']$-locatable.

**Proof**

See Theorem 4/2.28.

Suppose that a fault $f$ is $[B, A]$-locatable and $[B', A']$-locatable but not $[B'', A'']$-locatable for any proper subinterval $[B'', A'']$ of $[B, A]$ or $[B', A']$. From Theorem 2.2, $f$ is $[B \cup B', A \cap A']$-locatable, but since $[B \cup B', A \cap A'] \subseteq [B, A]$ it must be that $[B \cup B', A \cap A'] = [B, A]$ for otherwise we would violate the second part of the hypothesis. Similarly, we conclude that $[B \cup B', A \cap A'] = [B', A']$ and further that $[B, A] = [B', A']$. Thus, $L(f)$ is well-defined.

It should be noted that, although $L(f) = [B, A]$ establishes a lower bound $B$ and an upper bound $A$ on the faulty node set when the system behavior is $\alpha(f)$, it does not imply that any fault $\alpha$-equivalent to $f$ actually has faulty node set $B$ or faulty node set $A$. In fact, if $L(f) = [B, A]$ then $B$ is the greatest lower bound (g1b) and $A$ is the least upper bound (lub) of $\{K_g | \alpha(g) = \alpha(f)\}$ in the partially ordered set of subsets of $K$. Since we have a strict partial ordering, it is clear that the lub and g1b of a collection of subsets need not be included in the collection.
As an example, consider a three node system with fault-free structure \( b = (b_1, b_2, b_3) \) and fault-free behavior \( \alpha(b) \). Let \( f = (f_1, b_2, b_3) \) and \( f' = (b_1, f_2, b_3) \) be two faults with the same faulty behavior, i.e. \( \alpha(f) = \alpha(f') \neq \alpha(b) \). Further, let no other system fault produce the behavior \( \alpha(f) \). Then \( L(f) = [\emptyset, \{1, 2\}] \). Note that \( K_f = \{1\}, K_{f'} = \{2\}, \) \( \text{glb} \{K_f, K_{f'}\} = \emptyset \) and \( \text{lub} \{K_f, K_{f'}\} = \{1, 2\} \).

Recall that \( \alpha \) is a mapping whose domain is the fault set \( F \). As such it induces an equivalence relation \( \sim \) on the set \( F \), namely

\[
f \sim f' \iff \alpha(f) = \alpha(f')
\]

The close relationship between \( = \) and locatability is demonstrated by the following theorem.

**Theorem 2.3**

In a combinational network \( C = (D, S, F, b) \), a fault \( f \) is \([B, A]\)-locatable if and only if all faults \( \alpha \)-equivalent to \( f \) are \([B, A]\)-locatable.

**Proof**

If \( f \) is \([B, A]\)-locatable, then

\[
\forall g \in F, \quad \alpha(g) = \alpha(f) \Rightarrow K_g \in [B, A] \Rightarrow B \subseteq K_g \subseteq A
\]

Let \( h \) be any element of \( F \) such that \( \alpha(h) = \alpha(f) \), i.e. \( h \sim f \). Let \( e \) be any element of \( F \) that is \( \alpha \)-equivalent to \( h \), then

\[
\alpha(e) = \alpha(h) = \alpha(f) \Rightarrow K_e \in [B, A]
\]
Hence, \( h \) is \([B, A]\)-locatable. Since \( h \) was any element of \( F \) \( \alpha \)-equivalent to \( f \), it must be true that all faults \( \alpha \)-equivalent to \( f \) are \([B, A]\)-locatable.

Conversely, if all faults \( \alpha \)-equivalent to \( f \) are \([B, A]\)-locatable, then since \( f \equiv f' \) certainly \( f \) is \([B, A]\)-locatable.

It is now apparent that locatability is an invariant of \( \equiv \), i.e. all faults in the same equivalence class of \( \alpha \) have the same locatability. Stated as a corollary, this becomes:

**Corollary 2.3.1**

Locatability is an invariant of \( \equiv \), i.e. \( f \equiv f' \Rightarrow L(f) = L(g) \).

**Proof**

If \( f \equiv f' \), by Theorem 2.3 \( f \) is \( L(f') \) locatable. This implies \( L(f) \subseteq L(f') \). Similarly \( f' \) is \( L(f) \) locatable which implies \( L(f') \subseteq L(f) \). Therefore, \( L(f) = L(f') \).

Since locatability is an invariant of \( \equiv \), we will often refer to the locatability of an \( \alpha \)-equivalence class as being the locatability of any fault in the class.
To demonstrate the fact that locatability is not a complete set of invariants for $\sigma$, let us return to our example. It is certainly conceivable that two other faults $g' = (g_1, b_2, b_3)$ and $g'' = (b_1, g_2, b_3)$ might exist with $\alpha(f') \neq \alpha(g') = \alpha(g'') \neq \alpha(b)$. Furthermore, if no other fault produces behavior $\alpha(g')$, then the locatability of $g'$ and $g''$ is also $[\varnothing, \{1, 2\}]$. Since $\alpha(g') \neq \alpha(f')$, then locatability is not a complete set of invariants for $\sigma$.

