V. Conclusions

First- and second-order resolution are related to simple cover algebra concepts that are in turn used to develop procedures for finding the resolutions from the generalized fault table. The procedures given here are improvements over those in [1] for resolutions over domain D_A. However, there are applications in which domains other than D_A are useful. In these cases, the second-order resolution procedure in [1] is still of value in a modified form.

References

[1] C. R. Kime, "An analysis model for digital system diagnosis," *IEEE Trans. Comput.*, vol. C-19, pp. 1063–1073, Nov. 1970.
[2] J. D. Russell and C. R. Kime, "Structural factors in the fault diagnosis of combinational networks," in *Dig. 1971 Int. Symp. Fault-Tolerant Computing*, Mar. 1971, pp. 34–39; also, *IEEE Trans. Comput.*, vol. C-20, pp. 1276–1285, Nov. 1971.
[3] D. L. Dietmeyer, *Logic Design of Digital Systems.* Boston: Allyn and Bacon, 1971.
[4] F. C. Hennie, *Finite State Models for Logical Machines.* New York: Wiley, 1968.
[5] J. Hartmanis and R. E. Stearns, *Algebraic Structure Theory of Sequential Machines.* Englewood Cliffs, N. J.: Prentice-Hall, 1966.

Stochastic Automata and the Problems of Reliability in Sequential Machines

BEHROOZ PARHAMI, STUDENT MEMBER, IEEE

Abstract—A stochastic sequential machine model is employed to investigate some of the problems concerning the reliability of sequential machines. Two methods, using the notions of entropy for stochastic automata and principal entries in their transition matrices, are used and compared for reliability estimates. The problem of synthesizing automata of given known reliability through replication and voting is also examined.

Index Terms—Majority voting, redundancy, reliability estimation, reliable automata, sequential machines, stochastic automata.

Introduction

Stochastic sequential machine models have been used in the study of finite-state communication channels, sequential switching networks made of unreliable components, and learning systems. In this note, we will employ a stochastic machine model to investigate some of the problems concerning the reliability of sequential machines. The model that we will use is a modified version of that introduced by Carlyle [1].

Definition 1: A stochastic sequential machine (SSM) is a quintuple $S=(X, Y, Q, M, F)$, in which X and Y are finite sets of inputs and outputs, respectively, and Q is a finite set consisting of n states. M is the transition function $M: X \rightarrow \mathfrak{M}_n$, where $\mathfrak{M}_n$ is the set of all $n \times n$ stochastic matrices.[1] The ij entry of $M(x)$, $x \in X$, is the probability of a transition from $q_i \in Q$ to $q_j \in Q$ when the input x is applied. F is the output function $F: Q \rightarrow Y$.

We can extend the function M to X^*, the set of all input sequences of finite length, by defining $M(\Lambda)=I_n$ and

$$M(x_1x_2 \cdots x_k) = M(x_1)M(x_2) \cdots M(x_k) \qquad (1)$$

where Λ is the input sequence of length zero and I_n is the identity matrix of size n. Then the ij entry of $M(u)$ is the probability of a transition from q_i to q_j when the input sequence u is applied.

Reliability of Sequential Machines

A deterministic sequential machine (DSM) may be regarded as an SSM for which every entry in $M(x)$ is either 0 or 1. When realized in terms of actual gates and flip-flops, of course all sequential machines behave in a probabilistic manner. This is due to the unreliability of the components of which the machine is constructed. As a result of this unreliability, the entries of $M(x)$ will no longer be only 0's and 1's. However, if the probability of failure for each component is sufficiently small, these entries will be very close to their ideal values. Hence, to each sequential machine correspond two functions, M_i and M, which describe its ideal (intended) and actual behaviors. Each entry of $M_i(x)$ is either 0 or 1. Those entries in $M(x)$ which correspond to 1's in $M_i(x)$ are called *principal entries*. Hence, every row of $M(x)$ has one, and only one, principal entry. Similarly, we can define the principal entries of $M(x_1x_2 \cdots x_k)$ as those entries which correspond to 1's in $M_i(x_1x_2 \cdots x_k)$.

We now define a measure for the reliability of synchronous sequential machines.

Definition 2: A synchronous sequential machine functions with reliability R for k cycles if its probability of being in the correct state after the application of an input sequence of length k or less is at least R.

Obviously, for a machine which is intended to be deterministic, R must be very close to 1. In what follows, we will always assume that $R \geq 0.5$.