If one wishes only to locate faulty nodes to within some subset $A \subseteq K$ (i.e. to locate to within "module" $A$), then

**Definition 2.4**

In a combinational network $C = (D, S, F, b)$, a fault $f$ is $A$-locatable $(A \subseteq K)$ if $f$ is $[\varnothing, A]$-locatable. In other words, $f$ is $A$-locatable if, for all $g \in F$, $\alpha(g) = \alpha(f) \Rightarrow K_g \subseteq A$. Here, the lower bound on the set of faulty nodes is the empty set $\varnothing$, indicating that we cannot guarantee that any particular node is at fault upon observation of behavior $\alpha(f)$. We can, however, restrict our attention to nodes in the set $A$, since they are the only ones that can be faulty. Note that all faults are $K$-locatable.

**Corollary 2.3.2**

In a combinational network $C = (D, S, F, b)$, a fault $f$ is $A$-locatable if and only if all faults $\alpha$-equivalent to $f$ are $A$-locatable.

If one wishes to specify precisely the set of faulty nodes upon observation of system behavior with no area of uncertainty, we must have
Definition 2.5

In a combinational network \( C = (D, S, F, b) \), a fault \( f \) is locatable if \( f \) is \([K_f, K_f]\)-locatable.

i.e., \( f \) is \([K_f, K_f]\)-locatable if, for all \( g \in F \), \( \alpha(g) = \alpha(f) \Rightarrow K_g = K_f \).

Indeed, the upper and lower bounds on the set of faulty nodes are identical and hence there can be no uncertainty as to which nodes are faulty.

Corollary 2.3.3

In a combinational network \( C = (D, S, F, b) \), a fault \( f \) is locatable if and only if all faults \( \alpha \)-equivalent to \( f \) are locatable.

Location of Masked Faults

That the set of masked faults constitutes an \( \alpha \)-equivalence class should be apparent from Definition 2.1. In particular, the set of masked faults is the \( \alpha \)-equivalence class designated \([b]_{\alpha}\) i.e. the \( \alpha \)-equivalence class containing the 0-fault. Since locatability is an invariant of \( \equiv \), we have

\[
\text{Theorem 2.4}
\]

If \( f \) is a masked fault in a combinational network \( C = (D, S, F, b) \), then

\[
L(f) = L(b)
\]

In other words, the locatability of the class of masked faults is the locatability of the zero fault.
As shown by the following theorem, \( L(b) \) can be completely specified by a single set instead of the pair of sets required to describe the locatability of an arbitrary fault.

**Theorem 2.5**

In a combinational network \( C = (D, S, F, b) \), if a masked fault is \([B,A]-locatable\), then \( B = \emptyset \).

**Proof**

Let masked fault \( f \) be \([B,A]-locatable\), then

\[
\forall g \in F, \alpha(g) = \alpha(f) \Rightarrow B \subseteq K_g \subseteq A
\]

Since \( f \) is masked, \( \sigma(b) = \alpha(f) \), and \( B \subseteq K_b \subseteq A \). But \( K_b = \emptyset \), hence \( B = \emptyset \).

Since \( L(b) \) is always \([\emptyset,A]\) for some \( A \subseteq K \), we will refer to \( A \) as the locatability of \( b \). Since \( L(f) = L(b) \) for every masked fault \( f \), the set \( A \) is the locatability of all masked faults. An important implication of this result is that an inverse relationship exists between the locatability of masked faults (or equivalently the locatability of the 0-fault) and the size of the masked fault set. This may be more apparent from the following theorem.
Theorem 2.6

In a combinational network $C = (D, S, F, b)$, a masked fault $f$ is $A$-locatable if and only if, for every $g \in F$, $K_g \not\subseteq A \Rightarrow g$ is detectable.

Proof

If $f$ is $A$-locatable, then all masked faults are $A$-locatable (Corollary 2.3.2), i.e. for every masked fault $g$, $K_g \subseteq A$. Hence, $K_g \not\subseteq A \Rightarrow g$ is not masked, i.e. $g$ is detectable.

If, $\forall g \in F$, $K_g \not\subseteq A \Rightarrow g$ is detectable, then all masked faults $f$ must have $K_f \subseteq A$, i.e. $f$ is $A$-locatable.

It should now be clear that if $L(b) = A$, then for all masked faults $f$, $K_f \subseteq A$. If $L(b)$ is made smaller, then we have a more severe constraint on the number of masked faults. In the extreme, if $b$ is locatable, that is $L(b) = \emptyset$, then all proper faults must be detectable and $b$ is the only masked fault.

Similarly, if we mask more faults, we must gradually reduce the locatability of the masked faults. In this extreme, when all faults are masked, $L(b) = K$, the whole node set. In other words, when the system behavior is $a(b)$, any node in the system may be faulty.

Single Faults

In general, a fault can be $K_f$-locatable but not locatable. However, in the case of a single detectable fault we have
Theorem 2.7

In any combinational network \( C = (D, S, F, b) \), a single detectable fault at node \( i \), \( f = (b_1, \ldots, b_i-1, b_i, b_{i+1}, \ldots, b_k) \), is \( \{i\} \)-locatable if and only if it is locatable.

Proof

If \( f \) is \( \{i\} \)-locatable and detectable, then

\[
Vg \in F, \quad \alpha(g) = \alpha(f) \Rightarrow K_g \subseteq \{i\} \Rightarrow K_g = \emptyset \text{ or } K_g = \{i\}
\]

But, since \( f \) is detectable, \( \alpha(g) = \alpha(f) \Rightarrow g \) is detectable and, hence \( K_g \neq \emptyset \). We then must have

\[
Vg \in F, \quad \alpha(g) = \alpha(f) \Rightarrow K_g = \{i\} = K_f
\]

i.e. \( f \) is locatable.

The converse is trivial. If \( f \) is locatable, then, by definition, \( f \) is \([\{i\}, \{i\}]\)-locatable. Since \([\{i\}, \{i\}] \in [\emptyset, \{i\}]\), \( f \) is \([\emptyset, \{i\}]\)-locatable (from Theorem 2.1) i.e. \( f \) is \( \{i\} \)-locatable.

General Systems Form with Single Faults

In QPR 4, necessary and sufficient conditions were stated for a single detectable fault at node 2 in a general system form with single faults to be \( \{2\} \)-locatable (and hence, locatable). We now consider the class of masked faults. From Theorem 2.6, we have
Lemma 2.8.1
A masked fault in a general system form with single faults is \{1, 2\}-locatable if and only if all single faults at node 3 are detectable.

Lemma 2.8.2
All single faults at node 3 in a nontrivial general system form with single faults are detectable if and only if \( b_2 b_1 \) is onto \( W \times U \).

Proof
Let \( f = (b_1, b_2, f_3) \) be any single fault at node 3. Since \( b_1 \) and \( b_2 \) are known, we can combine them into a single node as shown in Figure 2.1. The new circuit is a two-node system and the lemma follows directly from Theorem 4/2.12.
From Lemmas 2.8.1 and 2.8.2, we have

**Theorem 2.8a**

A masked fault in a general system form with single faults is \( \{1, 2\}\)-locatable if and only if \( b_2b_1 \) is onto \( W \times U \).

The following statement follows directly from Corollary 2.3.2.

**Theorem 2.8b**

All masked faults in a general system form with single faults are \( \{1, 2\}\)-locatable if and only if \( b_2b_1 \) is onto \( W \times U \).

We now consider the node set \( \{2, 3\} \). From Theorem 2.6,

**Lemma 2.9.1**

A masked fault in a general system form with single faults is \( \{2, 3\}\)-locatable if and only if all single faults at node 1 are detectable.

**Lemma 2.9.2**

All single faults at node 1 in a general system form with single faults are detectable if and only if

\[
\left| \left[ b_1(x) \right] b_3b_2 \right| = 1 \quad \forall x \epsilon X
\]

where

\( b_3b_2 : V \times U \rightarrow Y \)

\( b_3b_2(v, u) = b_3(b_2(v), u) \)

\( \left[ b_1(x) \right] b_3b_2 \) is the equivalence class of \( \equiv \) containing the element \( b_1(x) \).
Proof

Let \( f = (f_1, b_2, b_3) \) be any single fault at node 1. Since, \( b_2 \) and \( b_3 \) are known, we can combine them into a single node as shown in Figure 2.2.

\[
\begin{align*}
B_1 &= b_1 \\
B_2 &= b_2 b_3
\end{align*}
\]

The new circuit is a two node system and the lemma follows directly from Theorem 4/2.5.

From Lemmas 2.9.1 and 2.9.2 we have

\textbf{Theorem 2.9a}

A masked fault in a general system form with single faults is \( \{2, 3\} \)-locatable if and only if

\[
|[b_1(x)]_{b_3 b_2}| = 1 \ \forall x \in X
\]
From Corollary 2.3.2 we obtain the following version of Theorem 2.9a.