The output y of an ideal component, gate, or flip-flop, can be written in the form $y=f(x, q)$, where x and q are its input and internal state, respectively. As a result of component faults[2] caused by temporary or permanent breakdown of elements, the preceding equation holds with probability p, which in general depends on x and q. In what follows, we will assume that p does not depend on x or q. The case where p is a function of x and q can be handled similarly, however, if we choose $p=\min_{x,q} p(x, q)$. It is also convenient to assume that the probability of failure for each component is the same for all cycles and is independent of other components. This assumption restricts the effectiveness of our method to transient faults of short duration. Permanent faults can be treated similarly if they are detected and removed promptly through diagnosis and repair.

One approach for analyzing the reliability of a sequential machine would be to find its transition matrices through

Manuscript received December 23, 1970; revised October 13, 1971. This note is adapted from a dissertation investigation while the author was at Oregon State University, Corvallis, Oreg. 97331.

The author is a student in the Department of Computer Science, University of California, Los Angeles, Calif. 90024.

[1] A matrix is stochastic if all of its entries are nonnegative and the entries of each row sum to one.

[2] We say that a fault has occurred if $y \neq f(x, q)$.

fault simulation, i.e., by studying the machine's behavior in the presence of all possible combinations of faults (or the most probable ones). These transition matrices will then completely specify the machine's behavior and hence its reliability. This method is obviously impractical for machines with a large number of states. Our approach, therefore, is to use the smallest principal entry in the set of transition matrices, or a lower bound for it, in reliability estimates.

Consider an arbitrary synchronous sequential machine realized by a set $C_1, C_2, \cdots, C_h$ of components. Let p_i denote the realiability of C_i for one cycle. Then the probability of all components functioning properly at any cycle is

$$p_0 = p_1 p_2 \cdots p_h. \tag{2}$$

Hence, given that the present state is correct, the next state will be correct with a probability of at least p_0. In other words, if p_s is the smallest principal entry in the set of matrices $\{M(x): x \in X\}$, we have

$$p_s \geq p_0. \tag{3}$$

Hence, p_0 is a lower bound for p_s. We will use this lower bound in our reliability estimates.

Reliability Estimates

We now establish some relationships between p_0, given by (2), and the reliability R (Definition 2) that will allow us to find: 1) a lower bound for R when p_0 is known, and 2) a lower bound for p_0 when the required reliability is r. We will assume in all cases that $p_0 \geq 0.5$.

Using the notion of entropy for SSM's, Tsertsvadze [2] shows that the reliability R of an n-state sequential machine for k cycles satisfies the inequality

$$g(R) \leq k[g(p_s) + (1 - p_s) \log (n - 1)] \tag{4}$$

and that

$$g(p_s) + (1 - p_s) \log (n - 1) \leq g(r)/k \tag{5}$$

is a sufficient condition for the reliability to be at least r for k cycles, where $g(t) = -t \log t - (1-t) \log (1-t)$.

Let the function $h_n(t)$ be defined by $h_n(t) = g(t) + (1-t) \log (n-1)$, and let $f^{-1}(s)$ denote the largest root of $f(t) = s$. Using inequality (3) and Fig. 1, we can write inequalities (4) and (5) in the following forms:

$$R \geq g^{-1}[k h_n(p_0)] \tag{6}$$

$$p_0 \geq h_n^{-1}[g(r)/k]. \tag{7}$$

These representations of Tsertsvadze's results will be later used for comparison purposes.

The principal entries in the transition matrices of a sequential machine can be used for reliability estimates.

Theorem 1: Let p_h denote the smallest principal entry in an $n \times n$ stochastic matrix M_h, $h = 1, 2, \cdots, k$. Then p, the smallest principal entry in $M = M_1 M_2 \cdots M_k$, satisfies the inequality $p \geq p_1 p_2 \cdots p_k$.

Proof: We prove this statement for $k = 2$. A simple induction on k will then establish the theorem. Let the principal entry of the ith row of M_1 be in the mth place. There is

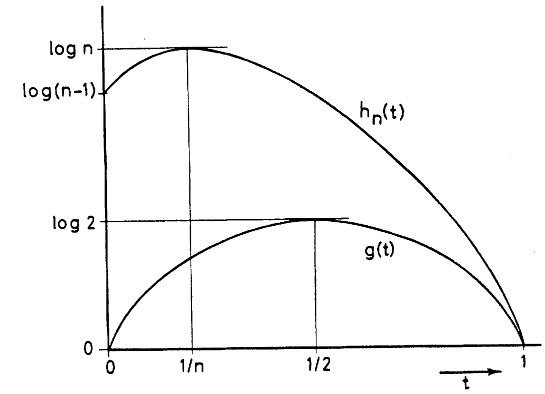

Fig. 1. Curves representing the functions $g(t)$ and $h_n(t)$.

one, and only one, column in M_2 whose mth element is a principal entry. Let this be the jth column. Then p_{ij}, the ij entry of $M = M_1 M_2$, satisfies the inequality $p_{ij} \geq p_1 p_2$. Since p_{ij} is the only principal entry in the ith row of M, the theorem is proved.