**Theorem 2.9b**

All masked faults in a general system form with single faults are \{2, 3\}-locatable if and only if

\[
\left| \left[ b_1(x) \right]_{b_2 b_3} \right| = 1 \ \forall x \in X
\]

We are now in a position to discuss locatability of faults in a general system.

**Theorem 2.10a**

A masked fault in a general system form with single faults is \{2\}-locatable if and only if

1. \( b_2 b_1 \) is onto \( W \times U \)
2. \( \left| \left[ b_1(x) \right]_{b_2 b_3} \right| = 1 \ \forall x \in X \)

**Proof**

To show necessity, let \( f \) be a masked fault that is \{2\}-locatable. Since \( \emptyset, \{2\} \subseteq \emptyset, \{2, 3\} \), \( f \) is \{2, 3\}-locatable (Theorem 2.1) and hence (2) holds (Theorem 2.9a). Similarly, since \( \emptyset, \{2\} \subseteq \emptyset, \{1, 2\} \), \( f \) is \{1, 2\}-locatable (Theorem 2.1) and therefore (1) holds (Theorem 2.8a).

To show sufficiency, let (1) and (2) be true, then (1) implies that \( f \) is \{1, 2\}-locatable (Theorem 2.8a) and (2) implies that \( f \) is \{2, 3\}-locatable (Theorem 2.9a). It then follows that \( f \) is \{2\}-locatable (Theorem 2.2).
From Corollary 2.3.2, we have

**Theorem 2.10b**

All masked faults in a general system with single faults are \{2\}-locatable if and only if

1. \( b_2b_1 \) is onto \( W \times U \)
2. \( |[b_1(x)]b_3b_2| = 1 \quad \forall x \in X \)
Sequential Machines

In the last annual report, we had introduced and discussed the concept of machine diagnosability. This concept was then used to derive techniques for modifying a given machine so that easy diagnosing experiments can be designed. The class of linear machines was found to possess some favorable properties for the design of such experiments. In this section we continue to develop some further relevant and useful properties of linear machines. Some generalizations of these properties are also made. For ease of reference, some basic definitions and results will be restated here.

Let \( M = (I, O, Q, \delta, \omega) \) be a Mealy type sequential machine having \(|Q| = n\) states and \(|O| = p\) output symbols. \( M \) is diagnosable if it has a distinguishing sequence (d.s.). \( M \) is \( k \)-diagnosable if \( k \) is the least integer such that \( M \) has a d.s. of length \( k \). \( M \) is \( k \)-definitely diagnosable (k-d.d.) if every input sequence of length \( kn \) is a d.s.

The concept of machine diagnosability is important in that it can be used to simplify the design of fault detectable sequential machine. The degree of diagnosability gives a measure of how "quickly" a machine's behavior can be checked (a \( k \)-diagnosable machine has a \( k \) degree of diagnosability). A problem of great interest is to design an optimally diagnosable machine which realizes a given machine.
behavior. This motivation underlies our studies of optimal diagnosability.

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 $K_i : Q \rightarrow O^i$ [see Lemma 3.3 of the Annual Report] induces a congruence relation on $Q$, it follows that the partition corresponding to this congruence relation is a coset partition. More precisely,

**Lemma 3.1**

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 $\pi_i$, we have

**Theorem 3.1**

Let $M$ be a linear machine over a finite field $F$ of characteristic $p$ and $|F| = p^m$, $n = \dim Q$ and $\ell = \dim O$. 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 3.1 we know that $\pi_1$ partitions $Q$ into cosets. Let $H_1$ be the set of states which are $i$-equivalent to $0$. Then $H_1$ is a subgroup of $Q$. The order of $H_1$ divides that of $Q$. Now the cardinality of $Q$ is a power of $p$, i.e. $Q$ is a $p$-group, it follows that $H_1$ is also a $p$-group or $H_1 = \{0\}$. If $H_1 = \{0\}$ or $H_1 = H_1 + 1$ then clearly $k_1 = 0$. If $H_1 \neq \{0\}$, then $|H_1| = p^{j_1}$

$$|\pi_1| = |Q/H_1| = p^{mn-j_1}$$

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

Therefore

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

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

Theorem 3.1 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 3.2

Let \( M \) be a reduced linear machine with \( q = p^m \), \( \ell \) and \( n \) given as in Theorem 3.2 and \( \ell | n \). Then \( M \) is optimally diagnosable iff \( |\pi_{i+1}| = q^\ell |\pi_i| \quad \forall i \ 1 \leq i < \frac{n}{\ell} \).

Proof

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

From Theorem 3.1, we have \( |\pi_{i+1}| = p^{\ell} |\pi_i| \), and our last assumption says \( k_i \neq \ell m \), i.e. \( k_i < \ell m \). But this says in turn that \( |\pi_i| < p^{\ell m} \) and \( |\pi_{\frac{n}{\ell}}| < p^{mn} \). Thus \( x \in \left[\frac{n}{\ell}\right] \) can not be a d.s., contrary to our assumption that \( M \) is optimally diagnosable. Conversely, if \( |\pi_{i+1}| = q^\ell |\pi_i| \), then \( \forall x \in \left[\frac{n}{\ell}\right] \), \( x \) is a d.s., i.e. \( M \) is optimally diagnosable.

The result of Theorem 3.2 can be generalized to non-linear sequential machines. We first introduce a concept of "generalized equivalence relation under some input sequence."
Definition 3.1

Let \( M = (I, O, Q, \delta, \omega) \) be a sequential machine and let \( x \in I^* \)
where \( x = y a \) (\( y \in I^*, a \in I \)). Then \( q R_x r \) if \( \omega(\delta(q, y), a) = \omega(\delta(r, y), a) \).
The partition induced by \( R_x \) is denoted \( \pi_x \).

In other words, \( q R_x r \) if the last output symbol for input sequence \( x \) is the same for initial states \( q \) and \( r \).

Theorem 3.3

If \( M = (I, O, Q, \delta, \omega) \) is a sequential machine, \( |Q| = p^n \),
\( |O| = p \) (\( p \) is an integer). Then \( M \) is optimally diagnosable iff
\[ \exists x = a_1 a_2 \ldots a_n \text{ such that } |\pi_{x_i+1} | = p |\pi_{x_i} | \quad \forall 1 \leq i < n \]
where \( x_i = a_1 a_2 \ldots a_i \).

Proof

To prove necessity, suppose there is no \( x_n \in I^n \) such that
\[ |\pi_{x_{i+1}} | = p |\pi_{x_i} | \quad \text{for } 1 \leq i < n. \]
Then \( \forall x_n \in I^n \), \( x_n \) can not be a d.s. 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 \( n \) can not be a d.s. This says that \( \exists q \neq r \) in \( Q \) \( \forall x_n \in I^n \), \( \beta_q (x) = \beta_r (x) \) i.e. \( q \equiv r \). 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 3.3 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 $d_s$. 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 $d_s$. The process is then iterated until an optimal $d_s$ of length $n$ is found or no optimal $d_s$ 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.

Returning now to the question of designing an optimally diagnosable machine which realizes a given machine behavior. From Theorem 3.3 we found that $\pi_x$ can be used to characterize an optimally diagnosable machine $M$ when $M$ satisfies the theorem's hypothesis. By Definition 3.1, $\pi_x$ is determined by both the output function $\omega$ and the state transition function $\delta$. This observation seems to indicate that with proper choice of $\delta$, we may be able to come up with an optimally diagnosable machine for any given diagnosable machine. This conjecture can be easily disproved by the following arguments. First we recall that if a machine $M$ is diagnosable, then $M$ must be reduced. Let $M$ and $M'$ be two reduced machines such that $M \equiv M'$. Then it can be shown that there exists a strong isomorphism between $M$ and $M'$ [3]. This says that the state behaviors of $M$ and $M'$ are isomorphic. Thus no choice of $\delta$ is possible. This conclusion should not discourage
our interest in the study of diagnosable and optimally diagnosable machines. For example, in the case of a redundant machine which realizes a given behavior, there are certain freedom which allow the designer to choose different δ and ω. Furthermore, the selection of δ and ω can be incorporated into the design of fault-tolerant switching network which realizes a given machine behavior. This is the main theme of our investigation.

Before concluding the discussion of machine diagnosis, we would like to remark on Theorem 4/3.12 of the annual report. This theorem says that there is a \( n = 2^s \) states, binary output, single-input machine which has a d.s. of length \( s \). But all periods from 1 to \( 2^s \) can be obtained from an \( s \)-stage shift register [2]. Thus, Theorem 4/3.12 can be generalized as follows:

**Theorem 3.4**

For every integer \( n \), there is an \( n \) state, binary output, single-input sequential machine which is optimally diagnosable.

**Network Diagnosis**

We begin by restating some basic definitions which were introduced in the annual report for ease of reference.

Let \( f_j^i: X \rightarrow \{0, 1\} \) be the Boolean function realized at node \( j \) when the gate function at node \( i \), \( g_i^1 \), is replaced by its complement, \( \overline{g_i^1} \).
Definition 3.2

Node $j$ detects node $i$ under $x$ ($x \in X$) if $f_j(x)^i \neq f_j(x)$. This is abbreviated as $j \text{d}_x i$.

Note that every node detects itself since by definition, $f_j(x)^i \neq f_j(x)$.