From (1) and Theorem 1, we can deduce that the smallest principal entry in $M(u_k)$ is not less than p_s^k, where u_k is an input sequence of length k. Hence, by definition

$$R \geq p_s^k. \tag{8}$$

Therefore, the following condition is sufficient for the reliability to be at least r for k cycles:

$$p_s \geq \sqrt[k]{r}. \tag{9}$$

Using inequality (3), inequalities (8) and (9) can be written in the following forms:

$$R \geq p_0^k \tag{10}$$

$$p_0 \geq \sqrt[k]{r}. \tag{11}$$

Note that inequality (10) is always defined while (6) is not.

We now prove that the bounds given by (10) and (11) are sharper (closer to actual values) than those of (6) and (7). In other words, we want to establish the following inequalities:

$$g^{-1}[k h_n(p_0)] \leq p_0^k \tag{12}$$

$$h_n^{-1}[g(r)/k] \geq \sqrt[k]{r}. \tag{13}$$

Theorem 2: For $1 \geq t \geq 0.5$, we have $k h_n(t) \geq g(t^k)$.

Proof: We can write: $1 - t^k = (1-t)(1 + t + t^2 + \cdots + t^{k-1}) \leq k(1-t)$. Hence, $t \leq 1 - (1-t^k)/k$. Since neither side of the above inequality is less than 0.5, we can write

$$g(t) \geq g[1 - (1 - t^k)/k] = g[(1 - t^k)/k]. \tag{14}$$

From the graph of $g(t)$ in Fig. 1, it is obvious that

$$g[(1 - t^k)/k] \geq g(1 - t^k)/k = g(t^k)/k, \tag{15}$$

since $(1 - t^k)/k \leq 0.5$ for all k. Combining inequalities (14) and (15) and noting that $h_n(t) \geq g(t)$ concludes the proof.

Inequalities (12) and (13) now follow directly from Theorem 2, since we have assumed that $p_0 \geq 0.5$ and $r \geq 0.5$. These inequalities imply the following.

1) For a given value of p_0, inequality (10) gives a better estimate for the reliability R than (6).

2) For a given reliability r, inequality (11) gives a smaller lower bound for p_0 than (7), and hence allows the use of less reliable components.

Furthermore, as noted earlier, inequality (10) is always defined while (6) is not. Hence, we have proved that it is preferable to use inequalities (10) and (11) for reliability estimates.

Reliable Synthesis of Sequential Machines

We have developed methods for estimating p_0, the probability of having no component failures at any cycle, for a given overall reliability r. Using this value of p_0 and (2), we can find the reliability p required of a particular component. If p does not exceed the reliability of available elements, then we synthesize the given machine with these elements and achieve reliability r. However, if elements of reliability p or higher are not available, other methods for synthesis must be employed. One such method, which we will describe in this section, is to utilize simple redundancy at the element level. In this method, we first synthesize the machine in the usual way, assuming perfect reliability for the elements. Then by replicating the original element in a majority scheme, we achieve the required component reliability. This method was first suggested by von Neumann [3].

Hence, given the required component reliability p, the reliability of available elements p_e, the reliability of majority organs p_m, we must determine the required redundancy in the majority scheme. We will assume that p_m does not depend on the number of inputs to the majority organ.

Let us consider the familiar configuration of Fig. 2, in which M is a majority organ with an odd number m of binary inputs and one binary output, and $E_1, E_2, \cdots, E_m$ are identical gates. The output y is, by definition, the majority of $y_1, y_2, \cdots, y_m$.

Let $\bar{p}$ be the probability that a majority of $y_1, y_2, \cdots, y_m$ be correct. Then

$$\bar{p} = \sum_{k=(m+1)/2}^{m} \binom{m}{k} p_e^k(1-p_e)^{m-k}. \tag{16}$$

Fig. 3 shows $\bar{p}$ as a function of p_e for different values of m. The overall reliability p for the circuit of Fig. 2 can be easily found from

$$p = \bar{p}p_m + (1-\bar{p})(1-p_m). \tag{17}$$

The following form of (17) can be used to find $\bar{p}$ when p and p_m are known ($p_m > p$):

$$\bar{p} = (p + p_m - 1)/(2p_m - 1). \tag{18}$$

Then Fig. 3 can be used to find the required redundancy.

The preceding equations are also valid for a memory element with a single output line whose next state depends only on its input (delay flip-flops for example).

For memory elements with two output lines, the configuration of Fig. 4 can be used. Then the circuit functions properly when both of its outputs are correct. If the next state of each memory element depends only on its input, as is the case for R-S flip-flops, we have the following equations (for $p_m > \sqrt{p}$) which correspond to (17) and (18):

$$p = \bar{p}p_m^2 + (1-\bar{p})(1-p_m)^2 \tag{19}$$

$$\bar{p} = [p - (1-p_m)^2]/(2p_m - 1). \tag{20}$$

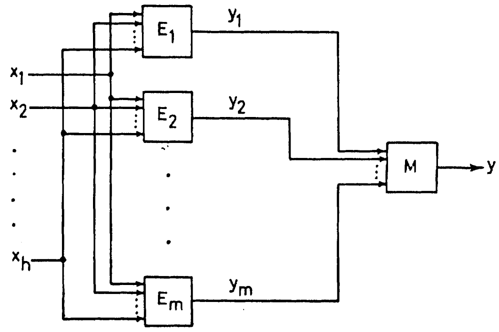

Fig. 2. Majority scheme for single-output elements.

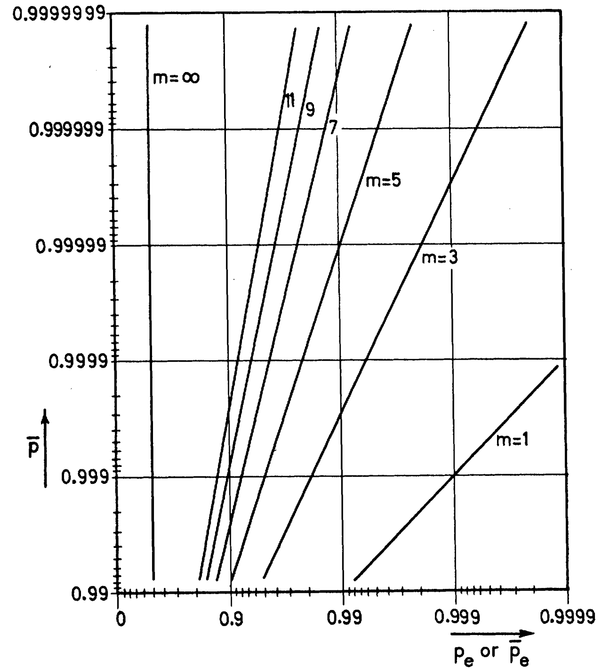

Fig. 3. The probability that a majority of m elements do not fail, $\bar{p}$, as a function of p_e, the reliability of each element.

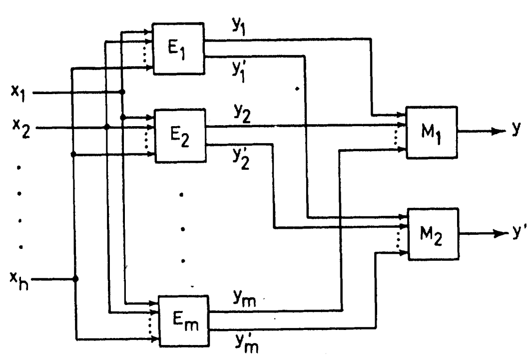

Fig. 4. Majority scheme for two-output elements.

For a memory element whose next state depends on its present state as well as the input (e.g., trigger, *J-K*, and *R-S-T* flip-flops), (16) is not valid. As an illustration, consider a set of m trigger flip-flops in a circuit similar to that of Fig. 4. Let $y_1=y_2=\cdots=y_{m-1}=1$, while $y_m=0$ because of an error in the previous cycle. Suppose that the input $x=1$ is applied to these flip-flops. Then the probability that a majority of them produce an output of 0 is not given by (16), since the mth flip-flop produces a 0 with probability $1-p_e$ instead of p_e.

In this case, an alternative method can be used. Since the operation of such flip-flops in one cycle is not independent of their operation in preceding cycles, the length of the input sequence will appear in our equations. Hence, we consider the operation of such flip-flops for input sequences of length k or less. We first prove the following theorem.