Definition 3.3

Node $j$ detects fault $g'_i$ under $x$ ($x \in X$) if

i) $j \text{d}_x i$

ii) $g'_1(x_1) \neq g_1(x_1)$, where $x_1$ is the input to node $i$ when $x$ is applied. This is abbreviated as $j \text{d}'_x g'_i$.

Given a network, from the analysis point of view we can only deal with the class of faults which satisfy condition (ii) of Definition 3.3. In the rest of this section we will only consider this class of faults unless explicitly stated.

Definition 3.4

A subgraph $H$ of a network graph $G$ is sensitized under $x$ if,

for all $i, j$, which are nodes in $H$, $\exists$ path from $i$ to $j \Rightarrow j$ detects $i$ under $x$.

It can be shown that $d_x$ is not in general a transitive relation on the nodes of the network graph. This observation can be easily seen to be equivalent to the fact that there is not necessarily a sensitized path passing through a sensitized node. However, if we restrict $d_x$ to the nodes of a sensitized subgraph, then $d_x$ is a partial
ordering. More precisely, if \( H \) is a subgraph of \( G \), let \( N(H) \) denote the set of nodes in \( H \), then

**Theorem 3.5**

If \( H \) is a sensitized subgraph of a network graph \( G \) (under \( x \)), then for all \( i, j, k \in N(H) \),

1) \( j \preceq x i \)
2) \( j \preceq x i \) and \( i \preceq x j \) \( \Rightarrow \) \( i = j \)
3) \( j \preceq x i \) and \( k \preceq x j \) \( \Rightarrow \) \( k \preceq x i \).

**Proof**

1) Already observed.

2) Recall that nodes in an acyclic directed graph can be labelled by integers so that node \( i \) is adjacent from nodes of labellings smaller than \( i \). Using this convention, if \( j \preceq x i \) then \( j \geq i \). Similarly \( i \preceq x j \) implies \( i \geq j \). Therefore \( i = j \).

3) In the sensitized subgraph \( H \), if \( j \preceq x i \), then by Definition 3.4 there is a path from node \( i \) to node \( j \) in \( H \). Similarly \( k \preceq x j \) means there is a path from node \( j \) to node \( k \). But the reachability in a directed graph is transitive. Thus there is a path from node \( i \) to node \( k \) and \( k \preceq x i \).

Thus, it has been shown that \( \preceq x \) is a partial ordering on \( N(H) \) if \( H \) is a sensitized subgraph. Similar results can be obtained for \( \preceq ' x \) although the notion of partial ordering no longer applies. This is stated as the next theorem.
Theorem 3.6

If $H$ is a sensitized subgraph of $G$ under $x$ then, for all $i,j,k \in N(H)$,

1) $j \xrightarrow{d_x} g'_j$

2) $j \xrightarrow{d'_x} g'_i$ and $i \xrightarrow{d_x} g'_j \implies i = j$

3) $j \xrightarrow{d'_x} g'_i$ and $k \xrightarrow{d'_x} g'_j \implies k \xrightarrow{d'_x} g'_i$

Proof

1) By definition of $d'_x$, $g'_j(x_j) \neq g_j(x_j)$ and $j \xrightarrow{d_x} i$, it follows then that $j \xrightarrow{d'_x} g'_j$.

2) $j \xrightarrow{d'_x} g'_i \implies j \geq i$ \quad $\implies i = j$.

3) $j \xrightarrow{d'_x} g'_i \implies g'_i(x_i) \neq g_i(x_i)$ and $j \xrightarrow{d_x} i$. Since $d_x$ is transitive on $N(H)$, it follows that $k \xrightarrow{d_x} i$. Now $k \xrightarrow{d_x} i$ and $g'_i(x_i) \neq g_i(x_i) \implies k \xrightarrow{d'_x} g'_i$.

A single fault at node $i$, $g'_i$, is said to be a stuck-at-0 (1) fault if $g'_i(x_i) = 0 \ (1)$ for all possible $x_i$. We use $s_0^{\top}(1)$ to denote a stuck-at-0 (1) $g'_i$. A single fault at node $i$, $g'_i$, is said to be $j$th input to node $i$ stuck-at-0 (1) fault if $g'_i(x_i) = g_i(x_i)0^{\top}(1)$ where $x_i0^{\top}(1)$ is obtained by replacing the $j$th coordinate of $x_i$ by 0(1) keeping the remaining coordinates unchanged. The latter fault is denoted $t_0^{\top}(1)$.

As an example let us consider node $i$ to be a 3-input AND gate.

Then
If \( P \) is a sensitized path which passes through node \( i \), let \( t_{i,j}^0(P) \) be the stuck-at-0 fault of the input to node \( i \) which is in \( P \). Theorem 4/3.17 can be modified to include the detection of node input stuck-at faults if the network graph satisfies some additional constraints.