Theorem 3: Let m memory elements of reliability p_e be connected in a majority scheme. Then p_e', the probability that after k cycles the ith flip-flop is in the same state as a majority of the flip-flops, satisfies the inequality $p_e' \geq 3p_e^k-2$, provided that $p_e^k \geq 0.75$. This condition is usually satisfied in practice.

Proof: The inequality is trivial for $m=1$. Hence, since m is odd, we prove it for $m\geq 3$. Let p_c be the probability that the ith flip-flop is in the correct state and $\bar{p}_c$ be the probability that at least half of the remaining flip-flops are in the correct state. We can write

$$p_c \geq p_e^k \tag{21}$$

and

$$\begin{aligned} 1-\bar{p}_c &= \sum_{j=(m-1)/2}^{m} \binom{m-1}{j}(1-p_c)^j p_c^{m-1-j} \\ &\leq \binom{m-1}{\frac{m-1}{2}} \sum_{j=(m-1)/2}^{m-1} (1-p_c)^j \\ &\leq \binom{m-1}{\frac{m-1}{2}} (1-p_c)^{(m-1)/2} \sum_{j=0}^{\infty} (1-p_c)^j \\ &= \binom{m-1}{\frac{m-1}{2}} (1-p_c)^{(m-1)/2}/p_c. \end{aligned}$$

Using inequality (21), we find that

$$1-\bar{p}_c \leq \binom{m-1}{\frac{m-1}{2}} (1-p_e^k)^{(m-1)/2}/p_e^k. \tag{22}$$

The right-hand side of inequality (22) is a function of m, $f(m)$, and we have $f(m+2)/f(m)=4(1-p_e^k)m/(m+1)$. Hence, for $p_e^k\geq 0.75$, $f(m)$ is a decreasing function of m and its value is maximum for $m=3$. Therefore, inequality (22) can be written as

$$\bar{p}_c \geq 3-2p_e^{-k}. \tag{23}$$

On the other hand, we can write

$$p_e' = p_c\bar{p}_c + (1-p_c)(1-\bar{p}_c) \geq p_c\bar{p}_c. \tag{24}$$

Combining inequalities (21), (23), and (24), we find the desired result.

Now, let $\bar{p}_e$ be the probability that the ith flip-flop produces the correct output (the output that a majority of the flip-flops should produce). We can write $\bar{p}_e \geq p_e'p_e + (1-p_e')(1-p_e) \geq p_e'p_e$. Therefore, using Theorem 3 we obtain

$$\bar{p}_e \geq p_e(3p_e^k - 2). \tag{25}$$

By using this lower bound for $\bar{p}_e$ instead of p_e in our calculations, the methods described earlier remain valid for this case.

Summary and Conclusions

In this note, we have developed techniques for estimating the reliability of sequential machines and for their reliable synthesis. The results obtained are general in form and can be applied to any synchronous sequential machine. The following procedures are direct consequences of the results obtained in the preceding sections.

To find a lower bound for the reliability R of a sequential machine for k cycles, find p_0 from (2) and substitute in inequality (10).

To synthesize a sequential machine with a given reliability r for k cycles do the following.

1) Synthesize the machine in the usual way, assuming perfect reliability for the components.

2) Find a lower bound for p_0 from inequality (11). Then use (2) to obtain a lower bound for p_i, $i=1, 2, \cdots, h$.

3) If p_i does not exceed the reliability of available elements, the synthesis of step 1 provides the required reliability. Otherwise, use the procedure of the previous section to find the required redundancy factor.

The above procedures deal only with the number of elements in a sequential machine and do not use any structural information about the machine. On the other hand, we know that sequential machines can be designed to have some error-correcting capabilities. Obviously, in such cases, the bounds obtained by the above procedures will not be sharp. Hence, further research in this area may be directed to such special classes of sequential machines in order to obtain better bounds for reliability values.

Acknowledgment

The author is deeply indebted to Dr. R. A. Short for his help and encouragement in the course of this study.

References

[1] J. W. Carlyle, "Reduced forms for stochastic sequential machines," *J. Math. Anal. Appl.*, vol. 7, pp. 167–175, Oct. 1963.

[2] G. N. Tsertsvadze, "Stochastic automata and the problem of constructing reliable automata from unreliable elements, I," *Automat. Remote Contr.* (USSR), vol. 25, pp. 198–210, Feb. 1964.

[3] J. von Neumann, "Probabilistic logics and the synthesis of reliable organisms from unreliable components," in *Automata Studies* (Annals of Mathematical Studies, no. 34), C. E. Shannon and J. McCarthy, Eds. Princeton, N. J.: Princeton Univ. Press, 1956, pp. 43–98.