**Theorem 3.7**

Let \( G \) be a combinational network graph in which every two adjacent nodes have no second path between them. If a path \( P = i_1, i_2, \ldots, i_p \) in \( G \) is 0-sensitized (under some \( x \in X \)) and 1-sensitized (under some \( y \in X \)), then all single node input-output stuck-at faults are detectable.

**Proof**

In Theorem 4/3.17 we proved that all single node (output) stuck-at faults \( s_{i,j}^0 \) and \( s_{i,j}^1 \) (\( 1 \leq j \leq P \) are detectable in \( P \). If each node in \( P \) has only unity fan-out, then \( s_{i,j}^0 \) and \( s_{i,j}^1 \) is clearly indistinguishable from \( t_{i,j}^0(P) \) and \( t_{i,j}^1(P) \) and the latter is detectable. If there exists non-unity fan-out at node \( i_j \), then the additional paths will not reconverge to \( P \) at node \( i_{j+1} \). By definition of path-sensitizing, \( i_{j+1} \) detects \( i_j \) under
x and y. Let us assume $i_{j+1}$ 0-detects $i_j$ under $x$ and 1-detects $i_j$ under $y$. Then $i_{j+1}$ detects $s_{i_j}^1(s_{i_j}^0)$ under $y(x)$. By hypothesis, $(i_j, i_{j+1})$ is the only path from node $i_j$ to node $i_{j+1}$. Thus $s_{i_j}^1(s_{i_j}^0)$ is indistinguishable from $t_{i_j}^1(P)$ ($t_{i_j}^0(P)$) at node $i_{j+1}$, and node $i_{j+1}$ detects $t_{i_j}^1(P)$ ($t_{i_j}^0(P)$) under $y(x)$. By Theorem 3.6, an output node detects $t_{i_j}^1(P)$ ($t_{i_j}^0(P)$) under $y(x)$. This completes the proof of the theorem.

The problem of multiple fault detection has been considered by many researchers [1,4] and yet it remained basically unsolved. In the following we will attempt to generalize the notions of single fault detection and sensitized subgraph to study the effect of multiple fault detection in combinational networks.

**Definition 3.5**

Let $T \subseteq N(G)$, $F_T = \{g_i' | i \in T\}$ and $j \in N(G)$. Node $j$ multiply detects fault set $F_T$ under $x$ if

1. $j \overset{d}{\overset{x}{\overset{\vee}{g_i'}}} g_i' \in F_T$,

2. $g_j(x_j^E) \neq g_j(x_j) \forall E \subseteq F_T$

and

3. $g_j'(x_j^E) \neq g_j(x_j) \forall E \subseteq F_T$

where $x_j^E$ represents input to node $j$ when the fault set $E$ occurs and $x$ is applied to the network.

This notion is sometimes abbreviated as $j m d_{x} F_T$. 


Example 3.1

Consider the following network and its network graph.

\[ b_1 = g_5(a_1, a_2) = a_1 a_2 \]
\[ b_2 = g_6(a_3) = \overline{a}_3 \]
\[ c_1 = g_7(b_1, b_2) = b_1 + b_2 \]
\[ d_1 = g_8(c_1, a_4) = c_1 a_4 \]

Figure 3.1

\[ T = \{5, 6, 8\} \]
\[ g'_5(a_1, a_2) = a_1 \]
\[ g'_6(a_3) = a_3 \]
\[ g'_8(c_1, a_4) = a_4 \]

Consider the input assignment \( \alpha(a_1, a_2, a_3, a_4) = (1, 0, 1, 1) = x \).
(1) Node 8 detects $F_T = \{g_5', g_6', g_8\}$ under $x = (1, 0, 1, 1)$.

(2) $x_8 = (c_1, a_4) = (0, 1)$

$x_8 = (1, 1) = x_8 = x_8$

$g_8(x_8) = g_8(x_8) = g_8(x_8)$

Thus node 8 multiplely detects $F_T = \{g_5', g_6', g_8\}$ under $x = (1, 0, 1, 1)$.

Theorem 3.8

If $P = i_1, i_2, \ldots, i_p$ is a sensitized path under $x$ in $G$, then the set of stuck-at faults in $P$, $F_{sx} = \{s_{ij} | k_j = 0$ or $1, 1 \leq j \leq p\}$ detected under $x$ is multiplely detected by node $i_p$ under $x$.

Proof

Suppose $\exists E = \{s_{i_j^k}, s_{i_l^m}, s_{i_m^m}, \ldots, s_{i_n^n}\} \subset F_{sx}$ such that $g_{i_j^k}(x_{i_j^k}) = g_{i_j^k}(x_{i_j^k})$.

Assuming $i_j < i_l < i_m < \ldots < i_n$, then $\forall i, i_j < i < i_l$.

Now, since $s_{i_l^k}$ is detected by $i_p$ under $x$,

$s_{i_l^k} = k = g_{i_j^k}(x_{i_l^k}) \neq g_{i_j^k}(x_{i_l^k})$. 


We claim that \( \forall i, i_\ell < i < i_m \)
\[
\{s_{i_j}, s_{i_\ell}^{k_j}\}
\]
\[
g_i(x_{i_j}^{1}, s_{i_\ell}^{k_\ell}) \neq g_i(x_i)
\]

Suppose this is not true, then \( \exists i \) such that
\[
\{s_{ij}, s_{i_\ell}^{k_\ell}\}
\]
\[
g_i(x_{ij}^{1}, s_{i_\ell}^{k_\ell}) = g_i(x_i)
\]

Choose the least such \( i \), call it \( i_f \). Then
\[
g_i(x_{i_f}^{1}, s_{i_\ell}^{k_\ell}) = g_i(x_{i_f})
\]
and yet
\[
g_{i_f}^{-1}(x_{i_f}^{1}, s_{i_\ell}^{k_\ell}) \neq g_{i_f}^{-1}(x_{i_f})
\]

Then from \( i \) to \( i_{f-1} \), all node output values differ from their fault free values yet \( i_f \) remains unchanged. This says that \( i_f \) does not detect \( s_{i_j}^{k_j} \), contrary to the assumption that \( P \) is a sensitized path by Theorem 3.6. This process can be iterated and a contradiction is obtained for the assumption that \( g_i(x_i^E) = g_i(x_i) \). Thus \( i_p \) multiply detects \( F_s \) under \( x \).

The above theorem says that in a sensitized path, any simultaneous occurrence of singly stuck-at faults is also multiply detected.

This is clearly in line with the common intuition that the last fault in a sensitized path dominates all faults that occur before it.

Theorem 3.8 can be generalized to a sensitized subgraph when the
network graph is a tree. First let us consider a single gate whose gate input is given. The gate output is said to be sensitive to the jth input under the given gate input if when the jth input is complemented, the gate output will also be complemented. Stated more precisely, if \( g_i \) is the gate function and \( x_i = (a_1, a_2, \ldots, a_r) \) is a given gate input, then gate \( i \) is sensitive to the jth input under \( x_i \) if

\[
g_i(a_1, a_2, \ldots, a_j, a_r) \neq g_i(a_1, a_2, \ldots, \overline{a_j}, \ldots, a_r).
\]

A gate function which is restricted to AND, OR, NAND or NOR types function is called a restricted gate function. This class of functions has the following interesting properties.

**Lemma 3.2**

Let \( g_i \) be a restricted gate function. If the output of gate \( i \) is sensitive to each of its inputs under some gate input \( x_i \), then it is sensitive to any combination of inputs under \( x_i \).

**Proof**

Let \( x_i = (a_1, a_2, \ldots, a_r) \). If gate \( i \) is an AND or NAND gate, then \( a_i = 1 \forall 1 \leq i \leq r \) and for any \( x_i' \) such that \( x_i' \neq x_i \), we have \( g_i(x_i) \neq g_i(x_i') \). Similarly if gate \( i \) is an OR or NOR gate, then \( a_i = 0 \forall 1 \leq i \leq r \) and we obtain the same conclusion.

We can proceed now to consider the case where more than a single path is involved. Let \( G \) be a combinational tree type network graph
whose gate functions are restricted. The following theorem gives a
set of faults which is multiplely detected by a node.

**Theorem 3.9**

Let G be a tree type combinational network graph and \( H_x \) be a
sensitized subgraph of G under x with a root \( i_0 \). Then \( i_0 \) multiplely
detects the set of stuck-at faults \( F_{H_x} \) which is detected by \( i_0 \) under x.

**Proof**

We divide the proof into two cases:

**Case 1:** By Theorem 3.8, if \( \forall E \subseteq F_{H_x} \), the faulty nodes in E belong
to the same path, then E is multiplely detected by \( i_0 \) under x.

**Case 2:** If the faulty nodes in E belong to different branches in \( H_x \),
then there exist \( i \in N(H_x) \) with in-degree of i greater than 1 and an \( E' \subseteq E \)
such that the faulty nodes in \( E' \) are predecessors of i. Choose the least
such \( i, i_m \), then by Lemma 3.2, \( g_{i_m}(x_{i_m}) = g_{i_m}(x_{i_m}) \). This argument
is then iterated on any such i with in-degree greater than 1 until \( E' = E \).

Thus \( \forall E \subseteq F_{H_x} \), E is multiplely detected by \( i_0 \) under x and
\( F_{H_x} \) is multiplely detected by \( i_0 \) under x.
REFERENCES


